GRH via exercises

The whole collection in one file

We present the arguments of Alpöge's proof of the generalized Riemann hypothesis for Dirichlet L-functions as a series of exercise sheets, each introducing one ingredient in its simplest setting. The sheets follow the proof in the form of the rewritten Lean proof of L. Sernau, which is shorter than the Lean code first released and proves many steps by other arguments. The presentation is inspired by the problem sequences of Onishchik and Vinberg, *Lie Groups and Algebraic Groups* (Springer, 1990). The sheets are drafts written and refereed by AI agents (Claude and Codex).

Status, 26 November 2026. The collection is being extended to cover the complete proof and is updated continuously (what changed). Parts I–V and the side series are stable apart from small corrections. Parts VI–IX present the whole proof. Part VI fixes the data and all the objects, and deduces the theorem from Theorems A, B and C. Each of Parts VII–IX states its theorem in a chapter that deduces it from its inputs, and the inputs are developed in sheets, each in a simplest instance and then in general. Stated and not proved here: the results listed as background in each sheet (classical, with references); the denominators of projections and the twisting theorem (Part IX), stated with all their definitions, of which the local loss and a lemma on roots of unity are developed; and statements read from the Lean code, named where they are used. These are, in Part VII, the block identity, the archimedean Bessel functions and the estimates for the terms that survive and for the open cell, each modelled in a sheet; in Part VIII, two bounds (the projection to good forms; the dimension of the ramified forms) and the theorem on elementary divisors used at exceptional primes; in Part IX, the auxiliary forms and one operator identity.

Built 26 November 2026 from commit `cf7dac5` of
`https://github.com/ultronozm/grh-workbook`.
The sheets, one file each, and this file:
`https://ultronozm.github.io/grh-workbook/`

Contents

Part I. The target **1**
1 From zeros to a one-sided bound 1
2 Inert primes and the choice of d 8
3 The places, the weights and the remainder 14
4 Places from a sphere 19

Part II. The method **24**
5 Size against divisibility 24
6 A twist for each prime 31
7 Stepanov without multiplicity 36
8 The chain and the square root 41
9 Few translates span 48
10 Poincaré series and near orthogonality 53

Part III. Divisibility at inert primes **60**
11 Complex tori, theta functions and periods 60
12 The Fock model and theta intertwiners 65
13 Complex multiplication and reduction at an inert prime 71
14 One CM determinant: Mertens modulo 4 75
15 The invariant derivation at a supersingular prime 82
16 The isotropic plane 88
17 Pairings on a formal group of height two 93
18 Hecke nondegeneracy on the tree 102
19 The bound is attained 108

Part IV. Sizes, periods and counts **113**
20 The Kronecker limit formula and Chowla–Selberg 113

21 Masses and the count of forms . . . 119
22 The Siegel–Weil formula in the smallest case . . . 125
23 Definite theta lifts and their norms . . . 132
24 Hecke operators and theta lifts . . . 139
25 Divisibility along the chain . . . 146

Part V. Denominators and congruences **152**
26 Denominators and the Stickelberger element . . . 152
27 Odd Tate twists . . . 157
28 Odd classes by Gauss sums . . . 164
29 Congruence modules . . . 171
30 Eisenstein congruences and Selmer classes . . . 178
31 Pseudocharacters and the length bound . . . 185
32 Black box: Galois representations of eigenforms . . . 191

Part VI. The frame **199**
33 The data . . . 199
34 Spaces, forms and twists . . . 205
35 The main inequality . . . 212

Part VII. Theorem B: enough forms **216**
36 Theorem B: enough forms . . . 216
37 Unfolding twice: Gram operators as sums over rational points . . . 224
38 Which terms survive: characters, minors and the gain at the level 230
39 The open cell: Siegel's formula and Poisson summation . . . 236
40 Positive type and the bootstrap: the second moment . . . 243
41 Good forms and the count of the target . . . 249

Part VIII. Theorem A: short forms **256**
42 Theorem A: short forms . . . 256
43 The seesaw identity . . . 262
44 Transferring a Bessel period through a theta lift . . . 268
45 Two lifts at a time . . . 275
46 Lattices, cuts and the ramified forms . . . 283
47 The seesaw tensor: translated vacua, gluing and the unit . . . 290
48 Divisibility of the composite lift . . . 297

49 The count: congruences, directions and factorials 305
50 One lift at a small non-split prime 311
51 The size of the composite lift 317
52 The level prime and the ramified forms 323
53 Exceptional primes: a full mark 329

Part IX. Theorem C: the lower bound **335**
54 Theorem C 335
55 The determinant of a chain 338
56 The norm of one lift 343
57 Equal multiplicities 350
58 The exchange identity 357
59 Squares and the triangle 365
60 The cost of one lift 371
61 Compressions and false lifts 374
62 Hecke values as norms of lifts 380
63 The bound is attained at many places 387
64 Test forms and the height of a Hecke ratio 393
65 Denominators of projections to lifts 399
66 The local loss and the sparse places 410
67 Twists with few congruences 416
68 Roots of unity for many polynomials 422

Side series: a model in the function-field setting **426**
S1 The sign-only proof of the Riemann hypothesis for curves 426
S2 Deligne's bound by the sign-only method 433

FROM ZEROS TO A ONE-SIDED BOUND

Prerequisites. The zeta function and Dirichlet L-functions as in [Dav]: orthogonality of characters and $L(1,\chi) \neq 0$ for nonprincipal χ (Ch. 4), the class number formula (Ch. 6), the Hadamard product and the constant B (Ch. 12), nonvanishing on $\operatorname{Re} s = 1$ (Ch. 13 and 14), the explicit formula for Chebyshev's function $\psi(x)$ and its contour shift (Ch. 17), their analogues for $L(s,\chi)$ (Ch. 12 and 19), and the prime number theorem in progressions to a fixed modulus (Ch. 20). Chebyshev's bound $\psi(x) \ll x$ [MV, §2.2]. Mellin transforms. Landau's theorem is stated in §1.2. Section 1.4 uses the auxiliary-prime theorem stated as Theorem 2.2.2 in Chapter 2. Chapter 16 is used only for motivation, in §1.3.

A comparison of divisibility with size, as in Chebyshev's method, gives upper bounds for weighted sums over primes. Can an upper bound for a sum over primes prove the Riemann hypothesis? This chapter shows that it can, for a suitable weight. After the zeta function, Theorem 1.4.1 gives the criterion for Dirichlet L-functions in the form used in the proof. The upper bound itself is not treated here.

1.1. The ramp sum

Write $v_+ := \max(v, 0)$ for real v, and let Λ be the von Mangoldt function. The *ramp* at x is the function $n \mapsto (x/n - 1)_+$: it is large for small n, decreases, and vanishes for $n \geq x$. Let

$$S(x) := \sum_n \Lambda(n)\Big(\frac{x}{n} - 1\Big)_+, \qquad G(x) := S(x) - x\log x + (1+\gamma)x, \tag{1}$$

where γ is Euler's constant, and let $\psi(x) := \sum_{n \leq x} \Lambda(n)$ be Chebyshev's function. In §1.4, ψ denotes a Dirichlet character. The two subtracted terms are the main term of S, as the problems show.

Problem 1.1.1. For $n \geq 1$ and $\operatorname{Re} s > 1$, $\int_1^\infty (x/n - 1)_+ \, x^{-s-1}\, dx = n^{-s}/\big(s(s-1)\big)$.

Problem 1.1.2. $S(x) = x\int_1^x \psi(t)\, t^{-2}\, dt$. Hence $G(x) \ll x\log x$ for $x \geq 2$.

Problem 1.1.3. For $\operatorname{Re} s > 1$,

$$F(s) := \int_1^\infty G(x)\, x^{-s-1}\, dx = -\frac{\zeta'}{\zeta}(s)\,\frac{1}{s(s-1)} - \frac{1}{(s-1)^2} + \frac{1+\gamma}{s-1}. \tag{2}$$

Problem 1.1.4. F is meromorphic in $\mathbb{C}$ and regular at $s = 1$. Its poles in $\operatorname{Re} s > 0$ are the zeros ρ of ζ in the critical strip $0 \leq \operatorname{Re} s \leq 1$, and a zero of multiplicity m gives residue $-m/\big(\rho(\rho-1)\big)$.

Problem 1.1.5. The residue of $F(s)x^s$ at $s = 0$ is $\log 2\pi$.

Problems 1.1.3–1.1.5 and a contour shift as in [Dav, Ch. 17], applied to $-\frac{\zeta'}{\zeta}(s)\, x^s/(s(s-1))$, the part of $F(s)x^s$ that comes from S, where now every integral converges absolutely because of the factor $1/(s(s-1))$, give the following.

Date: November 26, 2026.

Theorem 1.1.1. *For $x > 1$,*

$$G(x) = \log 2\pi - \sum_\rho \frac{x^\rho}{\rho(\rho-1)} + O(x^{-2}),$$

where ρ runs over the zeros of ζ in the critical strip with multiplicity, and the sum converges absolutely.

Problem 1.1.6. $\sum_\rho 1/\big(\rho(1-\rho)\big) = 2 + \gamma - \log 4\pi = 0.0461\ldots$, with multiplicity.

Problem 1.1.7. If the Riemann hypothesis holds, then $|G(x) - \log 2\pi| \le (2 + \gamma - \log 4\pi)\sqrt{x} + O(x^{-2})$.

For instance $G(10^4) \approx 1.749$, $G(10^5) \approx 3.671$, $G(10^6) \approx 11.040$ and $G(2 \cdot 10^6) \approx -12.268$, to be compared with $\log 2\pi \approx 1.838$ and $0.0462\sqrt{10^6} = 46.2$.

Problem 1.1.8. Let $\rho = \beta + i\gamma_0$ be a nonreal zero of ζ, and let $c := -1/\big(\rho(\rho-1)\big)$. The joint term $cx^\rho + \bar{c}x^{\bar\rho}$ of ρ and $\bar\rho$ in Theorem 1.1.1 exceeds $|c|x^\beta$ for all x in a set whose image under log has density $1/3$ in $[0,\infty)$, and it is less than $-|c|x^\beta$ on another such set.

If $\beta > \frac12$, the contribution of this conjugate pair exceeds $\sqrt{x}$ along one sequence tending to infinity and falls below $-\sqrt{x}$ along another. A comparison of divisibility with size sees only one sign. The next section shows that one is enough.

1.2. One side suffices

We use the following measurable version of Landau's theorem [Lan]. Montgomery and Vaughan [MV, Lemma 15.1] assume local Riemann integrability and use x^{-s}; their proof applies to the Lebesgue integral below after replacing s by $s+1$. Let $A\colon [1,\infty) \to \mathbb{R}$ be measurable and bounded on compact sets, with $A(x) \ge 0$ for $x \ge X_0$. Let σ_c be the infimum of the real σ with $\int_1^\infty |A(x)| x^{-\sigma-1}\,dx < \infty$, and suppose that $-\infty < \sigma_c < \infty$. Then $H(s) := \int_1^\infty A(x) x^{-s-1}\,dx$ is holomorphic in $\operatorname{Re} s > \sigma_c$, and it has no holomorphic continuation to a neighborhood of σ_c.

Problem 1.2.1. In this situation $H(\sigma)$ is bounded below for real $\sigma \in (\sigma_c, \sigma_c + 1]$.

Fix $0 < \theta < 1$, suppose that $G(x) \le x^\theta$ for all large x, and let $A(x) := x^\theta - G(x)$.

Problem 1.2.2. $-\infty < \sigma_c \le 1$, and $H(s) = 1/(s-\theta) - F(s)$ for $\operatorname{Re} s > 1$.

Problem 1.2.3. $\zeta(\sigma) < 0$ for $0 < \sigma < 1$.

Problem 1.2.4. If $\sigma_c > \theta$, then σ_c is a real zero of ζ, and $H(\sigma) \to -\infty$ as $\sigma \downarrow \sigma_c$. Hence $\sigma_c \le \theta$.

By Problem 1.2.3 ζ has no real zero in $(0,1)$, but Problem 1.2.4 does not use this, and in §1.4 the same argument will be applied where real zeros cannot be excluded in advance. By Problem 1.2.4, $F = 1/(s-\theta) - H$ is holomorphic in $\operatorname{Re} s > \theta$, and by Problem 1.1.4 this excludes zeros there.

Theorem 1.2.1. *Let $0 < \theta < 1$. If $G(x) \le x^\theta$ for all large x, then ζ has no zeros in $\operatorname{Re} s > \theta$.*

Problem 1.2.5. If for every $\varepsilon > 0$ one has $G(x) \le x^{1/2+\varepsilon}$ for all large x, then the Riemann hypothesis holds.

The transform F continues meromorphically, with at most simple poles in $\operatorname{Re} s > 0$. This, the sign of its residues at real points to the right of θ, and the eventual upper bound for G are what the argument of Problem 1.2.4 uses. In the variable $v = \log x$, with $E(v) := e^{-v}G(e^v)$, the transform $F(s)$ becomes $\int_0^\infty E(v)e^{(1-s)v}\,dv$, and the bound $G(x) \le x^\theta$ becomes $E(v) \le e^{(\theta-1)v}$. In this form the argument proves the following.

Theorem 1.2.2. *Let $E\colon \mathbb{R} \to \mathbb{R}$ and $r\colon \mathbb{C} \to \mathbb{C}$. Suppose that E is Borel measurable, and that there are $C \in \mathbb{R}$ and a meromorphic function Φ on $\mathbb{C}$ such that $|E(v)| \le Ce^v$ for all $v \ge 0$, such that $\Phi(s) = \int_0^\infty E(v)e^{(1-s)v}\,dv$ for all s with $\operatorname{Re} s > 2$, and such that $(z-\rho)\Phi(z) \to r(\rho)$ as $z \to \rho$, $z \ne \rho$, for every ρ with $\operatorname{Re}\rho > 0$. Let $\beta > 0$. Suppose that $\operatorname{Re} r(x) \ge 0$ for every real $x > \beta$, and that there is V with $E(v) \le e^{(\beta-1)v}$ for all $v \ge V$. Then $r(\rho) = 0$ for every $\rho \in \mathbb{C}$ with $\operatorname{Re}\rho > \beta$.*

The hypothesis on Φ says that its poles in $\operatorname{Re} s > 0$ are simple, with residues r; the conclusion says that it has none in $\operatorname{Re} s > \beta$. Only a sign is assumed at real points, and only there.

1.3. Smoothing, and the triangle weight

Why the ramp, and not another weight? Let $\phi\colon (0,\infty) \to \mathbb{R}$ be measurable, vanish on $(1,\infty)$, be bounded on compact subsets of $(0,1]$, and satisfy $\phi(t) = O(1/t)$ as $t \to 0$. Let

$$\psi_\phi(x) := \sum_n \Lambda(n)\phi(n/x), \qquad \tilde\phi(s) := \int_0^\infty \phi(t)t^{s-1}\,dt \quad (\operatorname{Re} s > 1).$$

We use $\tilde\phi$ on its half-plane of absolute convergence and, for the three weights below, also for the meromorphic continuation given by their rational formulas. The sharp cutoff $\phi = \mathbf{1}_{(0,1]}$ gives $\psi_\phi = \psi$ and $\tilde\phi(s) = 1/s$. The ramp is $\phi(t) = (1/t - 1)_+$, with $\tilde\phi(s) = 1/(s(s-1))$ by Problem 1.1.1. The *triangle weight* is $\phi(t) = (1-t)_+$, with $\psi_\phi(x) = x^{-1}\int_0^x \psi(t)\,dt$.

Problem 1.3.1. For $\operatorname{Re} s > 1$, $\int_0^\infty \psi_\phi(x)x^{-s-1}\,dx = -\frac{\zeta'}{\zeta}(s)\,\tilde\phi(s)$.

Problem 1.3.2. For the triangle weight $\tilde\phi(s) = 1/(s(s+1))$ for $\operatorname{Re} s > 0$. If $\phi_1(t) := \phi(t)/t$, then $\tilde\phi_1(s) = \tilde\phi(s-1)$ wherever either integral converges absolutely; for the triangle weight ϕ_1 is the ramp.

The following theorem is proved as Theorem 1.1.1: by Problem 1.3.1 with $\tilde\phi(s) = 1/(s(s+1))$, shift the line of integration to $\operatorname{Re} s = -3/2$ as in [Dav, Ch. 17], along horizontal segments at heights T where $\zeta'/\zeta \ll \log^2 T$. The factor $1/(s(s+1))$ makes every integral converge absolutely, and the poles of $-\frac{\zeta'}{\zeta}(s)\,x^s/(s(s+1))$ to the right of $-3/2$ are at 1, 0, -1 and the zeros ρ.

Theorem 1.3.1. *For $x > 1$,*

$$\sum_{n\le x}\Lambda(n)\Big(1-\frac{n}{x}\Big) = \frac{x}{2} - \log 2\pi - \sum_\rho \frac{x^\rho}{\rho(\rho+1)} + O\Big(\frac{1}{x}\Big).$$

As a check, the left side minus $(x/2 - \log 2\pi)$ is approximately 0.106, 7.975 and -12.115 at $x = 10^4$, 10^6 and $2\cdot 10^6$. For the ramp and the triangle weight

$|\tilde{\phi}(\rho)| \ll |\rho|^{-2}$, so the sums over zeros converge absolutely. For the sharp cutoff they do not, since $\sum_\rho 1/|\rho|$ diverges.

Problem 1.3.3. Let $0 < \theta < 1$. If $\sum_{n\le x} \Lambda(n)(1-n/x) \le x/2 + x^\theta$ for all large x, then ζ has no zeros in $\operatorname{Re} s > \theta$.

We return to real zeros in §1.4.

The ramp itself is forced by the arithmetic. Theorem 16.3.1 gives, at primes $p \equiv 3 \pmod 8$, lower bounds for p-adic valuations of the form $\sum_{i \text{ odd}} (\lfloor a/p^i \rfloor - w)_+$. Up to an error of 1 for each odd i with $p^i \le a$, and with $a = wx$, the summand is $(a/p^i - w)_+ = w(x/p^i - 1)_+$, which is w times the ramp at x. Bounds of this form at every inert prime, summed with weights $\log p$, give the ramp sum over odd powers of primes inert in an imaginary quadratic field; Chapter 2 says what this sum counts.

1.4. Dirichlet L-functions

What replaces G for the L-functions of the characters modulo q? The arithmetic bounds sums over primes that do not split in an imaginary quadratic field. For a prime $d \equiv 3 \pmod 4$, the Legendre symbol $\chi_d(n) = (n/d)$ is the character of $K = \mathbb{Q}(\sqrt{-d})$, and at a prime p the weight $1 - \chi_d(p)$ is 2 if p is inert, 1 if $p = d$, and 0 if p splits. This weight brings in the twisted L-functions $L(s, \psi\chi_d)$, whose orders of vanishing are subtracted from the untwisted ones in the residues below. The prime d will be chosen so that they do not vanish where it matters.

For a primitive nonprincipal Dirichlet character χ let $c_\chi := \frac{L'}{L}(1,\chi)$ and

$$G_\chi(x) := \sum_{n\le x} \Lambda(n)\chi(n)\Big(\frac{x}{n} - 1\Big) + c_\chi x. \tag{3}$$

Let d be an odd prime, $\chi_d(n) := (n/d)$ the Legendre symbol, and $q \ge 1$ an integer prime to d. Let φ be Euler's function. For $n \ge 1$ let

$$\lambda(n) := \Lambda(n)\big(1 - \chi_d(n)\big) \text{ if } n \equiv 1 \pmod q, \qquad \lambda(n) := 0 \text{ otherwise.}$$

The analytic definitions below apply to every odd prime d. For a Dirichlet character ψ modulo q, let $L(s,\psi)$ be the meromorphic continuation of $\sum_{n\ge1} \psi(n) n^{-s}$ from $\operatorname{Re} s > 1$; its Euler product there runs over the primes $p \nmid q$. Let $E_\psi := L(\,\cdot\,, \psi)$ if ψ is not principal, and if ψ is principal let E_ψ be the entire continuation of $(s-1)L(s,\psi)$, with $E_\psi(1) = \prod_{p\mid q}(1 - p^{-1})$. Let $m_\psi(\rho) \ge 0$ be the order of vanishing of E_ψ at ρ. The product $\psi\chi_d$ is a character modulo qd; it is not principal, and we write $E_{\psi\chi_d} := L(\,\cdot\,, \psi\chi_d)$ and $m_{\psi\chi_d}$ for its order. Let

$$G_{d,q}(s) := \frac{1}{\varphi(q)}\Big(\sum_\psi \Big(\frac{E'_{\psi\chi_d}}{E_{\psi\chi_d}}(s) - \frac{E'_\psi}{E_\psi}(s)\Big) - 1\Big),$$

the sum over the characters ψ modulo q. The E's do not vanish on $\operatorname{Re} s \ge 1$, so $G_{d,q}$ is holomorphic there. Let $c_{d,q} := \operatorname{Re} G_{d,q}(1)$, and for real $x > 0$ let

$$R_{d,q}(x) := \sum_{1\le n\le x} \lambda(n)\Big(\frac{1}{n} - \frac{1}{x}\Big) - \frac{\log x}{\varphi(q)} - c_{d,q}. \tag{4}$$

The simplest case is $q = 1$, where $\lambda(n) = \Lambda(n)(1 - \chi_d(n))$ for all n and $E_{\mathbf{1}}(s) = (s-1)\zeta(s)$ for $s \ne 1$, with $E_{\mathbf{1}}(1) = 1$.

Problem 1.4.1. $\lambda(n) = \varphi(q)^{-1}\sum_{\psi}\big(\psi(n) - \psi(n)\chi_d(n)\big)\Lambda(n)$, and $0 \le \lambda(n) \le 2\Lambda(n)$. For $q = 1$ and $d = 7$ the nonzero values for $n \le 11$ are $\lambda(3) = 2\log 3$, $\lambda(5) = 2\log 5$ and $\lambda(7) = \log 7$.

Problem 1.4.2. For $\operatorname{Re} s > 1$, $\sum_{n\ge1}\lambda(n)n^{-s} = s/\big(\varphi(q)(s-1)\big) + G_{d,q}(s)$.

Problem 1.4.3. For $\operatorname{Re} s > 1$, $\int_1^\infty R_{d,q}(y)\,y^{-s}\,dy = \big(G_{d,q}(s)/s - c_{d,q}\big)/(s-1)$.

Problem 1.4.4. (i) The function $\Phi(s) := \big(G_{d,q}(s)/s - c_{d,q}\big)/(s-1)$ is meromorphic on $\mathbb{C}$ and regular at $s = 1$. At every $\rho \ne 0, 1$ it has at most a simple pole, with residue

$$\frac{1}{\varphi(q)\,\rho(1-\rho)}\sum_{\psi}\big(m_\psi(\rho) - m_{\psi\chi_d}(\rho)\big).$$

(ii) If no $L(s, \psi\chi_d)$ vanishes at a real $x \in (0, 1)$, the residue at x is ≥ 0, and it is > 0 if some $L(s, \psi)$ vanishes there. A zero of order m of one $L(s, \psi\chi_d)$ at a point $\rho \ne 0, 1$ where no other E vanishes gives the residue $-m/\big(\varphi(q)\rho(1-\rho)\big)$.

At $\rho \ne 0, 1$ the residue depends on the difference between the total untwisted and twisted orders. A common zero can therefore reduce or cancel the contribution of an untwisted factor, and at a real point $0 < \rho < 1$ a twisted zero alone gives a negative residue. Neither happens where no twist vanishes.

Problem 1.4.5. $c_{d,1} = -1 - \gamma + \frac{L'}{L}(1, \chi_d)$. For $d = 7$, $L(1, \chi_7) = \pi/\sqrt{7} = 1.1874104\ldots$; with $\frac{L'}{L}(1, \chi_7) \approx 0.0156357$ this gives $c_{7,1} \approx -1.56158$.

Problem 1.4.6. For $y \ge 1$, $yR_{d,1}(y) = G(y) - G_{\chi_d}(y)$, with G as in (1) and G_{χ_d} as in (3).

For instance $R_{7,1}(y) \approx 6.27 \cdot 10^{-4}$, $1.05 \cdot 10^{-4}$ and $-7.71 \cdot 10^{-5}$ at $y = 10^4$, 10^5 and 10^6.

Problem 1.4.7. (i) $\sum_{n\le y}\lambda(n)(1/n - 1/y) - \log y/\varphi(q)$ has a limit as $y \to \infty$. (ii) The limit is $c_{d,q}$; that is, $R_{d,q}(y) \to 0$.

So $c_{d,q}$ is the constant that makes the remainder small. The proof gives more: for every odd prime d, every $q \ge 1$ prime to d and every integer $B \ge 0$, $|R_{d,q}(y)| \le (\log y)^{-B}$ for all large real y. It does this by a Tauberian theorem applied to $v \mapsto R_{d,q}(e^v)$ and the transform identity of Problem 1.4.3 for $\operatorname{Re} s > 2$.

Now fix a point ρ. The next problem is the analogue of Theorem 1.2.1 for the $L(s, \psi)$, at one prime d whose twists do not vanish near the real axis up to the height of ρ.

Problem 1.4.8. Let $d \equiv 7 \pmod 8$ be prime, $q \ge 1$ prime to d, $\beta > 0$, and $\rho \ne 1$ with $\operatorname{Re}\rho > \beta$. Suppose that $L(s, \psi\chi_d) \ne 0$ for every ψ modulo q and every s with $\operatorname{Re} s \ge \beta$ and $|\operatorname{Im} s| \le |\operatorname{Im}\rho|$, and that $R_{d,q}(y) \le y^{\beta-1}$ for all large real y. Then $L(\rho, \psi) \ne 0$ for every ψ modulo q.

Problem 1.4.8 assumes no separate exclusion of real zeros of the untwisted L-functions. For $\beta > 1/2$, Theorem 2.2.2 of Chapter 2 supplies the required twist nonvanishing for some prime d in any residue class satisfying its hypotheses. For a Dirichlet character ξ modulo N and an odd prime d not dividing N, write $\xi\chi_d$ for their product, a character modulo Nd. That theorem says: let $N \ge 1$, $\beta > 1/2$ and $t_0 \in \mathbb{R}$, and let a be a unit modulo N such that every prime $p \equiv a \pmod N$

satisfies $p \equiv 7 \pmod 8$ and $\gcd(N,p) = 1$; then there is a prime $d \equiv a \pmod N$ such that $L(s, \xi\chi_d) \neq 0$ for every character ξ modulo N and every s with $\operatorname{Re} s \geq \beta$ and $|\operatorname{Im} s| \leq t_0$. It says nothing about $R_{d,q}$.

Let q_0 be a positive multiple of 8, and let $d_0 \equiv 7 \pmod 8$ be prime to q_0. Every prime $d \equiv d_0 \pmod{q_0}$ is then $\equiv 7 \pmod 8$ and prime to q_0. The next theorem assumes the bound for R_{d,q_0} for every prime d in this class. Given ρ, Theorem 2.2.2 with $N = q_0$, $a = d_0$ and $t_0 = |\operatorname{Im}\rho|$ chooses d in the class, and Problem 1.4.8 applies to it.

Theorem 1.4.1. *Let $q_0 \geq 1$ with $8 \mid q_0$, let $d_0 \geq 0$ be an integer with $d_0 \equiv 7 \pmod 8$ and $\gcd(d_0, q_0) = 1$, and let $\beta > 1/2$. Suppose that for every prime $d \equiv d_0 \pmod{q_0}$ there is $Y \in \mathbb{R}$ such that $R_{d,q_0}(x) \leq x^{\beta-1}$ for every real $x \geq Y$. Then $L(\rho, \psi) \neq 0$ for every character ψ modulo q_0 and every $\rho \neq 1$ with $\operatorname{Re}\rho > \beta$.*

The hypothesis concerns every prime of one class modulo q_0, and the point Y from which the bound holds may depend on d. For $q = 1$, by Problem 1.4.6, a bound $R_{d,1}(x) \leq x^{\theta-1}$ reads $G(x) - G_{\chi_d}(x) \leq x^{\theta}$; compare Theorem 1.2.1.

Problem 1.4.9. Let $M \geq 1$. If for every $\beta > 1/2$ the hypothesis of Theorem 1.4.1 holds for $q_0 = 8M$ and $d_0 = 8M - 1$, then $L(s, \chi) \neq 0$ for every character χ modulo M and every $s \neq 1$ with $\operatorname{Re} s > 1/2$.

In the Lean formalization. In the Lean proof [GL] (readable edition), Theorem 1.4.1 is `New.LFunction_ne_zero_of_primeRemainder_le` in `New/Reduction/Zeros/Criterion.lean`; for $x > 0$, $R_{d,q}(x)$ is `New.primeRemainder` at d, q, x in `New/Reduction/Zeros/PrimeError.lean`. Theorem 1.2.2 is `New.IsPolar.landau` in `Lib/Analytic/Landau.lean`, with the definition `New.IsPolar` written out. The bound $|R_{d,q}(y)| \leq (\log y)^{-B}$ is `New.eventually_abs_primeRemainder_le` in `New/Reduction/Zeros/PrimeNumberTheorem.lean`.

Hints

§1.1.

1.1.2: Integrate each step of ψ. For the bound use Chebyshev's estimate.

1.1.3: Use Problem 1.1.1 termwise, and compute the transforms of $x \log x$ and x.

1.1.4: Use $-\zeta'/\zeta(s) = 1/(s-1) - \gamma + O(s-1)$ and expand $1/(s(s-1))$ at $s = 1$.

1.1.5: The functional equation gives $\zeta'/\zeta(0) = \log 2\pi$.

1.1.6: Write $1/(\rho(1-\rho)) = 1/\rho + 1/(1-\rho)$ and use the value of B in [Dav, Ch. 12].

§1.2.

1.2.1: Split the integral at X_0.

1.2.2: Use Problem 1.1.2 for $\sigma_c \leq 1$ and Problem 1.1.3 for the formula for H. For $\sigma_c > -\infty$ use Problem 1.1.4: ζ has infinitely many zeros in the critical strip [Dav, Ch. 12], so it has nonreal ones.

1.2.3: Consider $(1 - 2^{1-\sigma})\zeta(\sigma) = \sum_{n\geq 1}(-1)^{n-1}n^{-\sigma}$.

1.2.4: By Landau's theorem σ_c is a singularity of H. Of the real points in $(\theta, 1]$, only real zeros of ζ can be singular (Problem 1.1.4). Find the sign of the residue of F at a real zero $\beta \in (0,1)$, and compare with Problem 1.2.1.

1.2.5: Use Theorem 1.2.1 and the symmetry $\rho \mapsto 1-\rho$.

§1.3.

1.3.1: Substitute $x = n/t$ in each term.

1.3.3: Repeat §1.2 with $\tilde{\phi}(s) = 1/(s(s+1))$, including the argument for $\sigma_c > -\infty$ in Problem 1.2.2, and compare the sign of the residue at a real zero with that in Problem 1.2.4; conclude with Problem 1.2.3.

§1.4.

1.4.1: Orthogonality of the characters modulo q; a number $n \equiv 1 \pmod q$ is prime to q.

1.4.2: Problem 1.4.1 and $-\frac{L'}{L}(s,\chi) = \sum_n \chi(n)\Lambda(n)n^{-s}$; for the principal ψ, E'_ψ/E_ψ and L'/L differ by $1/(s-1)$.

1.4.3: As Problem 1.1.3: $(1/n - 1/y)_+ y^{-s} = (y/n - 1)_+ y^{-s-1}$, so Problem 1.1.1 applies; then Problem 1.4.2.

1.4.4: (i) A zero of order m of an entire function at ρ is a simple pole of its logarithmic derivative, with residue m. At $s = 1$: the characters modulo q are closed under complex conjugation, so $G_{d,q}(1)$ is real.

1.4.5: For $q = 1$ the untwisted factor is $(s-1)\zeta(s) = 1 + \gamma(s-1) + \cdots$. For $d = 7$ use the class number formula.

1.4.6: Problem 1.4.5; for $n \le y$ the ramp is $y(1/n - 1/y)$.

1.4.7: (i) Partial summation, as in Problem 1.1.2, with the prime number theorem with error term for the characters modulo qd [Dav, Ch. 20]. (ii) If $R_{d,q} \to \ell$, compare the behaviour of the two sides of Problem 1.4.3 as $s \downarrow 1$, using Problem 1.4.4.

1.4.8: Theorem 1.2.2 for $E(v) := R_{d,q}(e^v)$, with Problems 1.4.3 and 1.4.4. Check the sign of the residue at real x in $(\beta, 1)$, at 1 and in $(1, \infty)$ separately.

1.4.9: A character modulo M induces one modulo $8M$; the two L-functions differ by finitely many Euler factors.

References

[Dav] H. Davenport, *Multiplicative Number Theory*, 3rd ed., revised by H. L. Montgomery, Grad. Texts in Math. **74**, Springer, 2000.

[GL] L. Sernau, *GRH for Dirichlet L-functions, in Lean 4*, a shorter rewriting of the Lean proof, text by Claude, `https://github.com/lsernau/grh-lean`, commit `72fead1`, readable edition `grh/`.

[Lan] E. Landau, *Über einen Satz von Tschebyschef*, Math. Ann. **61** (1905), 527–550.

[MV] H. L. Montgomery and R. C. Vaughan, *Multiplicative Number Theory I. Classical Theory*, Cambridge Stud. Adv. Math. **97**, Cambridge University Press, 2007.

INERT PRIMES AND THE CHOICE OF d

Prerequisites. Chapter 1, *From zeros to a one-sided bound*, Sections 1.1, 1.2 and 1.4: the functions G and G_χ of its equations (1) and (3), the transform F of (2), Landau's theorem and the argument of Problem 1.2.4. Quadratic reciprocity with its supplements [SeA, Ch. I, §3], the Jacobi symbol and its reciprocity law [IR, Ch. 5], and the splitting of primes in an imaginary quadratic field [Ne, Ch. I, §8]. From Davenport [Dav]: Dirichlet's theorem in the form that $\sum \log p/p$ over the primes of an invertible class diverges (Ch. 4), primitive characters (Ch. 5), the theta functions of a primitive character and their transformation formula (Ch. 9), and the Pólya–Vinogradov inequality (Ch. 23). The three-lines theorem [Ru, Ch. 12].

The criterion of Theorem 1.4.1 assumes a one-sided bound for a remainder of a sum with coefficients $\Lambda(n)(1-\chi_d(n))$ over the $n \equiv 1 \pmod{q_0}$. We first study the unrestricted sum with these coefficients, which are supported on odd powers of primes inert in an imaginary quadratic field and on powers of the ramified prime. How does its centered value compare with G, and what information does it give about the zeros of ζ?

2.1. Inert primes and a quadratic character

Let $d \equiv 3 \pmod 4$ be a prime, let $K := \mathbb{Q}(\sqrt{-d})$, and let $\chi_d(n) := \left(\frac{n}{d}\right)$ be the Legendre symbol.

Problem 2.1.1. (i) For every prime p, $\chi_d(p)$ is 1, -1 or 0 according as p splits, is inert, or ramifies in K. (ii) For a prime power $r = p^h$, $1-\chi_d(r)$ is 2 if p is inert and h is odd, 1 if $p = d$, and 0 otherwise.

The ramp sum over odd powers of inert primes, with weight 2, and over powers of d, with weight 1, is therefore

$$S_d(x) := \sum_r \Lambda(r)\big(1-\chi_d(r)\big)\Big(\frac{x}{r}-1\Big)_+.$$

For a primitive nonprincipal character χ let $\Psi_\chi(t) := \sum_{n\le t}\Lambda(n)\chi(n)$, and let c_χ and G_χ be as in (3).

Problem 2.1.2. $G_\chi(x) = -\sum_n \Lambda(n)\chi(n)\min(1, x/n) = -x\int_x^\infty \Psi_\chi(t)\,t^{-2}\,dt$.

Problem 2.1.3. $S_d(x) - x\log x + (1+\gamma-c_{\chi_d})x = G(x) - G_{\chi_d}(x)$.

An upper bound for S_d minus its main term is thus an upper bound for $G - G_{\chi_d}$, not for G. How much does such a bound say about the zeros of ζ?

Problem 2.1.4. Let $0 < \theta < 1$. Suppose that $L(s,\chi_d)$ has no real zero in $(\theta, 1)$, and that $G(x) - G_{\chi_d}(x) \le x^\theta$ for all large x. Then every zero of $\zeta(s)$ or of $L(s,\chi_d)$ in $\operatorname{Re} s > \theta$ is a zero of both, with the same multiplicity.

Date: November 26, 2026.

Problem 2.1.4 leaves the possibility of a shared zero of equal multiplicity. We next consider a region free of zeros of $L(s,\chi_d)$. For $\beta, t_0 \in \mathbb{R}$ let

$$\mathcal{B}(\beta,t_0) := \{s \in \mathbb{C} : \operatorname{Re} s \geq \beta,\ |\operatorname{Im} s| \leq t_0\},$$

which is empty for $t_0 < 0$ and unbounded to the right otherwise.

Problem 2.1.5. Let $0 < \theta < \beta$ and $t_0 \geq 0$. Suppose that $L(s,\chi_d) \neq 0$ on $\mathcal{B}(\beta,t_0)$, and that $G(x) - G_{\chi_d}(x) \leq x^\theta$ for all large x. Then ζ has no zero in $\mathcal{B}(\beta,t_0)$.

Fix $\theta > 0$. If the bound $G - G_{\chi_d} \leq x^\theta$ holds for every prime d of some class, and every box $\mathcal{B}(\beta,t_0)$ with $\beta > \theta$ is free of zeros of $L(s,\chi_d)$ for at least one d of the class, then ζ has no zero in $\operatorname{Re} s > \theta$. The choice of d depends on the box. Section 2.2 shows that such a d exists in the class $d \equiv 7 \pmod 8$ when $\theta \geq \frac{1}{2}$. This class is used for the following reason.

Problem 2.1.6. Let $d \equiv 7 \pmod 8$. Then $\chi_d(2) = 1$ and $\chi_d(-1) = -1$. Hence 2 splits in K, $1 - \chi_d(r)$ vanishes at every power of 2, and χ_d is an odd character.

In the proof the weight is restricted further, to prime powers $n \equiv 1 \pmod{q_0}$, and the characters that occur are all ψ modulo q_0 and their twists $\psi\chi_d$. Its criterion, Theorem 1.4.1, takes q_0 a positive multiple of 8, a nonnegative integer $d_0 \equiv 7 \pmod 8$ prime to q_0, and $\beta > \frac{1}{2}$, and assumes, for every prime $d \equiv d_0 \pmod{q_0}$, that the remainder $R_{d,q_0}(x)$ of (4) is at most $x^{\beta-1}$ for all sufficiently large x. Given $\rho \neq 1$ with $\operatorname{Re}\rho > \beta$, its proof uses one such d, given by Theorem 2.2.2 below at the same β, with $N = q_0$, $a = d_0$ and $t_0 = |\operatorname{Im}\rho|$.

2.2. The choice of d

Is there a prime $d \equiv 7 \pmod 8$ for which $L(s,\chi_d)$ has no zero in a given box $\mathcal{B}(\beta,t_0)$ with $\beta > \frac{1}{2}$? Problem 2.2.13 bounds the number of exceptional primes $d \equiv 7 \pmod 8$ up to X. The quantity that detects a zero is built from theta series.

For $j \in \{0,1\}$ let $w_j(z) := z^j e^{-\pi z^2}$ for $z \in \mathbb{R}$, and let

$$\Gamma_j(s) := \int_0^\infty w_j(z)\, z^s\, \frac{dz}{z} \qquad (\operatorname{Re} s > 0).$$

For a sequence $c\colon \mathbb{Z}_{\geq 1} \to \mathbb{C}$ with $|c(n)| \leq 1$ let

$$\Theta_c(u) := u^{1/2} \sum_{n\geq 1} c(n)\, w_j(nu) \qquad (u > 0),$$

and write $c\mu$ for the sequence $n \mapsto c(n)\mu(n)$, with μ the Möbius function. The index j is fixed in each argument and is dropped from Θ_c. A Dirichlet character χ modulo q is a sequence of this kind, and has *parity* j if $\chi(-1) = (-1)^j$.

Problem 2.2.1. $\Gamma_j(s) = \frac{1}{2}\pi^{-(s+j)/2}\,\Gamma\big(\frac{s+j}{2}\big)$ for $\operatorname{Re} s > 0$. In particular $\Gamma_1(1) = 1/(2\pi)$.

Problem 2.2.2. (i) Let χ be a nonprincipal character modulo q of parity j. For $\operatorname{Re} s > 0$ the integral $\int_0^\infty \Theta_\chi(u)\, u^{s-1/2}\, du/u$ converges absolutely and equals $\Gamma_j(s)L(s,\chi)$. For $\chi = \chi_7$, $j = 1$ and $s = 1$ its value is $1/(2\sqrt{7}) = 0.18898\ldots$ (ii) For every character χ and $\operatorname{Re} s > 1$, $\int_0^\infty \Theta_{\chi\mu}(u)\, u^{s-1/2}\, du/u = \Gamma_j(s)/L(s,\chi)$.

Problem 2.2.3. Let χ be a primitive nonprincipal character modulo q of parity j. Then $|\Theta_\chi(1/(qu))| = |\Theta_\chi(u)|$ for $u > 0$. Hence the integrals of $|\Theta_\chi(u)|\, du/u$ over $u < q^{-1/2}$ and over $u > q^{-1/2}$ are equal.

For $T>0$ define the *tail integral* of a sequence c and the *mollifier* of a character χ:

$$J(c,T):=\int_{1/T}^{\infty}\bigl(|\Theta_c(u)|+|\Theta_{c\mu}(u)|\bigr)\,\frac{du}{u},\qquad \mathcal{M}_T(s):=\int_{1/T}^{\infty}\Theta_{\chi\mu}(u)\,u^{s-1/2}\,\frac{du}{u}.$$

By Problem 2.2.2(ii), for $\operatorname{Re}s>1$, $\mathcal{M}_T(s)$ is the integral for $\Gamma_j(s)/L(s,\chi)$ cut at $u=1/T$. For $\operatorname{Re}z>0$ where $L(z,\chi)$ is finite, let $\Phi(z):=\Gamma_j(z)L(z,\chi)\mathcal{M}_T(z)-\Gamma_j(z)^2$.

Problem 2.2.4. (i) $\sum_{n\ge1}|w_j(nu)|\le 3e^{-u}/u$ for $u>0$. (ii) For every character χ, every $T>0$ and $\operatorname{Re}z=2$: $|\Gamma_j(z)/L(z,\chi)-\mathcal{M}_T(z)|\le 3/T$ and $|\Gamma_j(z)L(z,\chi)|\le 3$, so $|\Phi(z)|\le 9/T$.

Problem 2.2.5. Let χ be a primitive nonprincipal character modulo q of parity j, and $T>0$ with $q\le T^2$. On $\operatorname{Re}z=\frac12$: $|\Gamma_j(z)L(z,\chi)|\le 2J(\chi,T)$ and $|\mathcal{M}_T(z)|\le J(\chi,T)$.

Problem 2.2.6. There is a constant C_j with the following property. Let $\delta>0$ and $T>0$, and let χ be a primitive nonprincipal character modulo q of parity j, with $q\le T^2$ and $J(\chi,T)\le T^{2\delta}$. If $L(s,\chi)=0$ and $\frac12+9\delta\le\operatorname{Re}s\le 1$, then $|\Gamma_j(s)|^2\le C_jT^{-2\delta}$.

Problem 2.2.7. Let $\delta>0$ and $t_0\in\mathbb{R}$. For all T large in terms of δ and t_0 the following holds for every q and every primitive nonprincipal character χ modulo q of parity j with $q\le T^2$: if $L(s,\chi)$ vanishes somewhere on $\mathcal{B}(\frac12+9\delta,t_0)$, then $J(\chi,T)>T^{2\delta}$.

A zero in the box therefore forces a large tail integral. It remains to show that the tail integrals of the characters χ_d are small on average over d. Write $n^\circ:=n/2^{v_2(n)}$ for the odd part of $n\ge1$, and $\left(\frac{b}{m}\right)$ for the Jacobi symbol, $m\ge1$ odd.

Problem 2.2.8. Let $d\equiv 7 \pmod 8$ be prime. For every $n\ge1$, $\left(\frac{n}{d}\right)=\left(\frac{-d}{n^\circ}\right)$. For instance $\left(\frac{12}{7}\right)=\left(\frac{-7}{3}\right)=-1$.

For a sequence α with $|\alpha(n)|\le1$ and $v\ge1$ let $c_v(n):=\alpha(n)\left(\frac{-v}{n^\circ}\right)$. The mean over $1\le v\le T^2$ below runs over all integers v. The Pólya–Vinogradov inequality [Dav, Ch. 23] states that $|\sum_{v\le X}\omega(v)|\le C\sqrt{m}\log m$ for every nonprincipal character ω modulo $m\ge2$ and every X, with C absolute.

Problem 2.2.9. Let $\delta>0$ and $n\ge1$, and suppose that n° is not a square. Then $v\mapsto\left(\frac{-v}{n^\circ}\right)$ is ±1 times a nonprincipal character modulo n°, and $\left|\sum_{1\le v\le X}\left(\frac{-v}{n^\circ}\right)\right|\le C_\delta\,n^{1/2+\delta/2}$ for every X, with C_δ depending only on δ.

Problem 2.2.10. Let $\delta>0$. For $u>0$, $\sum|w_j(nu)\,w_j(n'u)|\le C_\delta\,u^{-1-2\delta}$, the sum over the pairs $n,n'\ge1$ with $(nn')^\circ$ a square.

Problem 2.2.11. Let $\delta>0$, $T>0$ and $u\ge1/T$. Then $\sum_{1\le v\le T^2}|\Theta_{c_v}(u)|^2\le C_\delta\,T^2u^{-2\delta}$, with C_δ depending only on δ and j, not on α, T or u.

Problem 2.2.12. Let $\delta>0$. For $T>0$ and every α with $|\alpha(n)|\le1$, $\sum_{1\le v\le T^2}J(c_v,T)\le C_\delta\,T^{2+\delta}$, with C_δ depending only on δ and j.

We return to the primes. For a prime $d\equiv7 \pmod 8$, χ_d is nonprincipal modulo the prime d, hence primitive, and Problem 2.1.6 gives its odd parity.

Problem 2.2.13. Let $\delta > 0$ and $t_0 \geq 0$. For all large X, at most $CX^{1-\delta/2}$ primes $d \leq X$ with $d \equiv 7 \pmod 8$ have a zero of $L(s, \chi_d)$ on $\mathcal{B}(\frac{1}{2} + 9\delta, t_0)$; here C depends on δ and t_0.

Problem 2.2.14. For every $\beta > \frac{1}{2}$ and $t_0 \geq 0$ there are infinitely many primes $d \equiv 7 \pmod 8$ with $L(s, \chi_d) \neq 0$ on $\mathcal{B}(\beta, t_0)$.

Problem 2.2.13 gives a power saving of $X^{-\delta/2}$ relative to the trivial bound X. Density estimates for quadratic twists far stronger than Problem 2.2.13 are known; they rest on mean values of real character sums [Ju], [HB].

Now let ξ run over the characters modulo $N = q_0$, as at the end of Section 2.1. Here $\xi\chi_d$ denotes the character $n \mapsto \xi(n)\left(\frac{n}{d}\right)$ modulo Nd; for an odd prime $d \nmid N$ it is not principal, so $L(s, \xi\chi_d)$ is entire. The smallest case is $N = 8$ and the class $a = 7$.

Problem 2.2.15. Let $d \equiv 7 \pmod 8$ be prime, ξ a character modulo 8, and ξ^* the primitive character inducing ξ, of conductor $f \in \{1, 4, 8\}$. Then $\xi^*\chi_d$ is primitive modulo fd; $L(s, \xi\chi_d) = (1-2^{-s})L(s, \chi_d)$ if ξ is principal, and $L(s, \xi\chi_d) = L(s, \xi^*\chi_d)$ otherwise. Hence for $\beta > 0$ the four twists have no zero on $\mathcal{B}(\beta, t_0)$ exactly when the four $L(s, \xi^*\chi_d)$ have none.

For $d = 7$, each of the four $L(s, \xi\chi_7)$ has positive real part on $3/4 \leq \operatorname{Re} s \leq 1$, $|\operatorname{Im} s| \leq 1/10$, and has no zero in $\mathcal{B}(3/4, 1/10)$; this is a finite computation.

For general N, a character ξ modulo N is induced by a primitive character ξ^* of conductor $M \mid N$. For a prime $d \equiv 7 \pmod 8$ with $d \nmid N$, the twist $\xi^*\chi_d$ is primitive modulo Md and has parity opposite to that of ξ^*. The functions $L(s, \xi\chi_d)$ and $L(s, \xi^*\chi_d)$ have the same zeros in $\operatorname{Re} s > 0$, since the Euler factors removed on passing to level Nd are nonzero there. The following theorems give the exceptional count and the simultaneous choice of d.

Theorem 2.2.1. *Let $N \geq 1$, $\delta > 0$ and $t_0 \in \mathbb{R}$, and let $a \in \mathbb{Z}/N\mathbb{Z}$ be a class such that every prime $p \equiv a \pmod N$ satisfies $p \equiv 7 \pmod 8$ and $\gcd(N, p) = 1$. Call a prime $d \equiv a \pmod N$* bad *if for some character ξ modulo N the function $L(s, \xi\chi_d)$ vanishes at some s with $\operatorname{Re} s \geq \frac{1}{2} + 9\delta$ and $|\operatorname{Im} s| \leq t_0$. Then the number of bad primes $d \leq X$ is $O(X^{1-\delta/2})$ as $X \to \infty$ through the positive integers.*

Theorem 2.2.2. *Let $N \geq 1$, $\beta > \frac{1}{2}$ and $t_0 \in \mathbb{R}$, and let a be a unit of $\mathbb{Z}/N\mathbb{Z}$ such that every prime $p \equiv a \pmod N$ satisfies $p \equiv 7 \pmod 8$ and $\gcd(N, p) = 1$. Then there is a prime $d \equiv a \pmod N$ such that for every character ξ modulo N and every $s \in \mathbb{C}$ with $\operatorname{Re} s \geq \beta$ and $|\operatorname{Im} s| \leq t_0$, $L(s, \xi\chi_d) \neq 0$.*

The hypothesis on the class holds when $8 \mid N$ and $a \equiv 7 \pmod 8$ is a unit; for $1 \leq N < 8$ it holds for no unit class. One d serves all characters ξ and all points of the box at once, and the characters ξ and the class a have the same modulus N.

In the Lean formalization. In the readable edition of the Lean proof [GL], the file `grh/src/Lib/Analytic/QuadraticTwist.lean` contains `New.zero_density_quadTwist` (Theorem 2.2.1) and `New.exists_entireL_quadTwist_ne_zero` (Theorem 2.2.2). The latter states its conclusion for `New.entireL`; the chosen d is odd and prime to N, so `New.quadTwist_ne_one` and the definition of `New.entireL` identify this function with $L(\,\cdot\,, \xi\chi_d)$.

Hints

§2.1.

2.1.1: For odd $p \neq d$ compare $\left(\frac{-d}{p}\right)$ with $\left(\frac{p}{d}\right)$ by reciprocity. For $p = 2$ use $\mathcal{O}_K = \mathbb{Z}[(1+\sqrt{-d})/2]$.

2.1.2: Use $\sum_n \Lambda(n)\chi(n)/n = -c_\chi$, convergent by the prime number theorem for χ.

2.1.3: Write S_d as the ramp sum with coefficient 1 minus the one with coefficient χ_d, and use (1) and (3).

2.1.4: The Mellin transform of $G - G_{\chi_d}$ is $F(s) + \frac{L'}{L}(s,\chi_d)/(s(s-1)) - c_{\chi_d}/(s-1)$, with F as in (2). Follow Problem 1.2.4: a real zero of ζ gives the residue sign of that problem, but a real zero of $L(s,\chi_d)$ gives the opposite sign.

2.1.5: As in Problem 2.1.4, with $A(x) := x^\theta - G(x) + G_{\chi_d}(x)$. Show that the abscissa σ_c is less than β: a real singularity $\sigma_c \geq \beta$ would be a real zero of ζ that is not a zero of $L(s,\chi_d)$.

2.1.6: The supplementary laws.

§2.2.

2.2.2: Integrate term by term where the sum converges absolutely. For (i) with $0 < \operatorname{Re} s \leq 1$, bound $\sum_n \chi(n) w_j(nu)$ for small u by partial summation, using that the partial sums of χ are bounded. For the value, $L(1,\chi_7) = \pi/\sqrt{7}$ by the class number formula.

2.2.3: The transformation formula for the theta function of a primitive character [Dav, Ch. 9]; then substitute $u \mapsto 1/(qu)$.

2.2.4: (i) Compare the sum with an integral; w_j is unimodal on $(0,\infty)$. (ii) The difference is the integral over $0 < u \leq 1/T$; use (i) on both integrals.

2.2.5: On $\operatorname{Re} z = \frac{1}{2}$ the factor $u^{z-1/2}$ has modulus 1. Use Problem 2.2.3 and $q^{-1/2} \geq 1/T$.

2.2.6: Evaluate Φ at the given zero s. Apply the three-lines theorem to Φ on $\frac{1}{2} \leq \operatorname{Re} z \leq 2$, with Problems 2.2.4 and 2.2.5 on the two edges. The weight of the right edge at $\operatorname{Re} s$ is $(\operatorname{Re} s - \frac{1}{2})/\frac{3}{2} \geq 6\delta$.

2.2.7: For $t_0 < 0$ the box is empty. For $t_0 \geq 0$, use $L(s,\chi) \neq 0$ for $\operatorname{Re} s \geq 1$ and the positive minimum of $|\Gamma_j|$ on the compact rectangle $\frac{1}{2} \leq \operatorname{Re} s \leq 1$, $|\operatorname{Im} s| \leq t_0$.

2.2.8: Factor $n = 2^k n^\circ$, use $\left(\frac{2}{d}\right) = 1$, and apply reciprocity for the Jacobi symbol with $d \equiv 3 \pmod 4$.

2.2.9: $\left(\frac{-v}{m}\right) = \left(\frac{-1}{m}\right)\left(\frac{v}{m}\right)$. For nontriviality choose v by the Chinese remainder theorem at a prime dividing m to an odd power.

2.2.10: Write $n = 2^a g k^2$ and $n' = 2^b g k'^2$ with g odd and squarefree; the terms with n or n' much larger than $1/u$ are negligible.

2.2.11: Expand the square, so that the inner sum over v is $\sum_v \left(\frac{-v}{(nn')^\circ}\right)$. Bound it by T^2 for the pairs of Problem 2.2.10 and by Problem 2.2.9 for the others, and use $u^{-2} \leq T^2$.

2.2.12: Cauchy–Schwarz over v, Problem 2.2.11 for α and for $\alpha\mu$, then integrate over $u > 1/T$.

2.2.13: Use Problem 2.2.8 with $\alpha = 1$. Take $T = \sqrt{X}$, and compare Problems 2.2.7 and 2.2.12.

2.2.14: Reduce to $\beta < 1$ and put $\delta := (\beta - \frac{1}{2})/9$. If all large primes of the class were bad, partial summation and Problem 2.2.13 would make $\sum \log p/p$ over the class converge.

2.2.15: $\chi_d(2) = 1$. The characters ξ^* and χ_d have coprime conductors, and $\xi^*\chi_d(n) = 0$ for even n when $f > 1$.

References

[Dav] H. Davenport, *Multiplicative Number Theory*, 3rd ed., revised by H. L. Montgomery, Grad. Texts in Math. **74**, Springer, 2000.

[GL] L. Sernau, *GRH for Dirichlet L-functions, in Lean 4*, a shorter rewriting of the Lean proof, text by Claude, `https://github.com/lsernau/grh-lean`, commit `72fead1`, readable edition `grh/`.

[HB] D. R. Heath-Brown, *A mean value estimate for real character sums*, Acta Arith. **72** (1995), 235–275.

[IR] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, 2nd ed., Grad. Texts in Math. **84**, Springer, 1990.

[Ju] M. Jutila, *On mean values of Dirichlet polynomials with real characters*, Acta Arith. **27** (1975), 191–198.

[Ne] J. Neukirch, *Algebraic Number Theory*, Grundlehren Math. Wiss. **322**, Springer, 1999.

[Ru] W. Rudin, *Real and Complex Analysis*, 3rd ed., McGraw–Hill, 1987.

[SeA] J.-P. Serre, *A Course in Arithmetic*, Grad. Texts in Math. **7**, Springer, 1973.

THE PLACES, THE WEIGHTS AND THE REMAINDER

Prerequisites. From Chapter 1, *From zeros to a one-sided bound*: the weight λ, the constant $c_{d,q}$ and the remainder $R_{d,q}$ of equation (4), recalled below, and Problem 1.4.7. From Chapter 2, *Inert primes and the choice of d*: Section 2.1, on the values of $1-\chi_K$. Cyclotomic fields and their Galois groups [Wa, Ch. 2]; infinite places of a number field as conjugation orbits of embeddings into $\mathbb{C}$ [Ne, Ch. II, §8]; quadratic reciprocity [SeA, Ch. I, §3].

In the proof, the main inequality (Theorem 35.2.1) bounds from above a centered sum over the infinite places of class 1 modulo q_0 in the CM field obtained by adjoining a root of unity to $K=\mathbb{Q}(\sqrt{-d})$. Chapter 1 needs an upper bound for the remainder of a weighted sum over the prime powers $n\equiv 1 \pmod{q_0}$ up to x. How does the sum over places give such a bound? An exact finite-sum identity gives the answer. In the summand indexed by n, the weight at the translated place sets the cutoff. For an admissible datum the centered total over places of class 1 modulo q_0 equals a positive multiple of $R_{q_0}(x)$ plus two terms at x_1 (Theorem 3.2.1).

Throughout, $d\equiv 3 \pmod 4$ is a prime, $K:=\mathbb{Q}(\sqrt{-d})$, and $\chi_K(n):=\left(\frac{n}{d}\right)$ is the Legendre symbol (the χ_d of Chapter 1), so $\chi_K(d)=0$. For an integer $q\geq 1$ prime to d we write, as in Chapter 1,

$$\lambda_q(n):=\begin{cases}\Lambda(n)\big(1-\chi_K(n)\big), & n\equiv 1 \pmod q,\\ 0, & \text{otherwise,}\end{cases}\qquad R_q(z):=\sum_{1\leq n\leq z}\lambda_q(n)\Big(\frac{1}{n}-\frac{1}{z}\Big)-\frac{\log z}{\varphi(q)}-c_q$$

for real $z>0$, where $c_q:=c_{d,q}$ and $R_q:=R_{d,q}$ are the constant and the remainder of equation (4), and λ_q is the weight λ there for the modulus q; we drop d, which is fixed. The value of c_q plays no role in the identities of this chapter. We write $u_+:=\max(u,0)$ for real u.

3.1. The host field and its places

Let $q_0\geq 3$ and let q_1 be a multiple of q_0 such that every prime factor of q_1 divides q_0, and $d\nmid q_1$. Let $E:=K(\zeta)$ with ζ a primitive q_1-th root of unity, regarded as a subfield of $\mathbb{C}$. For $g\in \mathrm{Gal}(E/K)$ let $e(g)\in(\mathbb{Z}/q_1\mathbb{Z})^\times$ be the class with $g(\zeta)=\zeta^{e(g)}$.

Problem 3.1.1. The map $e\colon \mathrm{Gal}(E/K)\to(\mathbb{Z}/q_1\mathbb{Z})^\times$ is an isomorphism, and $[E:\mathbb{Q}]=2\varphi(q_1)$.

Let Φ be the set of infinite places of E and $f:=|\Phi|$. For $g\in\mathrm{Gal}(E/K)$ let $\langle g\rangle\in\Phi$ be the place of the embedding $g\colon E\to\mathbb{C}$.

Problem 3.1.2. Every infinite place of E is complex, and $g\mapsto\langle g\rangle$ is a bijection $\mathrm{Gal}(E/K)\to\Phi$. Hence $f=\varphi(q_1)$.

We make Φ a group through $g\mapsto\langle g\rangle$, and identify it with $(\mathbb{Z}/q_1\mathbb{Z})^\times$ through e: the place $\sigma\in\Phi$ has *label* $v\in(\mathbb{Z}/q_1\mathbb{Z})^\times$ if $\sigma=\langle g\rangle$ with $e(g)=v$. The place with label 1 is the identity. For $\nu\in\mathbb{Z}$ let $[\nu]\in\Phi$ be the place with label $\nu \bmod q_1$

Date: November 26, 2026.

if $\gcd(\nu, q_1) = 1$, and the identity place otherwise. Let $\mathrm{cl}\colon \Phi \to (\mathbb{Z}/q_0\mathbb{Z})^\times$ be the label reduced modulo q_0, and let

$$\Phi_a := \mathrm{cl}^{-1}(1),$$

the *a-places*. Fix a set $\Phi_b \subseteq \mathrm{cl}^{-1}(-1)$ of *b-places*. We write $\#$ for the number of elements.

Problem 3.1.3. $\#\Phi_a = q_1/q_0$ and $f = \#\Phi_a\, \varphi(q_0)$.

The place attached to an integer $n \geq 1$ and an a-place τ is $[-n]\tau$: for n prime to q_1, its label is $-n$ times the label of τ.

Problem 3.1.4. For $\tau \in \Phi_a$ and every integer $n \geq 1$, $\mathrm{cl}\big([-n]\tau\big) = -1$ if and only if $n \equiv 1 \pmod{q_0}$.

Problem 3.1.5. For every integer $n \geq 1$, the number of $\tau \in \Phi_a$ with $[-n]\tau \in \Phi_b$ is $\#\Phi_b$ if $n \equiv 1 \pmod{q_0}$, and 0 otherwise.

When $\gcd(n, q_1) > 1$, our convention gives $[-n]\tau = \tau$. Under the hypotheses of the next problem such n have coefficient $\lambda_1(n) = 0$ in the prime sums below, so the convention does not affect them.

Problem 3.1.6. (i) If $16 \mid q_0$, $q_0 \mid 2(d+1)$ and $q_0 \nmid d+1$, then $d \equiv 7 \pmod 8$ and $\chi_K(p) = 1$ for every prime $p \mid q_0$. (ii) In that case $\lambda_1(n) = 0$ for every $n \geq 1$ with $\gcd(n, q_1) > 1$.

The *toy example* is $q_0 = 4$, $q_1 = 16$, $d = 7$, so that $f = 8$, Φ_a consists of the places with labels $1, 5, 9, 13$, and Φ_b consists of the place with label 15, so $\#\Phi_a = 4$ and $\#\Phi_b = 1$. It does not satisfy the hypotheses of Problem 3.1.6(i), but $\chi_K(2) = (2/7) = 1$, and the conclusion of Problem 3.1.6(ii) holds.

Problem 3.1.7. In the toy example, the primes $p \leq 61$ with $\lambda_1(p) \neq 0$ are 7 and the primes inert in K, and the label of $[-p]$ is as follows.

label	1	3	5	7	9	11	13	15
p	31, 47	13, 61	59	41	7	5	3, 19	17

The other $n \leq 61$ with $\lambda_1(n) \neq 0$ are 27 and 49, with $\lambda_1(27) = 2\log 3$ and $\lambda_1(49) = \log 7$.

3.2. Two weights and the prime sum

Let $x < x_1$ and b be positive integers with $x_1 \mid b$, and let $a := xb$. The *weight* of a place is

$$\kappa(\sigma) := \begin{cases} a/x = b, & \sigma \in \Phi_b, \\ a/x_1, & \sigma \notin \Phi_b, \end{cases}$$

an integer; the b-places carry the larger weight. The *prime sum* at a place σ is, for real y,

$$s_{\mathrm{fin}}(y, \sigma) := \sum_{n=1}^{a} \lambda_1(n) \Big(\frac{y}{n} - \kappa\big([-n]\sigma\big) \Big)_+ .$$

For real $z > 0$ and $n \geq 1$ let $H_z(n) := (a/n - a/z)_+$.

Problem 3.2.1. $H_z(n) = a(1/n - 1/z)$ for $n < z$, and $H_z(n) = 0$ for $n \geq z$. Hence for $1 \leq n \leq a$ the n-th term of $s_{\mathrm{fin}}(a, \sigma)$ is $\lambda_1(n) H_x(n)$ if $[-n]\sigma \in \Phi_b$, and $\lambda_1(n) H_{x_1}(n)$ otherwise.

Problem 3.2.2. Let $\sigma \in \Phi$. (i) For $0 \le y \le a$ and $x_1 \le n \le a$, the n-th term of $s_{\mathrm{fin}}(y,\sigma)$ is 0. (ii) For $x \le n < x_1$, the n-th term of $s_{\mathrm{fin}}(a,\sigma)$ is 0 if $[-n]\sigma \in \Phi_b$, and $\lambda_1(n)\, a(1/n - 1/x_1)$ otherwise, which is positive unless $\lambda_1(n) = 0$.

The first step towards the total over the a-places is a ramp sum in a progression.

Problem 3.2.3. For integers $q \ge 1$ prime to d, $A_0 \ge 1$, and real $0 < z \le A_0$,

$$\sum_{n=1}^{A_0} \lambda_q(n)\Big(\frac{A_0}{n} - \frac{A_0}{z}\Big)_+ = A_0\Big(R_q(z) + \frac{\log z}{\varphi(q)} + c_q\Big).$$

For $d = 7$, $q = 4$, $A_0 = 60$, $z = 20$, both sides equal $18\log 5 + \frac{42}{13}\log 13 + \frac{18}{17}\log 17 = 40.2565\ldots$.

Problem 3.2.4. For every integer $n \ge 1$,

$$\sum_{\tau \in \Phi_a} \lambda_1(n)\Big(\frac{a}{n} - \kappa\big([-n]\tau\big)\Big)_+ = \#\Phi_a\, \lambda_1(n) H_{x_1}(n) + \#\Phi_b\, \lambda_{q_0}(n)\big(H_x(n) - H_{x_1}(n)\big).$$

Problem 3.2.5.

$$\sum_{\tau \in \Phi_a} s_{\mathrm{fin}}(a,\tau) = a\Big[\#\Phi_b\big(R_{q_0}(x) - R_{q_0}(x_1)\big) + \#\Phi_a R_1(x_1)\Big] + a\Big[\#\Phi_a(\log x_1 + c_1) + \#\Phi_b\,\frac{\log(x/x_1)}{\varphi(q_0)}\Big].$$

Problem 3.2.6. In the toy example with $x = 20$, $x_1 = 60$, $b = 960$, so that $a = 19200$ and the weights are 960 and 320, the four prime sums $s_{\mathrm{fin}}(a,\tau)$ at the places τ with labels $1, 5, 9, 13$ rounded to the nearest hundredth, are 45108.01, 45591.18, 47772.92, 46814.23. Their total and the right side of Problem 3.2.5 both round to 185286.35.

The expected value uses the mean of the logarithms of the weights over all places. We define the *expected value*

$$s_{\mathrm{main}} := a\Big(\log a - \frac{1}{f}\sum_{\sigma \in \Phi} \log \kappa(\sigma) + c_1\Big).$$

Problem 3.2.7. $\sum_{\sigma\in\Phi} \log\kappa(\sigma) = f\log(a/x_1) - \#\Phi_b \log(x/x_1)$. In the toy example both sides equal $47.24518\ldots$.

Problem 3.2.8. $\#\Phi_a\, s_{\mathrm{main}} = a\big[\#\Phi_a(\log x_1 + c_1) + \#\Phi_b \log(x/x_1)/\varphi(q_0)\big]$.

The *total remainder* is $\mathrm{rem} := \sum_{\tau\in\Phi_a}\big(s_{\mathrm{fin}}(a,\tau) - s_{\mathrm{main}}\big)$, so that the mean of $s_{\mathrm{fin}}(a,\tau)$ over Φ_a is $s_{\mathrm{main}} + \mathrm{rem}/\#\Phi_a$. The total remainder satisfies

$$\mathrm{rem} = a\Big[\#\Phi_b\big(R_{q_0}(x) - R_{q_0}(x_1)\big) + \#\Phi_a R_1(x_1)\Big] \tag{1}$$

in the setting of this chapter. In the toy example, $\mathrm{rem} + 76800\, c_1 = -118612.63\ldots$.

In the proof the *parameters* (q_0, d) are a positive multiple q_0 of 18480 and a prime d with $q_0 \mid 2(d+1)$ and $q_0 \nmid d+1$ (Definition 33.1.1 of Chapter 33). An *admissible datum* for them is a datum satisfying all the conditions of Definition 33.3.1 there. We record the components used here. The scales x, x_1, b are positive integers. The number m of theta lifts in each chain is a power of 2 with $\sqrt{x} \le m \le 2\sqrt{x}$, and the tower exponent is $s = 22\log_2 m$. With $e_s := \lfloor \log_3 s \rfloor$, let $q_1 := q_0\, 3^{e_s+5} 2^s$; the field E, its embedding into $\mathbb{C}$, the primitive root ζ and the labels of the places are as in §3.1. We have $q_1 x_1 \mid b$. The datum supplies $\Phi_b \subseteq \mathrm{cl}^{-1}(-1)$ with $q_1/q_0 \le \#\Phi_b \log b$, and the weight κ above.

Theorem 3.2.1. *For all parameters (q_0, d) and every admissible datum for them, (1) holds, where $a = xb$ and R_q and c_1 are those of Chapter 1 for the prime d.*

For these data q_0 and q_1 have the same prime factors, $d \nmid q_1$, and $d \equiv 7 \pmod 8$. The scale conditions give $0 < \log x$ and $10^6 \log x \le \log x_1$, so $x < x_1$.

3.3. The remainder at the first scale

Chapter 1 needs an upper bound for $R_{q_0}(x)$. When Φ_b is nonempty, equation (1) isolates $R_{q_0}(x)$ at the price of two terms at x_1.

Problem 3.3.1. If $\#\Phi_b > 0$, then $R_{q_0}(x) = \dfrac{\mathrm{rem}}{a\,\#\Phi_b} + R_{q_0}(x_1) - \dfrac{\#\Phi_a}{\#\Phi_b} R_1(x_1)$.

For $\#\Phi_b > 0$, the coefficient of $R_1(x_1)$ has magnitude $\#\Phi_a/\#\Phi_b$, the reciprocal of the proportion of the -1 fibre occupied by Φ_b; this is why Φ_b must be dense.

Problem 3.3.2. If $b > 1$ and $\#\Phi_a \le \#\Phi_b \log b$, then $\#\Phi_b > 0$ and

$$R_{q_0}(x) \le \frac{\mathrm{rem}}{a\,\#\Phi_b} + |R_{q_0}(x_1)| + \log b\,|R_1(x_1)|.$$

In the toy example $\#\Phi_a/\#\Phi_b = 4 \le \log 960 = 6.8669\ldots$.

Problem 3.3.3. Suppose $b > 1$, $\#\Phi_a \le \#\Phi_b \log b$, and m is a positive integer. If $m \cdot \mathrm{rem} \le f a (\log b)^5$, then

$$R_{q_0}(x) \le \frac{\varphi(q_0)(\log b)^6}{m} + |R_{q_0}(x_1)| + \log b\,|R_1(x_1)|.$$

The hypothesis $m \cdot \mathrm{rem} \le f a (\log b)^5$ is the *main inequality*. Chapter 35 proves it for every admissible datum (Theorem 35.2.1) and derives the bound of Problem 3.3.3 in Problem 35.3.1, before passing to the asymptotic estimate of Theorem 35.3.1; Chapter 4 constructs a set Φ_b dense enough for Problem 3.3.2.
In the Lean formalization. In the Lean proof [GL], the parameters and the admissible data are `New.Parameters` and `New.Data`; Theorem 3.2.1 is `New.Data.totalRemainder_eq`, in `New/Reduction/PrimeSums.lean`; and the conclusion of Problem 3.3.3 for every admissible datum, without further hypotheses, is `New.Data.primeRemainder_le`, in `New/Reduction/OneSidedBound.lean`.

Hints

§3.1.

- **3.1.1:** d ramifies in K and not in $\mathbb{Q}(\zeta)$, so $K \cap \mathbb{Q}(\zeta) = \mathbb{Q}$ [Wa, Ch. 2].
- **3.1.2:** Complex conjugation restricts to the nontrivial automorphism of K.
- **3.1.3:** cl is a surjective homomorphism, and $\varphi(q_1)/\varphi(q_0) = q_1/q_0$ when q_0 and q_1 have the same prime factors.
- **3.1.4:** cl is a homomorphism; if $\gcd(n, q_1) > 1$, then $n \not\equiv 1 \pmod{q_0}$.
- **3.1.5:** Multiplication by $[-n]$ is a bijection of Φ; Problem 3.1.4.
- **3.1.6:** (i) $d + 1 \equiv q_0/2 \pmod{q_0}$; for each odd prime $p \mid q_0$, $d \equiv -1 \pmod p$, and reciprocity. (ii) Section 2.1.
- **3.1.7:** p is inert in $\mathbb{Q}(\sqrt{-7})$ exactly when $p \equiv 3, 5, 6 \pmod 7$.

§3.2.

3.2.2: (i) Compare y/n and $\kappa([-n]\sigma)$ with a/x_1. (ii) Use the two possible weights at $[-n]\sigma$.

3.2.3: Problem 3.2.1 with A_0 in place of a, and the definition of R_q.

3.2.4: Write $(a/n - \kappa(\sigma))_+$ as $H_{x_1}(n)$ plus a correction supported on Φ_b; Problem 3.1.5, and $\lambda_{q_0}(n) = \lambda_1(n)$ for $n \equiv 1 \pmod{q_0}$.

3.2.5: Exchange the sums over τ and n; Problem 3.2.3 three times, with $(q, z) = (1, x_1), (q_0, x), (q_0, x_1)$.

3.2.6: Only the $n < 60$ with $\lambda_1(n) \neq 0$ contribute (Problems 3.1.7 and 3.2.2).

3.2.8: Problems 3.1.3 and 3.2.7.

§3.3.

3.3.1: Equation (1).

3.3.2: $\#\Phi_a > 0$.

3.3.3: Problem 3.1.3: $f/\#\Phi_b = \varphi(q_0)\,\#\Phi_a/\#\Phi_b$.

Theorems.

3.2.1: Compare Problems 3.2.5 and 3.2.8.

References

[Ne] J. Neukirch, *Algebraic Number Theory*, Grundlehren Math. Wiss. **322**, Springer, 1999.

[SeA] J.-P. Serre, *A Course in Arithmetic*, Grad. Texts in Math. **7**, Springer, 1973.

[GL] L. Sernau, *GRH for Dirichlet L-functions, in Lean 4*, a shorter rewriting of the Lean proof, text by Claude, `https://github.com/lsernau/grh-lean`, commit `72fead1`, readable edition `grh/`.

[Wa] L. C. Washington, *Introduction to Cyclotomic Fields*, 2nd ed., Grad. Texts in Math. **83**, Springer, 1997.

PLACES FROM A SPHERE

Prerequisites. The structure of $(\mathbb{Z}/p^c\mathbb{Z})^\times$ for a prime p [IR, Ch. 4, §1]. Linearity of expectation. From Chapter 3 we use the places Φ of E and their labels, the reduction cl of the label modulo q_0, the place $[\nu]$ of an integer ν, the a-places Φ_a and the b-places Φ_b (Section 3.1), and Problems 3.1.3, 3.1.6 and 3.3.2. From Chapter 33, the admissible data. We write $U_m := (\mathbb{Z}/m\mathbb{Z})^\times$ for $m \geq 1$.

In Chapter 3 a set Φ_b of places of class -1 modulo q_0 was given the weight b, and Problem 3.3.2 showed why it must be dense: if $b > 1$ and $\#\Phi_a \leq \#\Phi_b \log b$, then

$$R_{q_0}(x) \leq \frac{\text{rem}}{a\,\#\Phi_b} + |R_{q_0}(x_1)| + \log b\,|R_1(x_1)|.$$

How can Φ_b be chosen? The argument asks for a second property, which pulls against density: for every small prime ℓ, it restricts which signed powers of ℓ can occur as ratios of labels of b-places after reduction modulo the prime-to-ℓ part of q_1. Behrend's construction [Beh] meets both: lattice points on a sphere, written as digits in a large base, become exponents of one element of U_{q_1}.

Throughout, for $q' \mid q_1$ let $\mathrm{cl}_{q'} \colon \Phi \to U_{q'}$ be the label reduced modulo q', so that $\mathrm{cl} = \mathrm{cl}_{q_0}$; for a prime ℓ let $q_{(\ell)}$ be the largest divisor of q_1 prime to ℓ. For the parameters (q_0, d) and an integer $s \geq 0$, Chapter 33 sets

$$l_0(s) = 3^{\lfloor \log_3 s \rfloor + 4}, \qquad q_1 = q_0 \cdot 3\, l_0(s)\, 2^s,$$

with $\lfloor \log_3 0 \rfloor$ read as 0. With $e := \lfloor \log_3 s \rfloor$ this is the $q_1 = q_0\, 3^{e+5} 2^s$ of Chapter 3, and Problem 3.1.3 gives $\#\Phi_a = q_1/q_0 = 3 l_0(s) 2^s$. We write l_0 when s is fixed. Exponents in group powers and congruences are integers, as are the exponents in prime-power moduli.

4.1. Two requirements

The first requirement is size, measured against the class of -1.

Problem 4.1.1. Multiplication by $[-1]$ maps Φ_a bijectively onto $\mathrm{cl}^{-1}(-1)$, so $\mathrm{cl}^{-1}(-1)$ has $\#\Phi_a$ elements. In the toy example of Chapter 3, $q_0 = 4$, $q_1 = 16$, it consists of the places with labels $3, 7, 11, 15$.

An admissible datum (Chapter 33) requires

$$q_1/q_0 \leq \#\Phi_b \log b, \tag{1}$$

so Φ_b must contain at least the proportion $1/\log b$ of $\mathrm{cl}^{-1}(-1)$.

The second requirement concerns ratios of places. For $\ell \nmid q_1$, the label of $[\ell]$ is $\ell \bmod q_1$. For $\ell \mid q_1$, the convention of Chapter 3 makes $[\ell]$ the identity. In both cases the sparsity condition compares the reduced label of a ratio with signed powers of ℓ modulo $q_{(\ell)}$.

Date: November 26, 2026.

Problem 4.1.2. Let ℓ be a prime, $\sigma \in \Phi$ and $i \geq 1$. (i) If $\ell \nmid q_1$, then $q_{(\ell)} = q_1$, and the places τ with $\mathrm{cl}_{q_{(\ell)}}(\tau/\sigma) = \pm\ell^i$ are the two places $[\pm\ell^i]\sigma$. (ii) If $\ell^\nu \| q_1$ with $\nu \geq 1$, then for each sign there are $\ell^{\nu-1}(\ell-1)$ such places. For $q_1 = 36$, $\ell = 3$ this is 6.

The proof states the second requirement as follows. For a natural number L, a finite set $\mathcal{P} \subseteq \Phi$ is *sparse for the primes up to* L if for every prime $\ell \leq L$ and all integers $0 < i < i' < l_0(s)$ there are no $\sigma, \tau, \tau' \in \mathcal{P}$, distinct or not, and no signs $\varepsilon, \varepsilon' \in \{\pm 1\}$ with

$$\mathrm{cl}_{q_{(\ell)}}(\tau/\sigma) = \varepsilon\,\ell^i \quad \text{and} \quad \mathrm{cl}_{q_{(\ell)}}(\tau'/\sigma) = \varepsilon'\ell^{i'} \quad \text{in } \mathbb{Z}/q_{(\ell)}\mathbb{Z}.$$

An admissible datum requires Φ_b to be sparse for the primes up to kt, where $k = r + 1 - m$ and $t = 5r$, with m the number of lifts and r the rank of the target (Chapter 33).

Problem 4.1.3. Let $\mathcal{P}$ be sparse for the primes up to L, let $\ell \leq L$ be prime, $v \in U_{q_{(\ell)}}$, and choose a sign ε_μ for every integer μ. Among any l_0 consecutive integers μ, at most two have $\varepsilon_\mu \ell^\mu v \in \mathrm{cl}_{q_{(\ell)}}(\mathcal{P})$.

Problem 4.1.4. Let $\mathcal{P}$ be sparse for the primes up to L, let $p \leq L$ be a prime with $p \nmid q_1$, and $0 < i < i' < l_0$. For no σ are all three of σ, $[-p]^i\sigma$, $[-p]^{i'}\sigma$ in $\mathcal{P}$.

The sparsity of Φ_b is used in two places. Chapter 19 uses Problem 4.1.4 for Φ_b when $p \leq k$ and $\chi_K(p) \neq 1$, in the sharpness argument for the divisibility of derivatives (Problem 19.4.3 and the paragraph before it). The condition $\chi_K(p) \neq 1$ implies $p \nmid q_1$, since every prime divisor of q_1 divides q_0 and Problem 3.1.6(i) applies. Chapter 67, Section 67.2, states the bound $4f\,\mathrm{defect}_\ell$ per unit of rank for the local defect above ℓ; at primes $\ell \leq kt$ the local argument behind it uses sparsity to exclude a third b-place on a short arc. That chapter omits the local argument.

Why are the two requirements in tension? We shall look for Φ_b among the places $[-g^n]$ for the integer g of Section 4.3, whose order modulo a power of 2 is 2^s (Problem 4.3.2). Section 4.3 uses a set of exponents $\mathcal{N} \subseteq [0, 2^s)$ with the following property: for all $n_1, n_2, n_3 \in \mathcal{N}$ and positive integers α, α' with $\alpha + \alpha' \leq 2l_0$, the congruence $(\alpha + \alpha')n_2 \equiv \alpha n_1 + \alpha' n_3 \pmod{2^s}$ implies $n_1 = n_2 = n_3$. For $\alpha = \alpha' = 1$ this excludes nonconstant three-term progressions. The obvious sets without them are thin.

Problem 4.1.5. For an integer $\mu \geq 0$, let $\mathcal{N}_\mu$ be the set of integers in $[0, 3^\mu)$ whose base-3 digits are 0 or 1. (i) $\mathcal{N}_\mu$ contains no nonconstant three-term arithmetic progression, and $|\mathcal{N}_\mu| = (3^\mu)^{\log 2/\log 3}$. (ii) For $\mu \geq 2$, $\mathcal{N}_\mu$ contains $0, 1, 3$, and $3 \cdot 1 = 2 \cdot 0 + 1 \cdot 3$, a relation with $\alpha = 2$, $\alpha' = 1$.

We compare the expected size of a random set with its expected number of progressions.

Problem 4.1.6. Let $o \geq 4$ be even, and let $R \subseteq \mathbb{Z}/o\mathbb{Z}$ contain each element independently with probability δ. The expected number of pairs (n, η) with $\eta \notin \{0, o/2\}$ and $n, n+\eta, n+2\eta \in R$ is $o(o-2)\delta^3$. If $\delta^2(o-2) > 1$, this exceeds the expected size δo of R.

Problem 4.1.7. Let R be as in Problem 4.1.6. For each pair (n, η) counted there choose one of $n, n+\eta, n+2\eta$, and let R' be obtained from R by deleting the chosen points. Then R' contains no three distinct points $n, n+\eta, n+2\eta$, and its expected size is at least $\delta o - \delta^3 o^2$. For $\delta \leq (2o)^{-1/2}$ this is at least $\delta o/2$.

For an admissible datum let $o = 2^s$. Then $o = m^{22}$, $\sqrt{x} \le m \le 2\sqrt{x}$ and $(\log b)^{100} \le x$ (Chapter 33). The density guaranteed by Problem 4.1.7 is of order $o^{-1/2}$ at best, and $(2o)^{-1/2} < x^{-5}$. For places indexed injectively by exponents modulo o, (1) asks for an exponent density at least $3l_0/\log b > x^{-1/100}$. The deletion estimate falls short of the required density by a power of x. We now choose the exponents using lattice points on a sphere.

4.2. Behrend's construction

Behrend [Beh] encodes lattice points of fixed squared length by their digits. Let $D, H \ge 1$ be integers and $\Sigma_\rho := \{v \in \{0, \dots, H-1\}^D : |v|^2 = \rho\}$.

Problem 4.2.1. Let $v, v', v'' \in \mathbb{Z}^D$ have $|v|^2 = |v'|^2 = |v''|^2$, and let α, α' be positive integers with $(\alpha + \alpha')v' = \alpha v + \alpha' v''$. Then $v = v' = v''$.

Problem 4.2.2. Some ρ has $|\Sigma_\rho| \ge H^D/(DH^2)$.

Fix such a ρ and an integer $Q \ge 1$. Let $\beta := QH$, $\mathrm{enc}(v) := \sum_{\mu=0}^{D-1} v_\mu \beta^\mu$, and $\mathcal{N} := \mathrm{enc}(\Sigma_\rho)$.

Problem 4.2.3. If $z_0, \dots, z_{D-1}$ are integers with $|z_\mu| < \beta$ and $\sum_\mu z_\mu \beta^\mu = 0$, then every $z_\mu = 0$. In particular enc is injective on $\{0, \dots, H-1\}^D$.

Problem 4.2.4. Let $n_1, n_2, n_3 \in \mathcal{N}$, and let α, α' be positive integers with $\alpha + \alpha' \le Q$. If $(\alpha + \alpha')n_2 = \alpha n_1 + \alpha' n_3$, then $n_1 = n_2 = n_3$.

Problem 4.2.5. For $D = 3$, $H = 3$, $Q = 8$, so $\beta = 24$, the sphere with the most points is $\rho = 5$, with the six permutations of $(0, 1, 2)$, and $\mathcal{N} = \{26, 49, 578, 624, 1153, 1176\}$. With $Q = 6$, $\beta = 18$, the same sphere gives $\{20, 37, 326, 360, 649, 666\}$.

Problem 4.2.6. Let $o \ge \beta^D$ be an integer. (i) Every $n \in \mathcal{N}$ satisfies $n < o$. (ii) For $n_1, n_2, n_3 \in \mathcal{N}$ and positive integers α, α' with $\alpha + \alpha' \le Q$, the congruence $(\alpha + \alpha')n_2 \equiv \alpha n_1 + \alpha' n_3 \pmod{o}$ implies $n_1 = n_2 = n_3$.

Problems 4.2.1–4.2.4 and 4.2.6 give the following theorem for $D, H \ge 1$; the statement in the proof also covers $DH = 0$. Here D, H, Q, o are natural numbers, and the quotient $H^D/(DH^2)$ is taken in $\mathbb{R}$, with value 0 when $DH = 0$.

Theorem 4.2.1. *If $0 < Q$ and $(QH)^D \le o$, there is a finite set $\mathcal{N}$ of natural numbers such that $n < o$ for every $n \in \mathcal{N}$, $H^D/(DH^2) \le \#\mathcal{N}$, and for all $n_1, n_2, n_3 \in \mathcal{N}$ and all natural numbers α, α' with $0 < \alpha$, $0 < \alpha'$, $\alpha + \alpha' \le Q$, the congruence $(\alpha + \alpha')n_2 \equiv \alpha n_1 + \alpha' n_3 \pmod{o}$ implies $n_1 = n_2$ and $n_2 = n_3$.*

For $Q = 2$, the first Exercise below gives the density lower bound $\exp(-C\sqrt{\log o})$ of Behrend's construction [Beh]. No construction gives a density bounded below by a positive constant independent of N: by Roth's theorem [Ro] a set of integers in $[0, N)$ without nonconstant three-term progressions has $o(N)$ elements as $N \to \infty$. The size condition we need is (1).

4.3. From exponents to places

The exponents of Theorem 4.2.1 become places through one integer g prime to q_1. Let $w = v_2(q_0)$, so that $2^{s+w} \mid q_1$; since $16 \mid 18480$, $w \ge 4$, and the problems below use only $w \ge 2$. Following the construction of the proof, let

$$g := 1 + 3l_0q_0, \qquad \sigma_n := [-g^n] \in \Phi \quad (n \ge 0).$$

A toy of the same shape has $q_0 = 4$ and $l_0 = 3$ in place of the values of the proof, and $s = 13$: then $q_1 = 4 \cdot 9 \cdot 2^{13} = 294912$, $w = 2$ and $g = 37$. In the toy the prime 3 divides q_1 but not q_0, which nothing below uses, and "sparse" is taken with $l_0 = 3$.

Problem 4.3.1. (i) If $c \geq w \geq 2$ and y is odd, then $1 + 2^w y$ has order 2^{c-w} in U_{2^c}. (ii) If $c \geq 1$, then 4 has order 3^{c-1} in U_{3^c}. For example $5^0, 5^1, 5^2, 5^3 \equiv 1, 5, 9, 13 \pmod{16}$, and 4 has order 3 modulo 9.

Problem 4.3.2. The integer g has order 2^s modulo 2^{s+w}. The places σ_n, $0 \leq n < 2^s$, are distinct, and their labels are $\equiv -1 \pmod{3 l_0 q_0}$, in particular modulo q_0. In the toy, 37 has order 2^{13} modulo 2^{15}.

Problem 4.3.3. Let $0 < i < l_0$ and $n, n' \geq 0$. Then $\mathrm{cl}_{q_{(2)}}(\sigma_{n'}/\sigma_n) \neq \pm 2^i$.

Problem 4.3.4. Let ℓ be an odd prime, $0 < i < i'$, and $n_1, n_2, n_3 \geq 0$. If $\mathrm{cl}_{q_{(\ell)}}(\sigma_{n_2}/\sigma_{n_1}) = \pm \ell^i$ and $\mathrm{cl}_{q_{(\ell)}}(\sigma_{n_3}/\sigma_{n_1}) = \pm \ell^{i'}$, then

$$2i'\, n_2 \equiv 2(i' - i)\, n_1 + 2i\, n_3 \pmod{2^s}.$$

Problem 4.3.5. Let $\ell > 1$ be an odd integer, $\lambda \geq 1$ and $s \geq 0$. If $\ell^\lambda \equiv 1 \pmod{2^{s+1}}$, then $2^s \leq (\ell + 1)\lambda$.

Problem 4.3.6. In the toy, the places σ_n for $n = 20, 37, 326, 360, 649, 666$ have labels 153935, 39851, 74807, 243359, 190331, 43271 modulo 294912. These are $\equiv -1 \pmod{36}$, and the six places form a set sparse for the primes up to 1364, the largest L with $6(L + 1) < 2^{13}$.

Problems 4.3.2–4.3.5, with Theorem 4.2.1 for $Q = 2l_0$ and $o = 2^s$, prove the next theorem. It concerns the parameters (q_0, d) and natural numbers s, D, H, L, with the same convention for $H^D/(DH^2)$ as in Theorem 4.2.1.

Theorem 4.3.1. *If $(2l_0(s)H)^D \leq 2^s$ and $2l_0(s)(L + 1) < 2^s$, there is a finite set $\mathcal{P} \subseteq \Phi$ with $\mathrm{cl}(\sigma) = -1$ for every $\sigma \in \mathcal{P}$, with $H^D/(DH^2) \leq \#\mathcal{P}$, and sparse for the primes up to L.*

It remains to choose D and H so that $\#\mathcal{P}$ is large compared with q_1/q_0.

Problem 4.3.7. Let $D \geq 1$ be an integer and $W \geq 1$ real, with $W \leq 2^s \leq W^D$, $(2l_0)^D \leq W$ and $3 l_0 D 2^D \leq W^3$, and let H be the largest power of 2 with $H^D \leq 2^s/W$. Then $H \leq W$, $(2l_0 H)^D \leq 2^s$, and $q_1/q_0 \leq W^6 H^D/(DH^2)$.

With Theorem 4.3.1 this gives a set of places of class -1 modulo q_0, sparse for the primes up to L, with $q_1/q_0 \leq \#\mathcal{P} \cdot W^6$, under the hypotheses of Problem 4.3.7 and $2l_0(L + 1) < 2^s$. If moreover $W^6 \leq \log b$, then $\mathcal{P}$ satisfies (1) in place of Φ_b. This ends the choice of places. From Chapter 5 on, the next part develops the comparison of divisibility with size.

In the Lean formalization. In the Lean proof [GL], sparsity is the definition `New.Parameters.IsSparse` (file `New/Reduction/Data/AdmissibleData.lean`), and Theorems 4.2.1 and 4.3.1 are `New.exists_three_term_free` and `New.Parameters.exists_large_isSparse` (file `New/Reduction/Data/Existence.lean`); the proof of the latter is the construction of Section 4.3.

Exercises.

(1) With $Q = 2$, $D = \lceil\sqrt{\log o}\,\rceil$ and H the largest integer with $(2H)^D \le o$, Theorem 4.2.1 gives a set $\mathcal{N} \subset [0, o)$ without nonconstant three-term progressions modulo o and with $\#\mathcal{N} \ge o\exp(-C\sqrt{\log o})$ for large o, for an absolute constant C.

(2) The hypothesis $o \ge \beta^D$ cannot be dropped from Problem 4.2.6: for $D = 3$, $H = Q = 2$, $\rho = 1$ and $o = 27$, every element of $\mathcal{N}$ is less than o, but three distinct elements of $\mathcal{N}$ form an arithmetic progression modulo o.

Hints

§4.1.

4.1.1: Problem 3.1.3.
4.1.2: (ii) Count a fibre of $U_{q_1} \to U_{q_{(\ell)}}$.
4.1.3: Take three such μ.
4.1.4: $(-p)^i = (-1)^i p^i$.
4.1.5: (i) Add the outer terms digit by digit.
4.1.6: For $\eta \notin \{0, o/2\}$ the three points are distinct.
4.1.7: Linearity of expectation.

§4.2.

4.2.1: Three distinct points of a sphere are never collinear. Compute $\alpha|v|^2 + \alpha'|v''|^2 - (\alpha+\alpha')|v'|^2$ in terms of $v - v''$.
4.2.2: Count the possible values of $|v|^2$.
4.2.3: Look at the lowest nonzero z_μ modulo β.
4.2.4: Problem 4.2.3.
4.2.6: (ii) Bound the base-β digits of both sides.

§4.3.

4.3.1: Induction on the exponent of 2, resp. 3, in $(1+2^w y)^{2^r} - 1$, resp. $4^{3^r} - 1$.
4.3.2: Problem 4.3.1(i).
4.3.3: Use $3l_0 \mid q_{(2)}$ and Problem 4.3.1(ii).
4.3.4: For odd ℓ, $2^{s+w} \mid q_{(\ell)}$. Work modulo 2^{s+w}.
4.3.5: Compute $v_2(\ell^\lambda - 1)$ for λ odd and for λ even; for λ even use $\ell^2 - 1 = (\ell-1)(\ell+1)$ and Problem 4.3.1(i) for ℓ^2.
4.3.6: Problems 4.2.5 (base 18), 4.3.3 and 4.3.4 with $l_0 = 3$; if the exponents coincide, Problem 4.3.5.
4.3.7: Compare $(2H)^D$ with $2^s/W$.

References

[Beh] F. A. Behrend, *On sets of integers which contain no three terms in arithmetical progression*, Proc. Nat. Acad. Sci. U.S.A. **32** (1946), 331–332.

[GL] L. Sernau, *GRH for Dirichlet L-functions, in Lean 4*, a shorter rewriting of the Lean proof, text by Claude, `https://github.com/lsernau/grh-lean`, commit `72fead1`, readable edition `grh/`.

[IR] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, 2nd ed., Springer, 1990.

[Ro] K. F. Roth, *On certain sets of integers*, J. London Math. Soc. **28** (1953), 104–109.

SIZE AGAINST DIVISIBILITY

Prerequisites. Linear algebra over $\mathbb{C}$: Hermitian and positive semidefinite matrices, and Hadamard's inequality, in the form $\det A \le a_{11}\cdots a_{nn}$ for a positive semidefinite Hermitian matrix $A = (a_{ik})$, or $|\det(v_1,\dots,v_n)| \le \|v_1\|\cdots\|v_n\|$ for vectors. Dedekind domains, the absolute norm, the product formula [Ne, Ch. I and Ch. III], and the unique extension of the ℓ-adic absolute value to an algebraic closure $\overline{\mathbb{Q}}_\ell$ of $\mathbb{Q}_\ell$ [Ne, Ch. II, §4]. Transcendence bases [La, Ch. VIII, §1], and two consequences: $\mathbb{C}$ and $\overline{\mathbb{Q}}_\ell$ are isomorphic fields, both being algebraically closed of characteristic 0 and of transcendence degree the continuum over $\mathbb{Q}$; and an isomorphism between two subfields of $\mathbb{C}$ that are finitely generated over $\mathbb{Q}$ extends to an automorphism of $\mathbb{C}$. Legendre's formula $v_p(n!) = \sum_{e\ge1}\lfloor n/p^e\rfloor$, Stirling's formula, and the von Mangoldt function Λ. No earlier chapter is used. The next chapter, *A twist for each prime*, continues this one.

5.1. Divisibility against size

How can a divisibility statement bound a sum over primes? A binomial coefficient illustrates Chebyshev's factorial method [Ch]. Let $\theta(x) := \sum_{p\le x}\log p$. In the next two problems let n be a nonnegative integer.

Problem 5.1.1. Every prime p with $n < p \le 2n$ divides $\binom{2n}{n}$, and $\binom{2n}{n} \le 4^n$. Hence $\theta(2n) - \theta(n) \le n\log 4$.

The principle is the following. If a nonzero integer Δ is divisible by p^{e_p} for each prime p in a set S, where the e_p are nonnegative integers, then

$$\sum_{p\in S} e_p \log p \le \log|\Delta|. \tag{1}$$

For $\Delta = n!$ and $e_p = v_p(n!)$, with S the primes up to n, both sides of (1) are known exactly.

Problem 5.1.2. $\log n! = \sum_{r\le n}\Lambda(r)\lfloor n/r\rfloor$.

By Stirling's formula the left side is $n\log n - n + O(\log n)$. Without the floor function the right side would be $n\sum_{r\le n}\Lambda(r)/r$. Removing the floors overestimates the right side by $\sum_{r\le n}\Lambda(r)\{n/r\}$, an error of order n by Chebyshev's bounds, the scale of the linear term in Stirling's formula; so this estimate cannot see $\psi(n) - n$, where $\psi(x) := \sum_{r\le x}\Lambda(r)$. For a finer comparison one can seek divisibility bounds with a continuous weight on prime powers, such as $(x/p^e - 1)_+$, where $t_+ := \max(t, 0)$, and a size estimate whose error is smaller than its linear term.

The number Δ will be a minor of a matrix.

Problem 5.1.3. Let $A \in M_r(\mathbb{Z})$ with $\det A \ne 0$, and suppose that the jth column A_j is divisible by the positive integer g_j. Then

$$g_1\cdots g_r \le |\det A| \le \|A_1\|\cdots\|A_r\|.$$

Date: November 26, 2026.

For the columns $(6,6)$ and $(10,20)$, with $g_1 = 6$ and $g_2 = 10$, the three numbers are 60, 60 and $60\sqrt{10}$.

The same principle holds over a number field K, where the product formula accounts for the size of a number at every place. At a finite place v write $\mathcal{O}_v$, $\mathfrak{p}_v$ and q_v for the valuation ring, its maximal ideal and the size of its residue field, and let $|x|_v := q_v^{-\operatorname{ord}_v x}$. At an archimedean place use the usual modulus. Let $n_v := 2$ at complex places and $n_v := 1$ at the other places. Then $\sum_v n_v \log|x|_v = 0$ for $x \in K^\times$. Hence, if $\gamma \in K^\times$ satisfies $|\gamma|_v \le \exp(b_v - g_v)$ at every place, where b_v and g_v are real and vanish for almost all v, then

$$\sum_v n_v g_v \le \sum_v n_v b_v. \tag{2}$$

Typically γ is a minor of a matrix, b_v bounds it through the sizes of the entries, and g_v records an improvement from a congruence. The minor is chosen once over K, but the basis in which one proves the congruence may vary with v.

5.2. A minor of a jet evaluation map

Where does a minor with many prime factors come from? One source is Frobenius. Throughout this section p denotes a prime. Let $K = \mathbb{Q}(\mathrm{i})$, so that a prime $p \equiv 3 \pmod 4$ is inert and $\mathbb{Z}[\mathrm{i}]/p$ is the field with p^2 elements.

Problem 5.2.1. If $p \equiv 3 \pmod 4$ and $u \in \mathbb{Z}[\mathrm{i}]$, then $\bar{u} \equiv u^p \pmod p$.

Thus complex conjugation is the Frobenius at every inert prime. Let $u_1, \dots, u_I \in \mathbb{Z}[\mathrm{i}]$, let $\mathcal{T} \subset \mathbb{Z}^2_{\ge 0}$ be a finite set of s exponents, and let J be a positive integer. On the K-span of the monomials $X^a Y^b$, $(a,b) \in \mathcal{T}$, consider the jet evaluation map

$$\mathrm{ev}\colon f \longmapsto \big((\partial_X^j f)(u_i, \bar{u}_i)\big)_{1 \le i \le I,\ 0 \le j < J}.$$

Its matrix has entries in $\mathbb{Z}[\mathrm{i}]$. Let $g := X^p - Y$.

Problem 5.2.2. Let $p \equiv 3 \pmod 4$. For $f \in \mathbb{Z}[\mathrm{i}][X,Y]$, $u \in \mathbb{Z}[\mathrm{i}]$ and integers $j, k \ge 0$, the number $\big(\partial_X^j (g^k f)\big)(u, \bar{u})$ is divisible by p^k.

Problem 5.2.3. Let $p \equiv 3 \pmod 4$, and suppose that $(a-p, b+1) \in \mathcal{T}$ whenever $(a,b) \in \mathcal{T}$ and $a \ge p$. Then every $s \times s$ minor of the matrix of ev is divisible by p^{N_p}, where $N_p := \sum_{(a,b)\in\mathcal{T}} \lfloor a/p \rfloor$. The set $\mathcal{T} = \{(a,b) : a + 2b \le N\}$ satisfies the hypothesis for every p.

Let $\beta := \max(1, |u_1|, \dots, |u_I|)$, $D := \sum_{\mathcal{T}} (a+b)$ and $A_* := \max(\{1\} \cup \{a : (a,b) \in \mathcal{T}\})$. Every $s \times s$ minor of the matrix of ev has absolute value at most $s!\, A_*^{s(J-1)} \beta^D$.

Theorem 5.2.1. *Suppose that* ev *is injective, and let P be a set of primes $p \equiv 3 \pmod 4$ for which $\mathcal{T}$ satisfies the hypothesis of Problem 5.2.3. Then*

$$\sum_{p \in P} \log p \sum_{(a,b)\in\mathcal{T}} \left\lfloor \frac{a}{p} \right\rfloor \le D \log \beta + \log s! + s(J-1) \log A_*.$$

Over a finite field, Stepanov's method for curves likewise compares the forced vanishing of an auxiliary function with a bound on its degree [Bom].

5.3. Heights of families

In Section 5.1 the size and the divisibility of one number were compared at the places of one field. In the proof the number examined at a prime may depend on the isomorphism used there, and no number field is fixed in advance. The places are therefore replaced by isomorphisms.

For a prime ℓ let $|\cdot|_\ell$ be the absolute value on $\overline{\mathbb{Q}}_\ell$ that extends the ℓ-adic one, so that $|\ell|_\ell = \ell^{-1}$. Write $\iota \mid \ell$ for a field isomorphism $\iota\colon \mathbb{C} \to \overline{\mathbb{Q}}_\ell$, put $|x|_\iota := |\iota(x)|_\ell$ for $x \in \mathbb{C}$, and let $\bar\iota \mid \ell$ be the isomorphism $x \mapsto \iota(\bar x)$. Let $\mathrm{Aut}(\mathbb{C})$ be the group of all field automorphisms of $\mathbb{C}$; most of them are not continuous. A *family* y assigns a complex number y_ι to every isomorphism $\iota \mid \ell$, for every prime ℓ.

Problem 5.3.1. Let $\iota \mid \ell$. If $x \in \mathbb{Q}$, then $|x|_\iota = |x|_\ell$. If $\ell \equiv 3 \pmod 4$ and $0 \neq x \in \mathbb{Z}[\mathrm{i}]$, then $|x|_\iota = \ell^{-v}$, where ℓ^v is the exact power of ℓ dividing x in $\mathbb{Z}[\mathrm{i}]$. If $\ell = 5$, then exactly one of $|2+\mathrm{i}|_\iota$ and $|2+\mathrm{i}|_{\bar\iota}$ equals $1/5$, and the other equals 1.

So the constant family 2+i has different absolute values at different isomorphisms above one prime. The following notion bounds a family by one number. Let $c \in \mathbb{R}$. A family y has *height at most* c if there are $H \in \mathbb{C}$, $\alpha \in \mathbb{R}$ and real numbers $h(\ell)$, one for each prime ℓ, such that

(i) $H \neq 0$, and $h(\ell) \geq 0$ for every prime ℓ;
(ii) $|\sigma H| \leq e^\alpha$ for every $\sigma \in \mathrm{Aut}(\mathbb{C})$;
(iii) $|Hy_\iota|_\iota \leq \ell^{h(\ell)}$ for every prime ℓ and every $\iota \mid \ell$;
(iv) $\alpha + \sum_{\ell \in U} h(\ell) \log \ell \leq c$ for every finite set U of primes.

The multiplier H and the bound α at infinity are common to all ι, while y_ι may depend on ι, even among the isomorphisms above one prime. There is no condition on the sign of α. We write $\mathrm{ht}(y) \leq c$ when y has height at most c.

Problem 5.3.2. If the families y and y' have heights at most c and c', then the family $\iota \mapsto y_\iota y'_\iota$ has height at most $c + c'$. If y has height at most c, then for every integer $n \geq 0$ the family $\iota \mapsto y_\iota^n$ has height at most nc.

Problem 5.3.3. (a) Let $e(\ell)$ be real numbers, of any sign, one for each prime ℓ, with $\sum_{\ell \in U} e(\ell) \leq c$ for every finite set U of primes. If $|y_\iota|_\iota \leq e^{e(\ell)}$ for every $\iota \mid \ell$, then y has height at most c. (b) If $H \neq 0$ and $|\sigma H| \leq e^c$ for every $\sigma \in \mathrm{Aut}(\mathbb{C})$, then the constant family H^{-1} has height at most c.

Can a height be negative? For the constant family 1, every admissible bound is nonnegative.

Problem 5.3.4. If $H \in \mathbb{C}$ is transcendental over $\mathbb{Q}$, then for every prime ℓ the numbers $|H|_\iota$, $\iota \mid \ell$, are unbounded. Hence a number H with $|H|_\iota \leq C$ for all $\iota \mid 2$ is algebraic.

Problem 5.3.5. If the constant family 1 has height at most c, then $c \geq 0$.

We now compare a height bound for a nonzero constant family with a uniform upper bound on the absolute values of its conjugates.

Theorem 5.3.1. *Let $z \in \mathbb{C}$, $z \neq 0$, and $c, c' \in \mathbb{R}$. If the constant family z has height at most c, and $|\sigma z| \leq e^{c'}$ for every $\sigma \in \mathrm{Aut}(\mathbb{C})$, then $-c \leq c'$.*

Problem 5.3.6. Let $x \in \mathbb{Q}^\times$. The constant family x has height at most c if and only if $c \geq -\log|x|$. For instance, the constant family 2 has height at most $-\log 2$.

If $g = \prod_{p \in S} p^{e_p}$, with S a finite set of primes, divides the nonzero integer Δ, then the constant family Δ has height at most $-\log g$, and Theorem 5.3.1 then gives (1).

Problem 5.3.7. Let S be a finite set of primes and $N := \prod_{\ell \in S} \ell$. The family with $y_\iota = \ell^{-1}$ for $\iota \mid \ell$ with $\ell \in S$, and $y_\iota = 1$ for $\iota \mid \ell$ with $\ell \notin S$, has height at most c if and only if $c \geq \log N$. For $S = \{2, 3\}$ the least height is $\log 6$.

5.4. Index and covolume

The minor Δ of Section 5.2 is a Gaussian integer and a determinant. In the proof the corresponding comparison is between Gram determinants of families of vectors: bounds on squared lengths control the size, and at each ι the rows of a matrix of controlled determinant give integral combinations of the vectors, which controls the divisibility. Here we use one map; the next chapter allows a choice of twist for each $\iota \mid \ell$.

For $\iota \mid \ell$ let $\mathcal{O}_\iota := \{x \in \mathbb{C} : |x|_\iota \leq 1\}$, a subring of $\mathbb{C}$. A *lattice datum* consists of

(i) a complex vector space V, a complex inner product space W, with $\langle \cdot, \cdot \rangle$ conjugate-linear in the first variable, and a linear map $\Theta \colon V \to W$;
(ii) for every prime ℓ and every $\iota \mid \ell$, an $\mathcal{O}_\iota$-submodule $\Lambda_\iota \subseteq W$, such that $|\langle \varphi, \varphi' \rangle|_\iota \leq 1$ for all $\varphi \in \Lambda_{\bar{\iota}}$ and $\varphi' \in \Lambda_\iota$;
(iii) a finite set I, a linear map $b \colon W \to \mathbb{C}^I$, and a matrix $G \in M_I(\mathbb{Q})$, positive definite as a complex matrix, with $\langle \varphi, \varphi' \rangle = b(\varphi)^* G\, b(\varphi')$ for all $\varphi, \varphi' \in W$, where * is the conjugate transpose.

A vector $y \in V$ is *integral at* ι if $\Theta y \in \Lambda_\iota$; these vectors form an $\mathcal{O}_\iota$-submodule M_ι of V. The *standard datum* on $\mathbb{C}^n$ has $V = W = \mathbb{C}^n$, $\Theta = b = \mathrm{id}$, $G = 1$ and $\Lambda_\iota = \mathcal{O}_\iota^n$.

Let S be a finite set, $y = (y_s)_{s \in S}$ a family of vectors of V, and $\delta \in \mathbb{R}$. The family y has *index at most* δ if there are real numbers $e(\ell) \geq 0$, one for each prime ℓ, with $\sum_{\ell \in U} e(\ell) \log \ell \leq \delta$ for every finite set U of primes, such that for every $\iota \mid \ell$ some matrix $u \in M_S(\mathcal{O}_\iota)$ satisfies

$$|\det u|_\iota \geq \ell^{-e(\ell)} \quad \text{and} \quad \sum_{k \in S} u_{ik}\, y_k \in M_\iota \text{ for every } i \in S.$$

The matrix may depend on ι. Every admissible δ is nonnegative.

Problem 5.4.1. The standard datum satisfies condition (ii). In it, a family of vectors with entries in $\mathbb{Z}[\mathrm{i}]$ has index at most 0. On $\mathbb{C}^1$, the family consisting of the one vector $1/3$ has index at most δ if and only if $\delta \geq \log 3$.

Problem 5.4.2. If $y = (y_s)_{s \in S}$ has index at most δ and $y' = (y'_s)_{s \in S'}$ has index at most δ', then the family indexed by the disjoint union $S \sqcup S'$ that restricts to y and y' has index at most $\delta + \delta'$.

An index bound is usually proved one submodule at a time. For $\mathcal{O}_\iota$-submodules M, M' of V and $z \in \mathcal{O}_\iota$, say that *the colength of M' in M divides z* if for every $n \geq 0$ and all $\Phi_1, \ldots, \Phi_n \in M$ there is a matrix $m \in M_n(\mathcal{O}_\iota)$ such that $\det m$ divides z in $\mathcal{O}_\iota$ and $\sum_k m_{ik} \Phi_k \in M'$ for every i. No inclusion between M and M' is assumed. This colength condition gives an upper bound for the index.

Theorem 5.4.1. *Let $y_1, \ldots, y_n \in V$, $\delta \in \mathbb{R}$, and let $e(\ell) \geq 0$, one for each prime ℓ, satisfy $\sum_{\ell \in U} e(\ell) \log \ell \leq \delta$ for every finite set U of primes. Suppose that for every $\iota \mid \ell$ there are an integer $j \geq 0$ and an $\mathcal{O}_\iota$-submodule $M \subseteq V$ such that $j \leq e(\ell)$,*

every y_i lies in M, and the colength of M_ι in M divides ℓ^j. Then y has index at most δ.

Problem 5.4.3. Let $\Lambda \subset \mathbb{Q}^n$ be a subgroup that contains $\mathbb{Z}^n$ with finite index N, and let $y_1, \dots, y_n$ be a basis of Λ. In the standard datum on $\mathbb{C}^n$, the family y has index at most $\log N$, and $\det(y_i^* y_k)_{i,k} = N^{-2}$.

Now the size. For $\sigma \in \mathrm{Aut}(\mathbb{C})$ and $y \in V$ let $v_\sigma(y) \in \mathbb{C}^I$ be the vector $b(\Theta y)$ with σ applied to each coordinate, and let $N(y,\sigma) := \mathrm{Re}\big(v_\sigma(y)^* G\, v_\sigma(y)\big)$. A family $y = (y_s)_{s\in S}$ has *covolume at most c* if

$$\big|\det\big(v_\sigma(y_i)^* G\, v_\sigma(y_k)\big)_{i,k\in S}\big| \le e^c \quad \text{for every } \sigma \in \mathrm{Aut}(\mathbb{C}).$$

For $\sigma = \mathrm{id}$ the determinant is the Gram determinant of the vectors Θy_s, the square of a volume. So the family of Problem 5.4.3 has covolume at most c exactly when $c \ge -2\log N$. In the next example G differs from the identity when $D \ge 3$. For $f \in \mathbb{C}[z]$ let

$$\|f\|^2 := \frac{1}{\pi}\int_{\mathbb{C}} |f(z)|^2 e^{-|z|^2}\, dA(z).$$

Problem 5.4.4. The monomials are orthogonal, and $\|z^a\|^2 = a!$.

Problem 5.4.5. Let D be a positive integer, let $V = W$ be the polynomials of degree less than D with the inner product of Problem 5.4.4, $\Theta = \mathrm{id}$, $b(f) = (f_0, \dots, f_{D-1})$ the coefficients, $G = \mathrm{diag}(0!, 1!, \dots, (D-1)!)$, and Λ_ι the polynomials with coefficients in $\mathcal{O}_\iota$. This is a lattice datum. In it, the family $(z^a/a!)_{0\le a<D}$ has index at most $\sum_{a<D} \log a!$, and covolume at most c if and only if $c \ge -\sum_{a<D}\log a!$. For $D = 4$ the sum is $\log 12$.

Problem 5.4.6. Let $G \in M_I(\mathbb{C})$ be positive semidefinite and $w_1, \dots, w_n \in \mathbb{C}^I$. Then $|\det(w_i^* G w_k)_{i,k}| \le \prod_i w_i^* G w_i$. For $G = 1$ and the columns $(6,6)$ and $(10,20)$ of Problem 5.1.3 the two sides are 3600 and 36000.

A uniform bound on squared norms gives a covolume bound.

Theorem 5.4.2. *Let $y_1, \dots, y_n \in V$ and $h \in \mathbb{R}$. If $N(y_i, \sigma) \le e^h$ for every i and every $\sigma \in \mathrm{Aut}(\mathbb{C})$, then y has covolume at most nh.*

The hypothesis concerns every σ. For the vector $1-\sqrt{2}$ in the standard datum on $\mathbb{C}^1$, $N(1-\sqrt{2}, \mathrm{id}) = 3 - 2\sqrt{2}$, but $N(1-\sqrt{2}, \sigma) = 3 + 2\sqrt{2}$ when $\sigma\sqrt{2} = -\sqrt{2}$.

Size and divisibility now meet in one determinant. Let $y_1, \dots, y_n \in V$, and let $\Gamma := \det(\langle \Theta y_i, \Theta y_k\rangle)_{i,k}$ be their Gram determinant. For $\sigma \in \mathrm{Aut}(\mathbb{C})$ let σ' be the automorphism $x \mapsto \overline{\sigma(\bar{x})}$.

Problem 5.4.7. For $y, y' \in V$ and $\sigma \in \mathrm{Aut}(\mathbb{C})$, $\sigma\langle \Theta y, \Theta y'\rangle = v_{\sigma'}(y)^* G\, v_\sigma(y')$.

Problem 5.4.8. Let $G \in M_I(\mathbb{C})$ be positive semidefinite, and let A, B be $I \times n$ matrices. Then $|\det(A^*GB)|^2 \le |\det(A^*GA)|\,|\det(B^*GB)|$. Consequently, if y has covolume at most c, then $|\sigma\Gamma| \le e^c$ for every $\sigma \in \mathrm{Aut}(\mathbb{C})$.

Problem 5.4.9. Let $\iota \mid \ell$, and let $u, u' \in M_n(\mathbb{C})$ satisfy $\sum_k u_{ik} y_k \in M_\iota$ and $\sum_k u'_{ik} y_k \in M_{\bar\iota}$ for every i. Then $|\overline{\det u'}|_\iota\, |\Gamma|_\iota\, |\det u|_\iota \le 1$. Consequently, if y has index at most δ, then the constant family Γ has height at most 2δ.

If Θ is injective and y is a basis of V, then $\Gamma \ne 0$.

Theorem 5.4.3. *Let Θ be injective, and let $y_1, \dots, y_n$ be a basis of V. If y has covolume at most c and index at most δ, then*

$$0 \le c + 2\delta.$$

By Problems 5.4.1 and 5.4.3, equality holds for the vector $1/3$ in $\mathbb{C}^1$, with $c = -2\log 3$ and $\delta = \log 3$, and for a basis of a lattice $\Lambda \supseteq \mathbb{Z}^n$. In the datum of Problem 5.4.5 the bounds found there give $c + 2\delta = \sum_{a<D} \log a!$.

Problem 5.4.10. In the setting of Theorem 5.2.1, let Δ be a nonzero $s \times s$ minor of the matrix of ev, let $g := \prod_{p \in P} p^{N_p}$, and let $B := s!\, A_*^{s(J-1)} \beta^D$. In the standard datum on $\mathbb{C}^1$, the vector Δ/g has index at most 0 and covolume at most $2\log(B/g)$, and Theorem 5.4.3 gives Theorem 5.2.1. For $P = \{3\}$, $I = 1$, $u_1 = \mathrm{i}$, $J = 2$ and $\mathcal{T} = \{(3,0),(0,1)\}$: $\Delta = \pm 3\mathrm{i}$, $g = 3$ and $B = 18$.

In the Lean formalization. In the Lean proof [GL], the height bound $\mathrm{ht}(y) \le c$ is `HeightLe`, Problem 5.3.5 is `HeightLe.nonneg_of_one` and Theorem 5.3.1 is `HeightLe.neg_le_of_norm_map_le` (file `New/Reduction/Lattices/Heights.lean`). In `HeightLe` and `TwistedLattice.IndexLe`, respectively, the functions h and e are defined on all natural numbers and are nonnegative everywhere. Only their values at primes occur in the local bounds and finite sums. A lattice datum is a `TwistedLattice` with a single twist, allowed at every $m \in \mathbb{N}$; index and covolume are `TwistedLattice.IndexLe` and `TwistedLattice.CovolumeLe`, Theorems 5.4.1 and 5.4.2 are `TwistedLattice.indexLe_of_colengthDvd` and `TwistedLattice.covolumeLe_of_normSqAt_le`, and Theorem 5.4.3 is the case of `TwistedLattice.covolume_add_index_nonneg` with this single twist, no completing vectors, the auxiliary scalar 1 and the three auxiliary bounds 0, for any inner product on V (file `New/Reduction/Lattices/TwistedLattice.lean`).

Theorem 5.4.3 compares the size and divisibility bounds for a single nonzero Gram determinant. In the proof, integrality at $\iota \mid \ell$ is tested through every map allowed at ℓ, one allowed map is chosen for each ι, and the covolume is read through the map of the trivial twist; Chapter 6 adds a height bound for the family whose value at ι is the squared volume of the trivial map divided by that of the chosen map.

Hints

§5.1.

5.1.1: Write $\binom{2n}{n} = (2n)!/(n!)^2$. For the size, expand $(1+1)^{2n}$.
5.1.2: Count the multiples of p^e up to n.
5.1.3: Divide each column by g_j.

§5.2.

5.2.1: The binomial theorem modulo p.
5.2.2: Problem 5.2.1 and the Leibniz rule.
5.2.3: Write $a = kp + t$ with $0 \le t < p$, and consider the polynomials $X^t Y^b g^k$.

§5.3.

5.3.1: The restriction of $|\cdot|_\iota$ to $\mathbb{Q}(\mathrm{i})$ is an absolute value extending $|\cdot|_\ell$. For $\ell = 5$: $(2+\mathrm{i})(2-\mathrm{i}) = 5$, and $\bar{\iota}(2+\mathrm{i}) = \iota(2-\mathrm{i})$.
5.3.2: Multiply the multipliers.
5.3.3: (a) Take $H = 1$. (b) Take the multiplier H.

5.3.4: Fix one $\iota_0 \mid \ell$. Extend an isomorphism $\mathbb{Q}(H) \to \mathbb{Q}(\iota_0^{-1}(t))$, for a suitable transcendental $t \in \overline{\mathbb{Q}}_\ell$, to an automorphism of $\mathbb{C}$.

5.3.5: Problem 5.3.4, then the product formula for the norm of H from $\mathbb{Q}(H)$ to $\mathbb{Q}$.

5.3.6: Take $H = x^{-1}$; for the converse, Theorem 5.3.1.

5.3.7: Compare with the constant family $1/N$.

§5.4.

5.4.1: At $\iota \mid 3$ a 1×1 matrix (u) must satisfy $|u|_\iota \leq 1/3$.

5.4.2: Block diagonal matrices.

5.4.3: Express the standard basis in terms of y.

5.4.4: Polar coordinates.

5.4.5: A diagonal matrix.

5.4.6: The matrix $(w_i^* G w_k)$ is positive semidefinite.

5.4.7: The entries of G are rational.

5.4.8: The Gram matrix of the $2n$ columns of A and B is positive semidefinite; apply a Schur complement after adding ε times the identity, and let $\varepsilon \to 0$. Then Problem 5.4.7.

5.4.9: Compare the matrix of inner products of the two transformed families with that of the vectors Θy_k. Then Problem 5.3.3(a).

5.4.10: An automorphism of $\mathbb{C}$ restricts to the identity or to complex conjugation on $\mathbb{Q}(\mathrm{i})$.

References

[Bom] E. Bombieri, *Counting points on curves over finite fields (d'après S. A. Stepanov)*, Séminaire Bourbaki, Exp. 430, Lecture Notes in Math. 383, Springer, 1974, 234–241.

[Ch] P. L. Chebyshev, *Mémoire sur les nombres premiers*, J. Math. Pures Appl. **17** (1852), 366–390.

[GL] L. Sernau, *GRH for Dirichlet L-functions, in Lean 4*, a shorter rewriting of the Lean proof, text by Claude, `https://github.com/lsernau/grh-lean`, commit `72fead1`, readable edition `grh/`.

[La] S. Lang, *Algebra*, rev. 3rd ed., Grad. Texts in Math. 211, Springer, 2002.

[Ne] J. Neukirch, *Algebraic Number Theory*, Grundlehren Math. Wiss. 322, Springer, 1999.

A TWIST FOR EACH PRIME

Prerequisites. Finite-dimensional complex inner product spaces; Hadamard's inequality and Fischer's inequality for positive semidefinite hermitian matrices [HJ, §7.8]. From Chapter 5, *Size against divisibility*: Sections 5.3 and 5.4, whose notation we keep: isomorphisms $\iota \mid \ell$, $|\cdot|_\iota$, $\mathcal{O}_\iota$, $\bar{\iota}$, families and their heights, lattice data, index and covolume. Inner products are conjugate-linear in the first variable. For vectors $w_1, \dots, w_n$ in an inner product space let $\Gamma(w) := \det(\langle w_i, w_k \rangle)_{i,k}$, with $\Gamma(\varnothing) = 1$.

Theorem 5.4.3 compares the size and the divisibility of one Gram determinant, both read through one map Θ. In the proof the size of the Gram determinant of a basis is read through a fixed map Θ_1, and at each isomorphism $\iota \mid \ell$ its divisibility is read through the map Θ_{θ_ι} for a *twist* θ_ι allowed at ℓ. For injective maps the Gram determinant of a basis under Θ_1 is its Gram determinant under Θ_{θ_ι} times a number $Z(1)/Z(\theta_\iota)$ that does not depend on the basis. This chapter works this out on $\mathbb{C}^2$ and then states the general inequality.

6.1. One twist on $\mathbb{C}^2$

A lattice datum asks for $|\langle \varphi, \varphi' \rangle|_\iota \le 1$ with φ integral at $\bar{\iota}$ and φ' integral at ι. The two isomorphisms cannot be taken equal.

Problem 6.1.1. Some $\iota \mid 5$ has $|2 + \mathrm{i}|_\iota = 1$. For such ι, $v := (2 + \mathrm{i})^{-1}$ lies in $\mathcal{O}_\iota$, and $\langle v, v \rangle = 1/5$ does not.

A *twisted lattice* on a complex vector space V, with twists in a set Tw that has a distinguished element 1, consists of the following data.

(1) For each $\vartheta \in \mathrm{Tw}$, a complex inner product space W_ϑ and a linear map $\Theta_\vartheta \colon V \to W_\vartheta$.
(2) A predicate on $\mathbb{N} \times \mathrm{Tw}$. At a prime ℓ it specifies the twists *allowed* at ℓ. In the toys take it to be false at nonprimes.
(3) For each $\vartheta \in \mathrm{Tw}$ and each $\iota \mid \ell$, an $\mathcal{O}_\iota$-submodule $\Lambda_{\vartheta,\iota} \subseteq W_\vartheta$, such that $|\langle \varphi, \varphi' \rangle|_\iota \le 1$ for all $\varphi \in \Lambda_{\vartheta,\bar{\iota}}$ and $\varphi' \in \Lambda_{\vartheta,\iota}$ whenever ϑ is allowed at ℓ.
(4) Rational coordinates on W_1 alone: a finite set I, a linear map $b \colon W_1 \to \mathbb{C}^I$ and a matrix $G \in M_I(\mathbb{Q})$, positive definite as a complex matrix, with $\langle \varphi, \varphi' \rangle = b(\varphi)^* G\, b(\varphi')$ for all $\varphi, \varphi' \in W_1$.

A vector $y \in V$ is *integral at* $\iota \mid \ell$ if $\Theta_\vartheta y \in \Lambda_{\vartheta,\iota}$ for every ϑ allowed at ℓ; these vectors form an $\mathcal{O}_\iota$-submodule $M_\iota \subseteq V$. Sizes will be read through Θ_1 alone.

Throughout, p and r are distinct primes. The *toy* is the following twisted lattice on $V = \mathbb{C}^2$ with $\mathrm{Tw} = \{1, \vartheta\}$: $W_1 = W_\vartheta = \mathbb{C}^2$ with the standard inner product, $\Theta_1 = \mathrm{id}$, $\Theta_\vartheta = \mathrm{diag}(p^{-1}, 1)$; the twist 1 is allowed at every prime and ϑ at every prime except r; $\Lambda_{1,\iota} = \Lambda_{\vartheta,\iota} = \mathcal{O}_\iota^2$ for every ι; $I = \{1, 2\}$, $b = \mathrm{id}$, $G = 1$. Let e_1, e_2 be the standard basis.

Date: November 26, 2026.

Problem 6.1.2. The toy is a twisted lattice. Its integral vectors are $M_\iota = p\mathcal{O}_\iota \oplus \mathcal{O}_\iota$ for $\iota \mid p$, and $M_\iota = \mathcal{O}_\iota^2$ for $\iota \mid \ell$, $\ell \neq p$.

For a linear map $u\colon U \to W$ between finite-dimensional inner product spaces, u^* is its adjoint, and $u \circ w$ is the family $u(w_1), u(w_2), \ldots$.

Problem 6.1.3. If $w_1, \ldots, w_n \in U$ and $n = \dim U$, then $\Gamma(u \circ w) = \det(u^* u)\, \Gamma(w)$.

The hypothesis $n = \dim U$ cannot be dropped.

Problem 6.1.4. In the toy, $\Gamma(\Theta_\vartheta e_1) = p^{-2}\, \Gamma(\Theta_1 e_1)$ and $\Gamma(\Theta_\vartheta e_2) = \Gamma(\Theta_1 e_2)$.

Let $Z(\vartheta) := \det(\Theta_\vartheta^* \Theta_\vartheta)$; in the toy $Z(1) = 1$ and $Z(\vartheta) = p^{-2}$. Write $\Gamma_\vartheta(w) := \Gamma(\Theta_\vartheta \circ w)$.

Problem 6.1.5. In the toy, let w_1, w_2 be a basis of $\mathbb{C}^2$ with $w_1, w_2 \in M_\iota$ for every $\iota \mid p$. Then $\Gamma_1(w) = p^2\, \Gamma_\vartheta(w)$, and $|\Gamma_1(w)|_\iota \leq p^{-2}$ for every $\iota \mid p$.

Problem 6.1.5 gives divisibility by p^2 at every $\iota \mid p$. Section 6.3 compares the gains from different choices of twist.

6.2. Index, covolume and the inequality

Fix a twisted lattice on V with twists Tw. Heights of families are those of Section 5.3. We use two facts from there: Problem 5.3.2, that the product of families of heights at most a and a' has height at most $a + a'$, and the m-th power of a family of height at most a has height at most ma for every integer $m \geq 0$; and the product formula for families, Theorem 5.3.1: if $z \in \mathbb{C}$, $z \neq 0$, the constant family z has height at most c, and $|\sigma z| \leq e^{c'}$ for every $\sigma \in \mathrm{Aut}(\mathbb{C})$, then

$$-c \leq c'.$$

Index and covolume are defined as in Section 5.4, with two changes: M_ι is now the module of vectors integral at ι for every allowed twist, and sizes are read through Θ_1, with the coordinates b and the matrix G of W_1. Thus $v_\sigma(y)$ is $b(\Theta_1 y)$ with σ applied to each coordinate, $N(y, \sigma) = v_\sigma(y)^* G\, v_\sigma(y)$, a real number ≥ 0 because G is positive definite as a complex matrix, so that the real part in Chapter 5 may be omitted, and y has covolume at most c if $|\det(v_\sigma(y_i)^* G\, v_\sigma(y_k))_{i,k}| \leq e^c$ for every σ. A family y has index at most δ if there is a function $e\colon \mathbb{N} \to \mathbb{R}$, nonnegative everywhere, with $\sum_{\ell \in U} e(\ell) \log \ell \leq \delta$ for every finite set U of primes, such that for every $\iota \mid \ell$ some $u \in M_n(\mathcal{O}_\iota)$ *carries y into M_ι with loss $e(\ell)$*: $\sum_k u_{ik} y_k \in M_\iota$ for every i, and $|\det u|_\iota \geq \ell^{-e(\ell)}$. The matrix may depend on ι but not on the twist. For the untwisted coordinates, the conjugate bound of Problem 5.4.8 holds for every twisted lattice, with the same proof: the modules $\Lambda_{\vartheta,\iota}$ play no role. If y has covolume at most c, then

$$|\sigma(\Gamma_1(y))| \leq e^c \quad \text{for every } \sigma \in \mathrm{Aut}(\mathbb{C}).$$

Let $y_1, \ldots, y_n$ and $z_1, \ldots, z_{n'}$ be vectors in V. In Problems 6.2.1–6.2.3, assume that V is a complex inner product space. Write $y \sqcup z$ for the family $y_1, \ldots, y_n, z_1, \ldots, z_{n'}$, and $|\gamma|^2$ for the complex number $\bar{\gamma}\gamma$.

Problem 6.2.1. Let ϑ be allowed at ℓ, let $\iota \mid \ell$, let $w_1, \ldots, w_m \in V$, and let $u, u' \in M_m(\mathbb{C})$ be such that $\sum_k u_{ik} \Theta_\vartheta w_k \in \Lambda_{\vartheta,\iota}$ and $\sum_k u'_{ik} \Theta_\vartheta w_k \in \Lambda_{\vartheta,\bar{\iota}}$ for every i. Then

$$|\det u'|_{\bar{\iota}}\, |\Gamma_\vartheta(w)|_\iota\, |\det u|_\iota \leq 1.$$

Problem 6.2.2. Let ϑ be allowed at ℓ, let $\iota \mid \ell$ and $a \in \mathbb{R}$. Suppose that $u \in M_n(\mathcal{O}_\iota)$ carries y into M_ι with loss a, that $u' \in M_n(\mathcal{O}_{\bar\iota})$ carries y into $M_{\bar\iota}$ with loss a, and that $\gamma \in \mathbb{C}$ satisfies $\gamma\,\Theta_\vartheta z_i \in \Lambda_{\vartheta,\iota} \cap \Lambda_{\vartheta,\bar\iota}$ for every i. Then

$$\left|(|\gamma|^2)^{n'}\,\Gamma_\vartheta(y \sqcup z)\right|_\iota \le \ell^{2a}.$$

Problem 6.2.3. Let y have index at most δ. For each $\iota \mid \ell$ let $\theta_\iota \in \mathrm{Tw}$ be allowed at ℓ and $\gamma_\iota \in \mathbb{C}$, with $\gamma_\iota\,\Theta_{\theta_\iota} z_i \in \Lambda_{\theta_\iota,\iota} \cap \Lambda_{\theta_\iota,\bar\iota}$ for every i. Then the family $\iota \mapsto (|\gamma_\iota|^2)^{n'}\,\Gamma_{\theta_\iota}(y \sqcup z)$ has height at most 2δ.

Problem 6.2.4. If y has covolume at most c, and $N(z_i, \sigma) \le e^h$ for every i and every $\sigma \in \mathrm{Aut}(\mathbb{C})$, then $y \sqcup z$ has covolume at most $c + n'h$.

Now let V be a finite-dimensional complex inner product space. For $\vartheta \in \mathrm{Tw}$ let $Z(\vartheta)$ be the square of the absolute value of the determinant of Θ_ϑ, as a map $V \to \Theta_\vartheta(V)$, in orthonormal bases, when Θ_ϑ is injective, and $Z(\vartheta) := 0$ otherwise. When W_ϑ is finite-dimensional, $Z(\vartheta) = \det(\Theta_\vartheta^*\Theta_\vartheta)$, as in Section 6.1.

Problem 6.2.5. Let all Θ_ϑ be injective, let $y \sqcup z$ be a basis of V, and let $\gamma \in \mathbb{C}$, $\gamma \ne 0$. Then $\Gamma_1(y \sqcup z) \ne 0$, and for every $\vartheta \in \mathrm{Tw}$

$$\Gamma_1(y \sqcup z) = (|\gamma|^2)^{n'}\,\Gamma_\vartheta(y \sqcup z) \cdot (|\gamma|^{-2})^{n'} \cdot \frac{Z(1)}{Z(\vartheta)}.$$

Problems 6.2.3, 6.2.4 and 6.2.5, together with the height bounds and the product formula of Chapter 5, give the following theorem.

Theorem 6.2.1. *Let V be a finite-dimensional complex inner product space,* Tw *a set with a distinguished element* 1*, and L a twisted lattice on V with twists* Tw *whose maps Θ_ϑ are all injective. Let $y_1, \dots, y_n, z_1, \dots, z_{n'} \in V$ be linearly independent, with $\dim V = n + n'$. For each $\iota \mid \ell$, for every prime ℓ, let $\theta_\iota \in \mathrm{Tw}$ be allowed at ℓ. Let $c, \delta, c_{\mathrm{vol}}, c_{\mathrm{short}}, c_{\mathrm{den}} \in \mathbb{R}$, and suppose that y has covolume at most c and index at most δ. Let $\gamma\colon \mathrm{Tw} \to \mathbb{C}$ with $\gamma(\vartheta) \ne 0$ for every ϑ, and suppose that*

1. *$\gamma(\vartheta)\,\Theta_\vartheta z_i \in \Lambda_{\vartheta,\iota}$ for every i, every $\iota \mid \ell$ for every prime ℓ, and every ϑ allowed at ℓ;*
2. *$N(z_i, \sigma) \le e^{c_{\mathrm{short}}}$ for every i and every $\sigma \in \mathrm{Aut}(\mathbb{C})$;*
3. *the family $\iota \mapsto (|\gamma(\theta_\iota)|^2)^{-1}$ has height at most c_{den};*
4. *the family $\iota \mapsto Z(1)/Z(\theta_\iota)$ has height at most c_{vol}.*

Then

$$0 \le c + 2\delta + n'(c_{\mathrm{short}} + c_{\mathrm{den}}) + c_{\mathrm{vol}}.$$

Hypothesis (1) concerns every twist allowed at ℓ, including θ_ι when it differs from $\theta_{\bar\iota}$. To recover Theorem 5.4.3, give V the inner product in which its given basis y is orthonormal, and take $\mathrm{Tw} = \{1\}$, with 1 allowed at every prime, $n' = 0$, $\gamma = 1$ and $c_{\mathrm{short}} = c_{\mathrm{den}} = c_{\mathrm{vol}} = 0$.

In the Lean formalization. In the Lean proof [GL] (file `grh/src/New/Reduction/Lattices/TwistedLattice.lean`), a twisted lattice is `New.TwistedLattice`; the integral vectors, carrying with loss, index, covolume, $N(y,\sigma)$ and $Z(\vartheta)$ are `integralVectors`, `New.PrimePadicIso.Carries`, `IndexLe`, `CovolumeLe`, `normSqAt` and `volume`. Admissibility is tested only at primes. The function e is nonnegative on all of $\mathbb{N}$, and only its prime values occur in the sums and the carrying bounds. Theorem 6.2.1 is `New.TwistedLattice.covolume_add_index_nonneg`, whose `b_volume`, `b_short`, `b_denom` are $c_{\mathrm{vol}}, c_{\mathrm{short}}, c_{\mathrm{den}}$.

6.3. A twist for each prime

We first test Theorem 6.2.1 on the toy, then add a twist that is allowed at r.

Problem 6.3.1. In the toy, let $k \in \mathbb{Z}$ and $s \geq 1$ an integer, and take $n = n' = 1$, $y_1 = p^k e_1$, $z_1 = s^{-1} e_2$, $\gamma(1) = \gamma(\vartheta) = s$, $\theta_\iota = \vartheta$ for $\iota \mid \ell$ with $\ell \neq r$, and $\theta_\iota = 1$ for $\iota \mid r$. The hypotheses of Theorem 6.2.1 hold with

$$c = 2k \log p, \quad \delta = \max(1-k, 0) \log p, \quad c_{\mathrm{short}} = -2 \log s, \quad c_{\mathrm{den}} = 2 \log s, \quad c_{\mathrm{vol}} = -2 \log p,$$

and then $c + 2\delta + n'(c_{\mathrm{short}} + c_{\mathrm{den}}) + c_{\mathrm{vol}} = 2 \max(k-1, 0) \log p$. For $p = 3$, $k = -1$, $s = 2$: $c = -2 \log 3$ and $\delta = 2 \log 3$. For the constant choice $\theta_\iota = 1$, with the same c_{short} and c_{den}, the theorem gives only $c + 2\delta \geq 0$.

The *second toy* adds to the toy a twist ϑ': $\mathrm{Tw} = \{1, \vartheta, \vartheta'\}$, $W_{\vartheta'} = \mathbb{C}^2$, $\Theta_{\vartheta'} = \mathrm{diag}(1, r^{-1})$, $\Lambda_{\vartheta', \iota} = \mathcal{O}_\iota^2$, and ϑ' is allowed at every prime except p.

Problem 6.3.2. The second toy is a twisted lattice, with $M_\iota = p\mathcal{O}_\iota \oplus \mathcal{O}_\iota$ for $\iota \mid p$, $M_\iota = \mathcal{O}_\iota \oplus r\mathcal{O}_\iota$ for $\iota \mid r$, and $M_\iota = \mathcal{O}_\iota^2$ otherwise. For $y = (pe_1, re_2)$, $n' = 0$, $\theta_\iota = \vartheta$ for $\iota \mid p$, $\theta_\iota = \vartheta'$ for $\iota \mid r$, and $\theta_\iota = 1$ otherwise, the hypotheses of Theorem 6.2.1 hold with $\gamma = 1$, $c_{\mathrm{short}} = c_{\mathrm{den}} = 0$, $c = 2 \log(pr)$, $\delta = 0$ and $c_{\mathrm{vol}} = -2 \log(pr)$, and the inequality is an equality.

Problem 6.3.3. In the second toy, suppose that $\theta_\iota \in \{1, \vartheta\}$ for every ι. If $\iota \mapsto Z(1)/Z(\theta_\iota)$ has height at most c'', then $c'' \geq -2 \log p$. The same holds with ϑ' and r in place of ϑ and p.

So for y as in Problem 6.3.2, a choice of twists with values in $\{1, \vartheta\}$ or in $\{1, \vartheta'\}$ yields through Theorem 6.2.1 at most $c \geq 2 \log p$ or $c \geq 2 \log r$, while the choice that depends on the prime yields $c \geq 2 \log(pr)$, which is attained.

Under the other hypotheses of Theorem 6.2.1, a height bound of $-A$ for $\iota \mapsto Z(1)/Z(\theta_\iota)$ gives $c + 2\delta \geq A - n'(c_{\mathrm{short}} + c_{\mathrm{den}})$. The proof of Theorem C (Chapter 54) contains the sole application of Theorem 6.2.1. There V is the space T of target forms, and Tw is the set of m-fold twists. A twist ϑ with modulus Q_ϑ is allowed at ℓ when ℓ is prime to $\mathrm{Nm}\, Q_\vartheta$. Its volume $Z(\vartheta)$ is the Gram determinant of the images of an orthonormal basis under the chain of lifts (Chapter 55). The height of $\iota \mapsto Z(1)/Z(\theta_\iota)$ is bounded by combining the bounds for the single lifts of Chapter 60 with a height bound for the inverse scalar in the chain factorization of Chapter 55. The vectors z_i are chosen from the auxiliary forms of Section 55.5 to complete y to a basis, and each $\gamma(\vartheta)\Theta_\vartheta z_i$ is integral at every ι at which ϑ is allowed.

Hints

6.1.1: Problem 5.3.1.
6.1.2: Problem 5.4.1 for the pairing condition. At p the twist ϑ is allowed; elsewhere p is a unit.
6.1.3: Write $\Gamma(w) = |\det P|^2$ with P the matrix of w in an orthonormal basis.
6.1.5: Problem 6.1.3; for $\Gamma_\vartheta(w)$, the pairing condition at ι and $\bar{\iota}$.
6.2.1: Form the matrix of pairings of the rows formed with u' against those formed with u, in that order.
6.2.2: Block diagonal matrices.
6.2.3: Take the multiplier 1. The index gives matrices at ι and at $\bar{\iota}$, which lie above the same prime.

6.2.4: Fischer's inequality, then Hadamard's.
6.2.5: Problem 6.1.3 with target $\Theta_\vartheta(V)$ and its induced inner product.
6.3.1: Problem 6.1.2 for the index. For c_{vol} take $H = p^{-2}$.
6.3.2: For c_{vol} take $H = (pr)^{-2}$.
6.3.3: Compare with the constant family p^2 at every ι.

References

[GL] L. Sernau, *GRH for Dirichlet L-functions, in Lean 4*, a shorter rewriting of the Lean proof, text by Claude, `https://github.com/lsernau/grh-lean`, commit `72fead1`, readable edition `grh/`.

[HJ] R. A. Horn and C. R. Johnson, *Matrix Analysis*, 2nd ed., Cambridge University Press, 2013.

STEPANOV WITHOUT MULTIPLICITY: A DETERMINANT AGAINST SIEGEL ZEROS

Prerequisites. Fermat's little theorem, Euler's criterion, Legendre's formula for $\operatorname{ord}_p n!$, Stirling's formula, the Euler–Maclaurin formula, Mertens' estimate $\sum_{p\le x}\log p/p = \log x + O(1)$, and Chebyshev's bound $\theta(N) := \sum_{p\le N}\log p \le N\log 4$. Quadratic fields and the Kronecker symbol χ_D; every primitive real character is a χ_D [Dav, Ch. 5]. Section 7.2 uses Section 5.2 of Chapter 5. We follow [N, §§2–8, App. D]. Section 7.4 uses the function G of (1) in Chapter 1. Sections 7.4–7.5 point ahead to Sections 8.1–8.5 of the next chapter, Chapter 8, but use nothing from it.

7.1. Chebyshev's determinant

How much can the size and divisibility of one integer say about primes? For $N \ge 2$ let $V_N := \det(u^a)_{1\le u\le N,\,0\le a<N} = \prod_{1\le i<j\le N}(j-i)$.

Problem 7.1.1. $V_N = \prod_{a<N} a!$, and $\log V_N \le \frac{1}{2}N(N-1)\log N$.

Problem 7.1.2. $\operatorname{ord}_p V_N \ge \sum_{a<N}\lfloor a/p\rfloor \ge N^2/(2p) - N/2$. For $N = 4$, $p = 2$ the first inequality is an equality.

Problem 7.1.3. $\sum_{p\le N}\log p/p \le \log N + 2$.

Each prime is seen through the single congruence $u^p \equiv u \pmod p$, once for each complete block of p exponents. This proof is given in [N, App. A], which credits the observation to Pascadi and to Tao [Tao].

7.2. The Frobenius graph

Let D be a fundamental discriminant, $F := \mathbb{Q}(\sqrt{D}) \subset \mathbb{C}$, σ the nontrivial automorphism, and $\mathcal{O}_F = \mathbb{Z}[\omega]$ with $\omega = (1+\sqrt{D})/2$ or $\sqrt{D}/2$. We want $\sum_{p\le t,\,\chi_D(p)=-1}\log p/p \le (\frac{1}{2}+o(1))\log t$.

Problem 7.2.1. If p is odd and $\chi_D(p) = -1$, then $u^p \equiv \sigma(u) \pmod{p\mathcal{O}_F}$ for all $u \in \mathcal{O}_F$. For instance, $(1+i)^3 \equiv 1-i \pmod 3$.

So modulo such p the points $(u,\sigma(u))$ lie on the graph $Y = X^p$. This is all that Section 5.2 of Chapter 5 used about $\mathbb{Z}[i]$, and we now run that section with $\mathbb{Z}[i]$, $\bar{u}$ and the primes $p \equiv 3 \pmod 4$ replaced by $\mathcal{O}_F$, $\sigma(u)$ and the odd primes p with $\chi_D(p) = -1$. For integers $t \ge 2$, $H \ge 1$ let $\mathcal{T} := \{(a,b) \in \mathbb{Z}^2_{\ge 0} : a + Hb < t\}$, $T := |\mathcal{T}|$, $A := \sum_{\mathcal{T}} a$.

Problem 7.2.2. Problem 5.2.2 holds in this setting: if p is odd, $\chi_D(p) = -1$, $f \in \mathcal{O}_F[X,Y]$ and $u \in \mathcal{O}_F$, then $\big(\partial_X^j((X^p-Y)^k f)\big)(u,\sigma(u)) \in p^k\mathcal{O}_F$ for all $j,k \ge 0$.

Let $u_1,\dots,u_I \in \mathcal{O}_F$, $J \ge 1$, and let M be the $IJ \times T$ matrix with entries $(\partial_X^j X^a Y^b)(u_i,\sigma(u_i))$, $0 \le j < J$. Let P_H be the set of odd $p \ge H$ with $\chi_D(p) = -1$, and $k_p := \sum_{\mathcal{T}}\lfloor a/p\rfloor$.

Date: November 25, 2026.

Problem 7.2.3. For $p \in P_H$, the set $\mathcal{T}$ satisfies the hypothesis of Problem 5.2.3, and every $T \times T$ minor of M lies in $p^{k_p}\mathcal{O}_F$.

Problem 7.2.4. Let $|u_i|, |\sigma(u_i)| \le B$ with $B \ge 1$, and let δ be a nonzero $T \times T$ minor. Then $\delta\sigma(\delta)$ is a nonzero integer divisible by p^{2k_p} for $p \in P_H$, and $|\delta|, |\sigma(\delta)| \le T^T t^{T(J-1)} B^{\sum_{\mathcal{T}}(a+b)}$.

Problems 7.2.1–7.2.4 prove the following, which for $\mathbb{Z}[i]$ also follows from Theorem 5.2.1.

Theorem 7.2.1. *If $|u_i|, |\sigma(u_i)| \le B$, $B \ge 1$, and M has rank T, then*

$$\sum_{p \in P_H} k_p \log p \le \Big(\sum_{\mathcal{T}} (a+b)\Big) \log B + T \log T + T(J-1)\log t. \tag{1}$$

Problem 7.2.5. If $I \ge |D|$, there are I distinct $u \in \mathcal{O}_F$ with $|u|, |\sigma(u)| \le 4I^{1/2}|D|^{1/4}$.

7.3. Density one half

Without derivatives, (1) gives nothing in a quadratic field [N, Ex. 24].

Problem 7.3.1. Distinct $u_i \in \mathcal{O}_F$ with $|u_i|, |\sigma(u_i)| \le B$ number at most $25B^2$. Hence if $J = 1$ and M has rank T, then $\log B \ge \log t - \frac{1}{2}\log H - 3$.

So for $J = 1$ the bound from (1) for $\sum_{H \le p \le t,\, \chi_D(p) = -1} \log p/p$ is at least $\log t - \frac{1}{2}\log H - 3$, worse than Mertens' $\log(t/H) + O(1)$. Derivatives let I be about T/J [Gr]. The interpolation input, by a Wronskian argument that [Ko, proof of Thm. 1] and [N, Lemma 17] credit to Barreto: if the u_i are distinct, $I = 2t$ and $J = 2\lfloor (t-1)/H \rfloor + 1$, then M has rank T. For $t \ge 6$, $1 \le H \le t/2$ one has $T \le t^2/H$, $A \ge t^3/(8H)$ and $\sum_{\mathcal{T}} b \le 8A/H$.

Problem 7.3.2. Under the hypotheses of Theorem 7.2.1, with $t \ge 6$ and $H \le t/2$, $\sum_{p \in P_H,\, p \le t} \log p/p \le (1 + 8/H)\log B + (8/t)\big(\log T + (J-1)\log t\big) + 16$.

Problem 7.3.3. For $t \ge \max(16, |D|/2)$, $H = \lceil \log t \rceil$, $I = 2t$, $J = 2\lfloor (t-1)/H \rfloor + 1$ and the points of Problem 7.2.5,

$$\sum_{p \le t,\ \chi_D(p) = -1} \frac{\log p}{p} \le \frac{1}{2}\log t + \frac{1}{4}\log|D| + \log\log(3t) + 50.$$

A primitive real χ of conductor q has no real zero in $(1 - c/\log 2q, 1)$, with c effective and depending only on κ, B_0, provided $\sum_{p \le x,\, \chi(p) = -1} \log p/p \le \kappa \log x + B_0 \log 2q$ for all $x \ge 2$ and some $\kappa < 1$ [N, Lemma 2, App. F].

Problem 7.3.4. Problems 7.1.3 and 7.3.3 give this with $\kappa = \frac{3}{4}$, $B_0 = 30$.

Thus we have proved the following.

Theorem 7.3.1. *There is an effective absolute $c > 0$ such that $L(s, \chi) \ne 0$ for real $s > 1 - c/\log(2q)$, for every primitive real character χ of conductor q.*

This was first proved in [OAI], with three variables in a biquadratic field; the proof here follows [Gr] and [N].

7.4. One congruence per block

Alpöge called this argument "Stepanov without multiplicity" [Alp, p. 2]. What does it lose? For V_N both sides are exact. Let r_n be the remainder of N modulo n, and $W(N) := \sum_{n \le N} \Lambda(n)\, r_n(n - r_n)/(2n)$.

Problem 7.4.1. $\sum_{a<N} \lfloor a/n \rfloor = \frac{N}{2}\big(\frac{N}{n} - 1\big) + \frac{r_n(n-r_n)}{2n}$. Hence $\log V_N = \frac{N}{2}\sum_{n \le N} \Lambda(n)\big(\frac{N}{n} - 1\big) + W(N)$, with $0 \le W(N) \le N\psi(N)/8$, where $\psi(N) := \sum_{n \le N} \Lambda(n)$.

Problem 7.4.2. For G as in (1) of Chapter 1, $G(N) = (\gamma - \frac{1}{2})N - 2W(N)/N + O(1)$. In particular $G(N) \le (\gamma - \frac{1}{2})N + O(1)$.

For $N = 10^4$, $G(N) = 1.749\ldots$ while $(\gamma - \frac{1}{2})N = 772.15\ldots$. The determinant gives a one-sided bound for G with error of order N, and nothing more: the rest is the sawtooth sum $W(N)$. In Section 7.2 the floors $\lfloor a/p \rfloor$ cost the constant 16 of Problem 7.3.2 in the same way. An error $O(1)$ in $\sum \log p/p$ is Chebyshev strength. It suffices for Theorem 7.3.1, where a real zero would change the main term by a constant factor. It is far from $G(x) \le x^{1/2+\varepsilon}$, which the Riemann hypothesis needs. One determinant is a chain of length $m = 1$ in Problem 8.5.1.

7.5. Multiplicity in Bombieri's form

Stepanov's polynomial vanishes to order about $\sqrt{q}$ (Theorem 8.3.1); order one gives nothing (Problem 8.1.4). Bombieri gets multiplicity from a power of Frobenius [Bom74], [N, App. D].

Let k be a finite field of odd characteristic, $f \in k[X]$ of degree $d = 2g + 1$, $g \ge 1$, and $R := k[x, y]$ with $y^2 = f(x)$. For $\phi = a(x) + b(x)y$ let $\lambda(\phi) := \deg(a^2 - b^2 f)$, and $R_\ell := \{\phi : \lambda(\phi) \le \ell\}$.

Problem 7.5.1. $\lambda(a + by) = \max(2 \deg a, 2 \deg b + d)$ and $\lambda(\phi\psi) = \lambda(\phi) + \lambda(\psi)$; $\dim_k R_\ell = \ell + 1 - g$ for $\ell \ge 2g$.

Problem 7.5.2. A nonzero $\phi \in R$ vanishes at no more than $\lambda(\phi)$ points (ξ, η) over a finite extension of k.

Let Q be a power of $|k|$, and N the number of $(\xi, \eta) \in \mathbb{F}_{Q^2}^2$ with $\eta^2 = f(\xi)$. Let $2g \le \ell_1 < Q$, $\ell_2 \ge 2g$, and (x_i), (y_j) bases of R_{ℓ_1}, R_{ℓ_2} with distinct λ. For $c_{ij} \in k$ let $f_c := \sum c_{ij} x_i y_j^Q$ and $\tilde{f}_c := \sum c_{ij} x_i^Q y_j$.

Problem 7.5.3. If $c \ne 0$ and $\tilde{f}_c = 0$, then $f_c \ne 0$, f_c vanishes at all N points, and $N \le \ell_1 + Q\ell_2$.

Problem 7.5.4. Such c exists for $\ell_1 = Q - 1$, $\ell_2 = Q + 2g$ if $Q > (g + 1)^2$. Hence $N \le Q^2 + (2g + 1)Q - 1$.

For $f = X^3 - X$ over $\mathbb{F}_3$ and $Q = 27$, $N = 783$ and the bound is 809. The function f_c^Q vanishes to order at least Q at each of these points, for free, because $(\sum c\phi)^Q = \sum c^Q \phi^Q$, $c^Q = c$, and all points share the Frobenius $\xi \mapsto \xi^{Q^2}$.

Problem 7.5.5. $(X+Y)^p - X^p - Y^p \in p\mathbb{Z}[X, Y] \setminus p^2\mathbb{Z}[X, Y]$. The primes $p < 4000$ with $2^p \equiv 2 \pmod{p^2}$ are 1093 and 3511.

Over $\mathbb{Z}$ the p-th power is additive and fixes integers only modulo p, and p varies. The determinant of Section 7.2 is nonzero by interpolation, handles all $p \geq H$ because $\mathcal{T}$ is stable under $X^p \mapsto Y$, and sees p because $X^p - Y$ vanishes at $(u, \sigma u)$ to first order modulo p. In the proof the multiplicity returns through a chain of m maps (Theorem 8.4.1 of the next chapter), and the budget $x/m+m$ of Problem 8.5.2 balances at $m \approx \sqrt{x}$, as ℓ and Q do above.

Hints

§7.1.

7.1.2: Use $u^p \equiv u \pmod p$ to change the columns by a unitriangular matrix. For the second inequality, split $[0, N)$ into blocks of length p.

7.1.3: Sum Problem 7.1.2 over $p \leq N$ with weight $\log p$, and use Chebyshev's bound.

§7.2.

7.2.1: Write $2u = x + y\sqrt{D}$ and use Euler's criterion for $D^{(p-1)/2}$.

7.2.2: Problem 7.2.1 and the Leibniz rule, as for Problem 5.2.2.

7.2.3: $p \geq H$. Then the proof of Problem 5.2.3, with Problem 7.2.2.

7.2.5: Take $x + y\omega$ in a box with $|x| \approx |y|\sqrt{|D|}$; note $|\omega|, |\sigma\omega| \leq \sqrt{|D|}$.

§7.3.

7.3.1: Count the possible values of $u + \sigma u$ and $(u - \sigma u)/\sqrt{D}$. For the second claim compare T with I.

7.3.2: $\lfloor a/p \rfloor \geq a/p - 1$, and $\theta(t) \leq 2t$.

7.3.3: Insert Problem 7.2.5 into Problem 7.3.2, and treat the primes below H by Problem 7.1.3.

7.3.4: Absorb $\log\log(3t)$ into $\frac{1}{4}\log t$ plus a constant.

§7.4.

7.4.1: Split $[0, N)$ into blocks of length n. Then $\log a! = \sum_n \Lambda(n)\lfloor a/n \rfloor$.

7.4.2: Show $\frac{2}{N}\log V_N = N\log N - \frac{3}{2}N + O(1)$ by Stirling and Euler–Maclaurin.

§7.5.

7.5.1: Parity of $2\deg a$ and $2\deg b + d$; $a^2 - b^2 f$ is ϕ times its conjugate.

7.5.2: Count the roots of $a^2 - b^2 f$ with multiplicity.

7.5.3: The $\lambda(x_i y_j^Q)$ are distinct. At the points, $f_c^Q = \sum c\, x_i^Q y_j^{Q^2}$ takes the value of $\tilde{f}_c$.

7.5.4: $\tilde{f}_c \in R_{Q\ell_1+\ell_2}$; compare dimensions.

7.5.5: The coefficient of $X^{p-1}Y$ is p.

References

[Alp] L. Alpöge, untitled note announcing a proof of the Riemann hypothesis, 20 November 2026, `https://alpo.ge/remark.pdf`.

[Bom74] E. Bombieri, *Counting points on curves over finite fields (d'après S. A. Stepanov)*, Séminaire Bourbaki, Exp. 430, Lecture Notes in Math. **383**, Springer, 1974, 234–241.

[Dav] H. Davenport, *Multiplicative Number Theory*, 3rd ed., revised by H. L. Montgomery, Grad. Texts in Math. **74**, Springer, 2000.

[Gr] B. Green, *On Landau–Siegel zeros*, Hexagon preprint hexagon:2610.00311v2, 2026, `https://hexagonmath.org/2610.00311v2`.

[Ko] S. D. Kominers, *Small algebraic integers and Frobenius prime sums*, Hexagon preprint hexagon:2610.00451v1, 2026, https://hexagonmath.org/2610.00451v1.

[N] P. D. Nelson, *Some notes on recent results on Landau–Siegel zeros*, note, 2026, https://ultronozm.github.io/math/20261020T163023--siegel-zeros.html.

[OAI] OpenAI, *Uniform exclusion of Landau–Siegel zeros*, OpenAI Math Release preprint, 1 October 2026, https://github.com/openai/math/blob/main/preprints/Uniform-exclusion-of-Landau-Siegel-zeros-October-1-2026/paper.pdf.

[Tao] T. Tao, *A sketch of the proof of non-existence of Siegel zeroes*, What's new, 19 October 2026, https://terrytao.wordpress.com/2026/10/19/a-sketch-of-the-proof-of-non-existence-of-siegel-zeroes/.

THE CHAIN AND THE SQUARE ROOT

Prerequisites. Finite fields and Euler's criterion; polynomials over a field, their roots and multiplicities; a homogeneous linear system with more unknowns than equations has a nonzero solution. Lattices in a Euclidean space and their covolumes [Ne, Ch. I, §4]; the adjoint of a linear map between inner product spaces. The von Mangoldt function Λ and Mertens' estimate $\sum_{n\le x}\Lambda(n)/n = \log x + O(1)$. The problems in Sections 8.1–8.4 require no earlier chapter; Chapter 7, *Stepanov without multiplicity*, is their motivation: one determinant, without multiplicity, is the case $m = 1$ of the chain. Section 8.5 uses the function G of (1) and Theorem 1.2.1 of Chapter 1. The closing paragraphs of Sections 8.4 and 8.5 point to Chapters 6, 33, 55 and 35; Problem 8.5.5 states what it needs as hypotheses.

8.1. The auxiliary polynomial

How can a polynomial show that a set of about $q/2$ elements of $\mathbb{F}_q$ has at most $q/2+O(\sqrt{q})$ elements? Stepanov's answer [Ste69] is to make it vanish to high order on the set. We follow his method for the curve $y^2 = f(x)$.

Let q be a power of an odd prime p, and let $f \in \mathbb{F}_q[X]$ have odd degree $d = 2g+1$ with $3 \le d < q$. Let

$$c := \frac{q-1}{2}, \qquad D := \frac{q-d}{2}.$$

For $\eta \in \{1,-1\}$ let $S_\eta := \{x \in \mathbb{F}_q : f(x)^c = \eta\}$, let $S_0 := \{x \in \mathbb{F}_q : f(x) = 0\}$, and let N^{aff} be the number of solutions $(x,y) \in \mathbb{F}_q^2$ of $y^2 = f(x)$.

Problem 8.1.1. $\mathbb{F}_q$ is the disjoint union of S_1, S_{-1} and S_0, and $N^{\mathrm{aff}} = 2|S_1|+|S_0|$. For $q = 7$ and $f = X^3 - X$, $S_1 = \{4,5\}$, $S_{-1} = \{2,3\}$ and $N^{\mathrm{aff}} = 7$.

Hence $N^{\mathrm{aff}} - q = |S_1| - |S_{-1}|$, and a bound $|S_\eta| \le q/2 + B$ for both signs gives $|N^{\mathrm{aff}}-q| \le 2B+d$. For squarefree f, Weil's theorem [Wei48] gives $|N^{\mathrm{aff}}-q| \le 2g\sqrt{q}$.

The principle is the count of zeros against the degree: if $F \in \mathbb{F}_q[X]$ is nonzero and vanishes to order at least ℓ at every point of S_η, then

$$\ell\,|S_\eta| \le \deg F. \tag{1}$$

The polynomials $f^c-\eta$ and X^q-X vanish on S_η, and give $|S_\eta| \le dc$ and $|S_\eta| \le q$. To reach $q/2$ one needs $\deg F/\ell$ close to $q/2$. Stepanov combines the two polynomials. Let $J \ge 1$ be an integer, and let $r_j, s_j \in \mathbb{F}_q[X]$, for $0 \le j < J$, have degree less than D and be not all zero. The *auxiliary polynomial* is

$$F := \sum_{j<J} \bigl(r_j + s_j f^c\bigr) X^{jq}. \tag{2}$$

Problem 8.1.2. $\deg f^c = gq + D$, and $2D < q$.

Problem 8.1.3. The nonzero terms $r_j X^{jq}$ and $s_j f^c X^{jq}$ of (2) have pairwise distinct degrees. Hence $F \ne 0$ and $\deg F \le (J+g)q - d - 1$.

Date: November 26, 2026.

For $x \in S_\eta$ we have $x^{jq} = x^j$ and $f(x)^c = \eta$, so $F(x) = C_0(x)$, where

$$C_0 := \sum_{j<J} (r_j + \eta s_j) X^j.$$

If $C_0 = 0$, then F vanishes on all of S_η.

Problem 8.1.4. If $C_0 = 0$, then $\deg F \geq q$. If $D \geq 2$ and $J \geq 2$, the tuple $r_0 = -X$, $r_1 = 1$, all others zero, gives $F = X^q - X$.

So the gain must come from the order of vanishing.

8.2. Vanishing to order ℓ

In characteristic p the derivative of order p vanishes identically, so one uses Hasse derivatives. For $G \in \mathbb{F}_q[X]$ define $H^k G \in \mathbb{F}_q[X]$ by

$$G(X+Y) = \sum_{k \geq 0} (H^k G)(X)\, Y^k \qquad \text{in } \mathbb{F}_q[X,Y].$$

Problem 8.2.1. For $0 \leq k \leq n$, $H^k(X^n) = \binom{n}{k} X^{n-k}$, and $H^k(X^n) = 0$ for $k > n$. Also $H^k(G_1 G_2) = \sum_{i \leq k} H^i G_1 \cdot H^{k-i} G_2$. For $\alpha \in \mathbb{F}_q$, $(X-\alpha)^\ell$ divides G if and only if $(H^k G)(\alpha) = 0$ for all $k < \ell$.

Problem 8.2.2. $(X+Y)^{jq} = (X^q + Y^q)^j$. Hence $H^k(GX^{jq}) = (H^k G) X^{jq}$ for $k < q$.

To differentiate f^c, write $f(X+Y)^c = f(X)^c \big(f(X+Y)/f(X)\big)^c$ and define $U_i \in \mathbb{F}_q(X)$ by

$$\Big(\frac{f(X+Y)}{f(X)}\Big)^c = \sum_{i \geq 0} \frac{U_i}{f^i}\, Y^i \qquad \text{in } \mathbb{F}_q(X)[[Y]].$$

Problem 8.2.3. Each U_i is a polynomial of degree at most $i(d-1)$. Moreover $U_0 = 1$ and $U_1 = cf'$.

For $k \geq 0$ let

$$C_k := \sum_{j<J} \Big(f^k H^k r_j + \eta \sum_{i \leq k} f^{k-i} U_i\, H^{k-i} s_j \Big) X^j. \tag{3}$$

For $k = 0$ this is the polynomial C_0 of Section 8.1.

Problem 8.2.4. Let $\alpha \in S_\eta$, so that $f(\alpha) \neq 0$, and let $k < q$. Then $(H^k F)(\alpha) = f(\alpha)^{-k} C_k(\alpha)$.

Problem 8.2.5. $\deg C_k \leq D + J - 2 + k(d-1)$.

By Problems 8.2.1 and 8.2.4, if $\ell \leq q$ and

$$C_0 = C_1 = \cdots = C_{\ell-1} = 0, \tag{4}$$

then F vanishes to order at least ℓ at every point of S_η, whatever S_η is.

8.3. The count and the balance

Problem 8.3.1. If $2JD > \ell(D+J-1)+(d-1)\ell(\ell-1)/2$, then there is an auxiliary polynomial (2) satisfying (4).

Problem 8.3.2. Let ℓ be an even integer with $0 \le \ell < q-d$, and let $J = \ell/2 + t$. Then

$$2JD - \ell(D+J-1) - (d-1)\frac{\ell(\ell-1)}{2} = t\,(q-d-\ell) - \frac{d\ell^2 - (d+1)\ell}{2}.$$

Hence the hypothesis of Problem 8.3.1 holds if $t > d\ell^2/\big(2(q-d-\ell)\big)$.

The preceding problems give the following estimate.

Theorem 8.3.1 (A bound by Stepanov's method)**.** *Let ℓ be even with $2 \le \ell < q-d$, and let $t := \lfloor d\ell^2/(2(q-d-\ell))\rfloor + 1$. Then, for $\eta = \pm 1$,*

$$|S_\eta| \le \frac{q}{2} + \frac{(g+t)\,q}{\ell}.$$

This is Stepanov's method [Ste69]; see [Sch76] for Hasse derivatives. For example, for $q = 1009$, $d = 3$ and $\ell = 24$ one has $t = 1$, and the bound is $588.58\ldots$; for $f = X^3 + X + 1$ the sets have $|S_1| = 516$ and $|S_{-1}| = 492$.

Problem 8.3.3. If $q \ge 16d^2$ and ℓ is an even integer with $|\ell - \sqrt{q}| \le 1$, then $|S_\eta| \le q/2 + 2d\sqrt{q}$ for $\eta = \pm 1$, and $|N^{\mathrm{aff}} - q| \le 4d\sqrt{q} + d$.

Where does the square root come from? Write $(J+g)q - d - 1 = \frac{\ell}{2}q + \big((g+1)q - d - 1\big) + (t-1)q$. After division by ℓ the first term is the main term $q/2$. The second is paid once, however high the order. The third comes from the growing number of equations of the kth identity, through $t - 1 = \lfloor d\ell^2/(2(q-d-\ell))\rfloor$. For fixed d and $d + \ell \le q/2$ the error term is $O_d(q/\ell + \ell)$, of the shape $q/m + m$, and the two terms of this upper bound balance at ℓ of order $\sqrt{q}$.

Problem 8.3.4. For every ℓ as in Theorem 8.3.1, $(g+t)q/\ell > \sqrt{2gdq}$.

Thus the error term in Theorem 8.3.1 never gives $o(\sqrt{q})$. We expect the same for Bombieri's form [Bom74], but do not prove it here.

8.4. The chain inequality

What does a chain of m linear maps give that one map does not?

Let V and W be Euclidean spaces of the same dimension $n \ge 1$, with lattices $L \subset V$ and $M \subset W$ of rank n. The *volume* of a linear map $u\colon V \to W$ is $\det(u^*u)$, where u^* is the adjoint; in orthonormal bases it is $(\det u)^2$.

Problem 8.4.1. Let $u\colon V \to W$ be injective, and let $\lambda > 0$ be real with $u(L) \subseteq \lambda M$. Then

$$n \log \lambda \le \log \mathrm{covol}(L) - \log \mathrm{covol}(M) + \tfrac{1}{2}\log\det(u^*u).$$

For $L = M = \mathbb{Z}$, u the multiplication by 6 and $\lambda = 6$, both sides are $\log 6$.

Let $m \ge 1$ be an integer, and let $V_0, \ldots, V_m$ be Euclidean spaces of dimension n with lattices $L_j \subset V_j$ of rank n. Let $u_j\colon V_{j-1} \to V_j$ be linear maps and $\lambda_j > 0$ real numbers with $u_j(L_{j-1}) \subseteq \lambda_j L_j$, and let $\Psi := u_m \circ \cdots \circ u_1$.

Problem 8.4.2. $\det(\Psi^*\Psi) = \prod_{j=1}^m \det(u_j^* u_j)$, also when some u_j is not injective. The identity fails for spaces of different dimensions: for $u_1(x) = (x, 0)$ from $\mathbb{R}$ to $\mathbb{R}^2$ and $u_2(y, z) = y$ from $\mathbb{R}^2$ to $\mathbb{R}$ the left side is 1 and the right side is 0.

Problem 8.4.3. $\Psi(L_0) \subseteq \lambda_1 \cdots \lambda_m L_m$. In particular, if $u_j(L_{j-1}) \subseteq p^{e_j} L_j$ for each j, then $\Psi(L_0) \subseteq p^{e_1+\cdots+e_m} L_m$.

For the composite of the chain we have the following inequality; if Ψ is injective, then so is every u_j, because all dimensions are equal.

Theorem 8.4.1 (Chain inequality)**.** *If Ψ is injective, then*

$$n \sum_{j=1}^m \log \lambda_j \le \log \operatorname{covol}(L_0) - \log \operatorname{covol}(L_m) + \frac{1}{2} \sum_{j=1}^m \log \det(u_j^* u_j).$$

The right side uses the two ends and the volume of each step, and the ends are paid once: if Ψ is injective, $\log \lambda_j \ge \beta$ and $\frac{1}{2n} \log \det(u_j^* u_j) \le \sigma$ for every j, and $\frac{1}{n}(\log \operatorname{covol}(L_0) - \log \operatorname{covol}(L_m)) \le c_{\mathrm{end}}$, then $\beta \le \sigma + c_{\mathrm{end}}/m$.

Problem 8.4.4. Suppose that every u_j is injective. The sum of the inequalities of Problem 8.4.1 for $u_1, \dots, u_m$ and $\lambda_1, \dots, \lambda_m$ is the inequality of Theorem 8.4.1.

Measured by volumes, then, the intermediate lattices cost nothing. The product of the operator norms, by contrast, can strictly exceed the operator norm of the composite.

Problem 8.4.5. Let $w \ge 2$ be an integer, $L_0 = L_2 = \mathbb{Z}^2$ and $L_1 = \mathbb{Z}e_1 + \mathbb{Z}we_2$, all in $\mathbb{R}^2$ with the standard norm, and let $u_1(x, y) = (x, wy)$ and $u_2(x, y) = (x, y/w)$. Then $\lambda_1 = \lambda_2 = 1$ are the largest admissible scalars, $\det(u_1^* u_1) = w^2$, $\det(u_2^* u_2) = w^{-2}$, and the inequalities of Problem 8.4.1 for u_1, u_2 and of Theorem 8.4.1 are equalities. But $\|u_1\| \, \|u_2\| = w$, while Ψ is the identity.

A divisibility is often known only on a sublattice. Its index is a loss, paid once.

Problem 8.4.6. Suppose that Ψ is injective and that $\Psi(L_0') \subseteq \lambda L_m$ for a sublattice $L_0' \subseteq L_0$ of finite index and a real $\lambda > 0$. Then

$$n \log \lambda \le \log \operatorname{covol}(L_0) - \log \operatorname{covol}(L_m) + \frac{1}{2} \sum_{j=1}^m \log \det(u_j^* u_j) + \log [L_0 : L_0'].$$

Theorem 6.2.1 gives a related index and covolume inequality for a twisted lattice. For the chain of the proof, the determinant divided by its value at the trivial twist is the product of the corresponding quotients for the single lifts, times a correction factor (Theorem 55.4.1). This factor is a power of the norm of the modulus times a product of ratios of absolute values of partial Hecke L-values, all raised to the dimension of the target forms.

How precisely must the two ends and the volumes of the steps be known?

8.5. The budget $x/m + m$

How long should the chain be? Let $G(x) = \sum_{n \le x} \Lambda(n)(x/n - 1) - x \log x + (1 + \gamma)x$ be the function of (1) in Chapter 1. By Mertens' estimate, $G(x) = O(x)$. By Theorem 1.2.1, if $G(x) \le x^\theta$ for some $0 < \theta < 1$ and all large x, then $\zeta(s) \ne 0$ for $\operatorname{Re} s > \theta$. So a one-sided bound with exponent $\frac{1}{2}$ gives the Riemann hypothesis.

Let $a, b > 0$ and $x := a/b$. As in Section 1.3, $(a/p^e - b)_+ = b(x/p^e - 1)_+$, so that

$$\sum_p \log p \sum_{e\ge 1} \Big(\frac{a}{p^e} - b\Big)_+ = b \sum_{\nu \le x} \Lambda(\nu) \Big(\frac{x}{\nu} - 1\Big),$$

where $u_+ := \max(u, 0)$; for integral a the inner sum is a smoothed analogue of Legendre's sum $\sum_{e\ge 1} \lfloor a/p^e \rfloor$ for $v_p(a!)$. We consider a chain as in Section 8.4, with Ψ injective, and real numbers c_{end} and $c_1, \dots, c_m$ such that for $1 \le j \le m$

$$\begin{gathered} \log \lambda_j \ge b \sum_{\nu \le x} \Lambda(\nu) \Big(\frac{x}{\nu} - 1\Big), \qquad \frac{1}{2n} \log \det(u_j^* u_j) \le a(\log x - 1 - \gamma) + c_j, \\ \frac{1}{n} \big(\log \mathrm{covol}(L_0) - \log \mathrm{covol}(L_m)\big) \le c_{\mathrm{end}}. \end{gathered} \tag{5}$$

Here c_{end} is the cost at the ends, and c_j the cost of the jth step. This models the bookkeeping only.

Problem 8.5.1. Under (5), $G(x) \le (c_{\mathrm{end}} + c_1 + \cdots + c_m)/(mb)$.

Problem 8.5.2. If $c_{\mathrm{end}} = a$ and $c_j = (2j-1)b$, then $G(x) \le x/m + m$. With $m = \lceil \sqrt{x} \rceil$ this gives $G(x) \le 2\sqrt{x} + 1$. For $x = 10^6$ the bound is 2000 at $m = 1000$ and 10100 at $m = 100$.

What happens if the cost at the ends is paid separately for every step?

Problem 8.5.3. Retain the first two bounds of (5). Suppose that every u_j is injective and that Problem 8.4.1 is applied to each u_j separately, with $\frac{1}{n}(\log \mathrm{covol}(L_{j-1}) - \log \mathrm{covol}(L_j)) \le a$ for every j and $c_j = (2j-1)b$. Then the jth step gives $G(x) \le x + 2j - 1$, so the best of these bounds is $G(x) \le x + 1$, the bound for $m = 1$.

Problem 8.5.4. $\sum_{j=1}^m (3j^2 - 3j + 1) = m^3$. So if $c_{\mathrm{end}} = a$ and $c_j = (3j^2 - 3j + 1)b$, then $G(x) \le x/m + m^2$. For every $m > 0$, $x/m + m^2 \ge 3 \cdot 2^{-2/3} x^{2/3}$. For $x = 10^6$ the least value over integers m is $18899.2\ldots$, at $m = 79$.

If such chains exist for every sufficiently large x at a length minimizing the bound in Problem 8.5.4, that bound gives $G(x) \le x^\theta$ eventually for each $\theta > 2/3$, and hence a zero-free half-plane $\mathrm{Re}\, s > 2/3$ for ζ. The exponent is decided by how the total cost grows with the length of the chain.

The chain of the proof. This chapter serves the main inequality. Chapter 35 proves $m \cdot \mathrm{rem} \le f a \log^5 b$ (Theorem 35.2.1) and deduces a bound for $R_{d,q_0}(x)$. From here on f is the number of infinite places of the field E, $k = r + 1 - m$ is the rank of the source, and $U = f a \log^3 b$ is the unit of error, all as in Chapter 33 (they are not the polynomial f and the index k of Sections 8.1–8.3); the data have $\sqrt{x} \le m \le 2\sqrt{x}$. In the proof two estimates involve m through m^2 relative to their budgets. First, the level N is a prime with $m \log b \le \log N \le 30 m \log b$; the allowed loss at N is $2mfb$ (here $N \ge b > x_1$, so N is not a small non-split prime); and for every finite set of natural numbers the sum over its elements p of the allowed loss at p times $\log p$, with the summand at $p = 0$ defined to be zero, is at most U. Second, local defect bounds δ_p satisfy $\sum_{p \in T} \delta_p \log p \le C_{\mathrm{loc}} f (m/k) b \log b$ for every finite set T of primes, with $C_{\mathrm{loc}} = 4 \cdot 10^6 e^{180}$, while for each lift index the sum of the logarithmic denominator bounds over every finite set of primes must be at most $B = U/(mk)$.

Problem 8.5.5. Let $m, x, f, k > 0$, $b > 1$, $L := \log b$, $a := xb$ and $U := faL^3$. (a) If $mL \le \log N \le 30mL$, then $2m^2fbL \le 2mfb\log N \le 60m^2fbL$; hence $2mfb\log N \le U$ forces $m \le L\sqrt{x/2}$, and holds if $m \le L\sqrt{x/60}$. (b) For $C_{\mathrm{loc}} > 0$, $C_{\mathrm{loc}} f(m/k)bL \le U/(mk)$ if and only if $m \le L\sqrt{x/C_{\mathrm{loc}}}$.

The data have $\log\log b \ge 10^{12}C$, with $C \ge 1$ the constant of Chapter 33, so both comparisons of Problem 8.5.5 hold in the range $\sqrt{x} \le m \le 2\sqrt{x}$. Up to powers of $\log b$, the length has the same square-root scale as in Problem 8.5.2.

In the Lean formalization. In the Lean proof [GL] the main inequality is `New.star_inequality` (`grh/src/New/Reduction/MainInequality.lean`); the allowed loss is `New.Data.allowedLoss`, and the estimates used in the discussion of Problem 8.5.5 are `New.Data.log_N_mem_Icc`, `New.Data.sum_allowedLoss_mul_log_le`, `New.Selmer.sum_localDefectBound_mul_log_le` and `New.Data.IsDenominatorBound.sum_le` with `New.Data.denominatorBudget`, together with the fields `N_prime`, `m_mem` and `constantBound_le` of `New.Data`.

Hints

§8.1.

8.1.1: Euler's criterion: $f(x)$ is a nonzero square in $\mathbb{F}_q$ exactly when $f(x)^c = 1$.

8.1.2: Substitute $d = 2g + 1$ in dc.

8.1.3: Look at the quotient and the remainder of each degree on division by q.

8.1.4: If $r_j = s_j = 0$ for all $j \ge 1$, then $s_0 \ne 0$. Otherwise use Problem 8.1.3.

§8.2.

8.2.1: For the last statement, expand $G(\alpha + Y)$ and substitute $Y = X - \alpha$.

8.2.2: The map $u \mapsto u^q$ is a ring homomorphism in characteristic p.

8.2.3: Write $f(X + Y) = f(X) + \Delta$ with $\Delta = \sum_{k\ge1}(H^k f)Y^k$, and expand $(1 + \Delta/f)^c$ by the binomial theorem. Note $\deg H^k f \le d - k$.

8.2.4: Expand $F(\alpha + Y)$ modulo Y^{k+1}. Use Problem 8.2.2, $\alpha^q = \alpha$, and $f(\alpha)^c = \eta$.

8.2.5: Bound each of the two kinds of terms in (3) separately, using Problem 8.2.3.

§8.3.

8.3.1: Compare the number of unknowns with the upper bound for the number of equations from Problem 8.2.5.

8.3.2: Use $2D = q - d$.

8.3.3: Check that $\sqrt{q} \ge 12$, $q - d - \ell \ge 8q/9$ and $11\sqrt{q}/12 \le \ell \le 13\sqrt{q}/12$. Then bound $t - 1$ and g by multiples of d.

8.3.4: $t > d\ell^2/(2q)$. Then use the inequality between arithmetic and geometric means.

§8.4.

8.4.1: Compare $\mathrm{covol}(u(L)) = |\det u|\,\mathrm{covol}(L)$ with $\mathrm{covol}(\lambda M)$.

8.4.2: Take orthonormal bases. For the counterexample write out the 2×2 matrix of $u_2^* u_2$.

8.4.3: Track the image of one lattice vector along the chain.

8.4.4: Follow the coefficient of each intermediate $\log \operatorname{covol}(L_j)$.
8.4.5: $u_1(L_0) = L_1$ and $u_2(L_1) = L_2$.
8.4.6: Apply Problem 8.4.1 to Ψ and the lattice L_0'.

§8.5.

8.5.1: Divide Theorem 8.4.1 by n before applying (5).
8.5.2: Write $2j - 1$ as a difference of consecutive squares.
8.5.3: Each step gives a bound for the same quantity.
8.5.4: Minimize over real $m > 0$ first.

References

[Bom74] E. Bombieri, *Counting points on curves over finite fields (d'après S. A. Stepanov)*, Séminaire Bourbaki, Exp. 430, Lecture Notes in Math. **383**, Springer, 1974, 234–241.

[GL] L. Sernau, *GRH for Dirichlet L-functions, in Lean 4*, a shorter rewriting of the Lean proof, text by Claude, `https://github.com/lsernau/grh-lean`, commit `72fead1`, readable edition `grh/`.

[Ne] J. Neukirch, *Algebraic Number Theory*, Grundlehren Math. Wiss. **322**, Springer, 1999.

[Sch76] W. M. Schmidt, *Equations over Finite Fields: An Elementary Approach*, Lecture Notes in Math. **536**, Springer, 1976.

[Ste69] S. A. Stepanov, *On the number of points of a hyperelliptic curve over a finite prime field*, Izv. Akad. Nauk SSSR Ser. Mat. **33** (1969), 1171–1181.

[Wei48] A. Weil, *Sur les courbes algébriques et les variétés qui s'en déduisent*, Hermann, 1948.

FEW TRANSLATES SPAN

Prerequisites. Finite-dimensional complex inner product spaces: adjoints, orthogonal projections, the spectral theorem for self-adjoint maps, and the trace. No earlier chapter is used.

In the proof, Theorem B bounds how many translates of a map between spaces of automorphic forms are needed for their images to span almost all of the target. The translates are indexed by a finite group. When do a few translates of one map span? Section 9.1 bounds the rank of a sum of images from below by a second moment. The rest of the chapter turns a second moment over the group into a choice of few translates, by Cauchy–Schwarz and a greedy choice. All spaces are finite-dimensional, and inner products are linear in the second variable.

9.1. Gram matrices

For a linear map A between inner product spaces, $\|A\|_{\mathrm{HS}}^2 := \operatorname{tr}(A^*A)$ is the squared Hilbert–Schmidt norm. Let $\mathcal{H}$ be a complex inner product space of dimension $D' > 0$. Let $B_i \colon X_i \to \mathcal{H}$, $i \in I$, be a finite family of linear maps from inner product spaces of dimensions r_i, with $R := \sum_i r_i > 0$, let $\gamma_i > 0$, and let $K_i := \gamma_i B_i^* B_i$ and $Q := \sum_i \gamma_i B_i B_i^*$. Let $X := \bigoplus_i X_i$ and $\Phi \colon X \to \mathcal{H}$, $\Phi((x_i)_i) := \sum_i \sqrt{\gamma_i} B_i x_i$, so that $Q = \Phi\Phi^*$. The *Gram matrix* of the family is $G := \Phi^*\Phi$. Its blocks are $G_{ij} = \sqrt{\gamma_i\gamma_j}\, B_i^* B_j \colon X_j \to X_i$, and $G_{ii} = K_i$. When every X_i is a line spanned by a unit vector ξ_i, G is the Gram matrix of the vectors $\sqrt{\gamma_i} B_i \xi_i$.

Problem 9.1.1. If $Q \neq 0$, then $\operatorname{rank} Q \geq (\operatorname{tr} Q)^2 / \operatorname{tr} Q^2$, with equality exactly when Q is a multiple of an orthogonal projection.

Problem 9.1.2. $Q(\mathcal{H}) = \sum_i B_i(X_i)$.

Problem 9.1.3. Q and G have the same nonzero eigenvalues, with multiplicities. Hence $\operatorname{tr} Q = \sum_i \operatorname{tr} K_i$ and $\operatorname{tr} Q^2 = \sum_{i,j} \|G_{ij}\|_{\mathrm{HS}}^2$.

Problems 9.1.1–9.1.3 prove the following.

Theorem 9.1.1. *If some B_i is nonzero, then*

$$\dim \sum_i B_i(X_i) \geq \frac{\left(\sum_i \operatorname{tr} K_i\right)^2}{\sum_{i,j} \|G_{ij}\|_{\mathrm{HS}}^2}.$$

For lines this is a form of Welch's bound [We]. Unlike the left side, the right side changes little when the B_i are perturbed.

Problem 9.1.4. Let $v, w \in \mathbb{C}^2$ be unit vectors, $X_1 = X_2 = \mathbb{C}$, $B_1(1) = v$, $B_2(1) = w$ and $\gamma_1 = \gamma_2 = 1$. The right side of Theorem 9.1.1 is $2/(1 + |\langle v, w\rangle|^2)$.

So two nearly parallel lines count as about one direction. In the proof a finite group acts on the target of one map B. The moment hypothesis bounds the dimension of the projected target times the sum of the squared overlaps $\|B^*\rho(s)B\|_{\mathrm{HS}}^2$ over all group elements, including the identity (Theorem 9.3.1 below).

Date: November 26, 2026.

9.2. Translates and the second moment

From now on S and T are finite-dimensional complex inner product spaces, Γ is a finite group, and ρ is a representation of Γ on T with $\langle \rho(s)x, \rho(s)y\rangle = \langle x, y\rangle$ for all $s \in \Gamma$ and $x, y \in T$. Let $B\colon S \to T$ be linear. For a subspace $W \subseteq T$ let P_W be the orthogonal projection of T onto W, as a map $T \to T$. The *second moment* of B is $\sum_{s\in\Gamma} \|B^*\rho(s)B\|_{\mathrm{HS}}^2$. Write $\langle A, A'\rangle_{\mathrm{HS}} := \operatorname{tr}(A^*A')$ for linear maps A, A' with the same source and target.

Problem 9.2.1. For every orthonormal basis (e_k) of S and all $A, A'\colon S \to T$, $\langle A, A'\rangle_{\mathrm{HS}} = \sum_k \langle Ae_k, A'e_k\rangle$. For every subspace $W \subseteq T$, $\|P_W\|_{\mathrm{HS}}^2 = \dim W$ and $\|P_W A\|_{\mathrm{HS}}^2 = \langle P_W, AA^*\rangle_{\mathrm{HS}}$.

Consider the family of all translates, $I = \Gamma$, $X_s = S$, $B_s = \rho(s)B$ and $\gamma_s = 1$, in the notation of Section 9.1.

Problem 9.2.2. $G_{st} = B^*\rho(s^{-1}t)B$, and $\langle \rho(s)BB^*\rho(s)^*, \rho(t)BB^*\rho(t)^*\rangle_{\mathrm{HS}} = \|B^*\rho(s^{-1}t)B\|_{\mathrm{HS}}^2$. Hence

$$\Big\|\sum_{s\in\Gamma} \rho(s)BB^*\rho(s)^*\Big\|_{\mathrm{HS}}^2 = \sum_{s,t\in\Gamma} \|G_{st}\|_{\mathrm{HS}}^2 = \#\Gamma \sum_{s\in\Gamma} \|B^*\rho(s)B\|_{\mathrm{HS}}^2.$$

Problem 9.2.3. Let $S \neq 0$, let B be an isometry, and let $\varepsilon \geq 0$. If $\dim T \cdot \sum_s \|B^*\rho(s)B\|_{\mathrm{HS}}^2 \leq \#\Gamma\,(1+\varepsilon)(\dim S)^2$, then the images $\rho(s)B(S)$, $s \in \Gamma$, together span a subspace of dimension at least $\dim T/(1+\varepsilon)$.

Problem 9.2.3 uses all $\#\Gamma$ translates. For $0 < \varepsilon < 1/16$, Theorem 9.4.1 will give a span of at least $(1-16\varepsilon)\dim T$ dimensions in this setting, using at most $\frac{5}{2}(1 + \log(1/(16\varepsilon)))\dim T/\dim S$ translates. The first step is a bound for one subspace at a time.

Problem 9.2.4. For every subspace $W \subseteq T$,

$$\Big(\sum_{s\in\Gamma} \|P_W\rho(s)B\|_{\mathrm{HS}}^2\Big)^2 \leq \dim W \cdot \#\Gamma \sum_{s\in\Gamma} \|B^*\rho(s)B\|_{\mathrm{HS}}^2.$$

An isometry condition on the projected map gives a lower bound for the second moment. Let $p\colon T \to T$ be a linear map with $p^2 = p$ and $p^* = p$, commuting with every $\rho(s)$, and let $T_0 := \operatorname{im} p$.

Problem 9.2.5. T_0 and $T_0^\perp$ are stable under Γ, and $p = P_{T_0}$. If pB is an isometry, then $\#\Gamma\,(\dim S)^2 \leq \dim T_0 \cdot \sum_s \|B^*\rho(s)B\|_{\mathrm{HS}}^2$.

When pB is an isometry and $T_0 \neq 0$, Problem 9.2.5 says that the mean of $\|B^*\rho(s)B\|_{\mathrm{HS}}^2$ over $s \in \Gamma$ is at least $(\dim S)^2/\dim T_0$. The hypothesis below requires it to be at most $1+\varepsilon$ times this value.

9.3. One translate

Let $A\colon S \to T$ be linear and $\varepsilon \in \mathbb{R}$. We say that A is a *near isometry with error* ε if $\dim U - \varepsilon \dim S \leq \|AP_U\|_{\mathrm{HS}}^2$ for every subspace $U \subseteq S$, where now $P_U\colon S \to S$ is the orthogonal projection onto U. This is a lower bound in mean square only.

Problem 9.3.1. If $\varepsilon \geq 0$ and $\|A^*A - 1\|_{\mathrm{HS}}^2 \leq \varepsilon^2 \dim S$, then A is a near isometry with error ε.

Let Θ be a set, let V and Y be finite-dimensional complex vector spaces, and let $C_\theta\colon V \to Y$, $\theta \in \Theta$, be linear maps. For $\eta \in \mathbb{R}$, we say that the family (C_θ) *spreads with error* η if for every subspace $F \subseteq Y$, with $\alpha := \dim F / \dim Y$ (and $\alpha := 0$ if $Y = 0$), there is $\theta \in \Theta$ with

$$\dim C_\theta^{-1}(F) \le \Big(\frac{1+\alpha}{2} + \eta\Big) \dim V.$$

The index θ may depend on F.

Now return to Section 9.2, and let $C_s := p\rho(s)B$, viewed as a map $S \to T_0$. Assume that $\varepsilon \ge 0$, that pB is a near isometry with error ε, and that

$$\dim T_0 \cdot \sum_{s\in\Gamma} \|B^*\rho(s)B\|_{\mathrm{HS}}^2 \le \#\Gamma\,(1+\varepsilon)(\dim S)^2. \tag{9.3.1}$$

Let $W \subseteq T_0$ be a subspace and let $\alpha := \dim W / \dim T_0$, with $\alpha := 0$ if $T_0 = 0$.

Problem 9.3.2. Some $s \in \Gamma$ has $\|P_W\rho(s)B\|_{\mathrm{HS}}^2 \le \frac{1}{2}(1+\alpha+\varepsilon)\dim S$.

Problem 9.3.3. For every $s \in \Gamma$, let $U := C_s^{-1}(W) \subseteq S$. Then $\|pBP_U\|_{\mathrm{HS}}^2 \le \|P_W\rho(s)B\|_{\mathrm{HS}}^2$. For s as in Problem 9.3.2, $\dim U \le \big(\frac{1+\alpha}{2} + \frac{3}{2}\varepsilon\big)\dim S$.

Problems 9.2.4, 9.3.2 and 9.3.3 prove the following, which is a step of the proof.

Theorem 9.3.1. *Let S and T be finite-dimensional complex inner product spaces, Γ a finite group, and ρ a representation of Γ on T with $\langle\rho(s)x, \rho(s)y\rangle = \langle x, y\rangle$ for all $s \in \Gamma$ and $x, y \in T$. Let $p\colon T \to T$ be linear with $p^2 = p$, $p^* = p$ and $p\rho(s) = \rho(s)p$ for every $s \in \Gamma$. Let $B\colon S \to T$ be linear and $\varepsilon \in \mathbb{R}$, with $\varepsilon \ge 0$, such that pB is a near isometry with error ε and* (9.3.1) *holds with $T_0 := \operatorname{im} p$. Then the maps $p\rho(s)B\colon S \to T_0$, $s \in \Gamma$, spread with error $\frac{3}{2}\varepsilon$.*

Here $T_0 = 0$ and $\varepsilon = 0$ are allowed.

9.4. The greedy choice

Return to maps $C_\theta\colon V \to Y$, $\theta \in \Theta$, as in Section 9.3. For a subspace $F \subseteq Y$ let $c(F) := \dim Y - \dim F$ be its codimension. In Problems 9.4.2–9.4.4 assume that $\dim Y > 0$, that $0 < \varepsilon < 1/16$, and that the family spreads with error $\frac{3}{2}\varepsilon$, and put $c_0 := 2\dim V/(5\dim Y)$.

Problem 9.4.1. For every linear $A\colon V \to Y$ and every subspace $F \subseteq Y$, $\dim(F + A(V)) + \dim A^{-1}(F) = \dim F + \dim V$.

Problem 9.4.2. If $c(F) > 16\varepsilon \dim Y$, then some θ has $c(F + C_\theta(V)) \le (1-c_0)\,c(F)$.

Problem 9.4.3. For every integer $\ell \ge 0$ there is a set $t \subseteq \Theta$ with $\#t \le \ell$ and $c\big(\sum_{\theta\in t} C_\theta(V)\big) \le \max\big(16\varepsilon, e^{-\ell c_0}\big)\dim Y$.

Problem 9.4.4. If $V \ne 0$, then $0 < c_0 \le 1$.

Problem 9.4.5. Under the hypotheses of Problem 9.4.4, with $V \ne 0$, there is an integer $\ell \ge 0$ such that $e^{-\ell c_0} \le 16\varepsilon$ and $\ell c_0 \le 1 + \log(1/(16\varepsilon))$, where log is the natural logarithm.

Problems 9.4.3 and 9.4.5 give the following theorem, used in the proof.

Theorem 9.4.1. *Let Θ be a set, let V and Y be finite-dimensional complex vector spaces, let $C_\theta\colon V \to Y$, $\theta \in \Theta$, be linear maps, and let $\varepsilon \in \mathbb{R}$. Assume that $V \neq 0$, that the family spreads with error $\frac{3}{2}\varepsilon$, that $\dim Y > 0$, and that $0 < \varepsilon < 1/16$. Then there is a finite set $t \subseteq \Theta$ with*

$$\#t \cdot \dim V \le \frac{5}{2}\Big(1 + \log\frac{1}{16\varepsilon}\Big)\dim Y \quad \textit{and} \quad (1-16\varepsilon)\dim Y \le \dim \sum_{\theta\in t} C_\theta(V).$$

Applied with $\Theta = \Gamma$, $V = S$, $Y = T_0$ and $C_s = p\rho(s)B$, Theorems 9.3.1 and 9.4.1 say: if $S \neq 0$, $T_0 \neq 0$, $0 < \varepsilon < 1/16$, pB is a near isometry with error ε and (9.3.1) holds, then the images of at most $\frac{5}{2}(1 + \log(1/(16\varepsilon)))\dim T_0/\dim S$ of the maps $p\rho(s)B$ span at least $(1-16\varepsilon)\dim T_0$ dimensions of T_0. This is the step that Theorem B of the proof needs. There (Chapter 36) Γ is the finite group $\bar{G}$, p is the action of the good idempotent e_0, T_0 is the space T of target forms, of dimension d_T, and the theorems are used with $\varepsilon = 1/(8b^2)$, where b is the weight at the b-places (Chapter 33). The resulting statement, after restriction to the ramified source forms, is Theorem 36.4.2. For a related logarithmic bound in greedy submodular covering, see Wolsey [Wo].

In the Lean formalization. In the Lean proof [GL], file `grh/src/New/Spanning/SecondMoment/FewTranslates.l` Theorem 9.3.1 is `New.isSpread_of_second_moment` and Theorem 9.4.1 is `New.IsSpread.exists_few_le_finrank_iSup_range`; spreading and near isometry are `New.IsSpread` and `New.IsNearIsometry`.

9.5. Translations of a cyclic group

Let $\Gamma = \mathbb{Z}/N\mathbb{Z}$, $T = \mathbb{C}^\Gamma$ with $\langle f, g\rangle = \sum_x \overline{f(x)}g(x)$, $(\rho(s)f)(x) = f(x-s)$, and $1 \le M \le N$. Let $S = \mathbb{C}^M$ with standard basis $e_0, \dots, e_{M-1}$, and $I := \{0, 1, \dots, M-1\} \subseteq \mathbb{Z}/N\mathbb{Z}$.

Problem 9.5.1. Let $Be_j := \delta_j$, the indicator function of $\{j\}$. Then $\|B^*\rho(s)B\|_{\mathrm{HS}}^2 = \#(I \cap (I+s))$, and the second moment is M^2. Hence, with $p = 1$, (9.3.1) holds with $\varepsilon = 0$, with equality.

Problem 9.5.2. In Problem 9.5.1, for $0 < \varepsilon < 1/16$, the least number of translates $\rho(s)B$ whose images span at least $(1-16\varepsilon)N$ dimensions is $\lceil (1-16\varepsilon)N/M \rceil$. For $N = 12$, $M = 3$, $\varepsilon = 1/128$ it is 4, while the bound of Theorem 9.4.1 is $10(1+\log 8) \approx 30.79$.

Every translate of $B(S)$ is orthogonal to any Γ-stable subspace orthogonal to $B(S)$.

Problem 9.5.3. Let $Be_j(x) := N^{-1/2}e^{2\pi i jx/N}$, $0 \le j < M$. Then B is an isometry, every $B^*\rho(s)B$ is diagonal and unitary, the second moment is NM, and the images of any nonempty set of translates span exactly $B(S)$. With $p = 1$, (9.3.1) holds exactly when $N \le (1+\varepsilon)M$. The subspace $B(S)$ is Γ-stable, and with $p = P_{B(S)}$, (9.3.1) holds with $\varepsilon = 0$.

Problem 9.5.4. In the setting of Section 9.2, let $S \neq 0$, let B be an isometry, and let $T_1 \subseteq T$ be a Γ-stable subspace orthogonal to $B(S)$. If (9.3.1) holds with $p = 1$, then $\dim T_1 \le \varepsilon \dim T/(1+\varepsilon)$.

Thus a stable subspace orthogonal to $B(S)$ gives a lower bound for the second moment. In general the theorems bound the dimension spanned inside the chosen target $T_0 = \operatorname{im} p$.

Hints

§9.1.

9.1.1: $Q = \Phi\Phi^* \geq 0$. Cauchy–Schwarz for the nonzero eigenvalues of Q.
9.1.2: $\ker \Phi^* = (\operatorname{im} \Phi)^\perp$.
9.1.3: If $Gx = \lambda x$ with $\lambda \neq 0$, then $Q(\Phi x) = \lambda \Phi x$. Then expand $\operatorname{tr} G^2$ by blocks.
9.1.4: G is the 2×2 matrix with diagonal entries 1 and off-diagonal entries $\langle v, w\rangle$ and $\langle w, v\rangle$.

§9.2.

9.2.1: For the last identity, $\operatorname{tr}(XY) = \operatorname{tr}(YX)$ and $P_W^2 = P_W = P_W^*$.
9.2.2: $\rho(s)^* = \rho(s^{-1})$; then Problem 9.1.3, and count the pairs (s, t) with given $s^{-1}t$.
9.2.3: Theorem 9.1.1 and Problem 9.2.2.
9.2.4: Sum Problem 9.2.1 over s, apply Cauchy–Schwarz for $\langle \cdot, \cdot \rangle_{\mathrm{HS}}$, and use Problem 9.2.2.
9.2.5: Problem 9.2.4 with $W = T_0$.

§9.3.

9.3.1: $\|AP_U\|_{\mathrm{HS}}^2 = \dim U + \langle P_U, A^*A - 1\rangle_{\mathrm{HS}}$.
9.3.2: Problem 9.2.4, with W viewed inside T, and $\sqrt{ab} \leq (a + b)/2$.
9.3.3: Compare $\rho(s)pB$ and $P_W \rho(s)B$ on U.

§9.4.

9.4.1: Rank–nullity for the restriction of A to $A^{-1}(F)$, and $\dim(F + A(V)) + \dim(F \cap A(V)) = \dim F + \dim A(V)$.
9.4.2: Problem 9.4.1 with $A = C_\theta$. Compare $\frac{1+\alpha}{2} + \frac{3}{2}\varepsilon$ with $1 - \frac{2}{5}(1 - \alpha)$.
9.4.3: Induction on ℓ, and $1 - c_0 \leq e^{-c_0}$.
9.4.4: Problem 9.4.2 with $F = 0$.
9.4.5: Round $\log(1/(16\varepsilon))/c_0$ up to an integer.

§9.5.

9.5.1: Count the pairs $(j, k) \in I \times I$ with $j - k = s$.
9.5.2: The images are spanned by indicator functions of points.
9.5.3: Each Be_j is an eigenvector of every $\rho(s)$.
9.5.4: Problem 9.2.5 with $p = P_{T_1^\perp}$.

References

[GL] L. Sernau, *GRH for Dirichlet L-functions, in Lean 4*, a shorter rewriting of the Lean proof, text by Claude, `https://github.com/lsernau/grh-lean`, commit `72fead1`, readable edition `grh/`.

[We] L. R. Welch, *Lower bounds on the maximum cross correlation of signals*, IEEE Trans. Inform. Theory **20** (1974), 397–399.

[Wo] L. A. Wolsey, *An analysis of the greedy algorithm for the submodular set covering problem*, Combinatorica **2** (1982), 385–393.

POINCARÉ SERIES AND NEAR ORTHOGONALITY

Prerequisites. Modular forms for $\mathrm{SL}_2(\mathbb{Z})$: q-expansions, the cusp form Δ and the dimension formula [SeA, Ch. VII, §3]. The residue theorem and the mean value property of holomorphic functions. The power series $J_\nu(x) = \sum_{j\ge0}(-1)^j(x/2)^{\nu+2j}/(j!\,\Gamma(\nu+j+1))$. Gershgorin's theorem on the eigenvalues of a matrix. Chapter 9, *Few translates span*, for the closing paragraphs only.

Chapter 9 asked for a map into a space of automorphic forms that is almost an isometry. If the weight is large, Poincaré series of small index are almost orthogonal, and Petersson's formula proves it with nothing more than a bound for a Bessel function. This chapter works it out on $\mathrm{SL}_2(\mathbb{Z})$, where the vectors are holomorphic Poincaré series and their Petersson inner products recover Fourier coefficients up to an explicit factor.

Throughout, $k \ge 4$ is even, $\Gamma := \mathrm{SL}_2(\mathbb{Z})$, $\Gamma_\infty := \{\pm \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \mid n \in \mathbb{Z}\}$, $j(\gamma, z) := cz + d$ for $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, $e(z) := e^{2\pi i z}$, and $d\nu := y^{-2}\,dx\,dy$ on the upper half-plane $\mathbb{H}$.

10.1. Poincaré series

Let S_k be the space of cusp forms of weight k for Γ, with the Petersson inner product $\langle f, g\rangle := \int_{\Gamma\backslash\mathbb{H}} f(z)\overline{g(z)}\,y^k\,d\nu(z)$. For $f \in S_k$ write $f(z) = \sum_{n\ge1} a_f(n)\,e(nz)$. For each positive integer m the *Poincaré series*

$$P_m(z) := \sum_{\gamma\in\Gamma_\infty\backslash\Gamma} j(\gamma, z)^{-k}\,e(m\gamma z)$$

converges absolutely and uniformly on compact sets, and $P_m \in S_k$ [Iw, §§3.1–3.2].

Problem 10.1.1. For $f \in S_k$ and $m \ge 1$,

$$\langle f, P_m\rangle = \frac{\Gamma(k-1)}{(4\pi m)^{k-1}}\,a_f(m).$$

Problem 10.1.2. The series P_m, $m \ge 1$, span S_k.

So $P_m = 0$ for $k \in \{4, 6, 8, 10, 14\}$, where $S_k = 0$, although no term of the series vanishes. The first nonzero case is $k = 12$, where $S_{12} = \mathbb{C}\Delta$ with $\Delta = \sum_{n\ge1}\tau(n)\,e(nz)$.

Problem 10.1.3. For $k = 12$,

$$P_m = \frac{10!\,\tau(m)}{(4\pi m)^{11}\,\|\Delta\|^2}\,\Delta.$$

In particular P_1 and P_2 are proportional.

So distinct Poincaré series need not be independent. Petersson's formula, in the next section, measures how far they are from orthogonal.

Date: November 25, 2026.

10.2. Petersson's formula

What is the Fourier expansion of P_m? For integers m, n and $c \geq 1$ let

$$S(m,n;c) := \sum_{\substack{d \bmod c \\ (d,c)=1}} e\Big(\frac{m\bar{d}+nd}{c}\Big), \qquad d\bar{d} \equiv 1 \pmod{c},$$

be the Kloosterman sum. It is real, and $S(m,n;c) = S(n,m;c)$.

Problem 10.2.1. The map $\gamma \mapsto (c,d)$ induces a bijection from $\Gamma_\infty\backslash\Gamma$ onto the set of pairs of coprime integers modulo ± 1. If $c \neq 0$, then $\gamma z = \frac{a}{c} - \frac{1}{c(cz+d)}$.

Problem 10.2.2. Let $\ell \geq 2$ be an integer, $\beta \in \mathbb{R}$ and $y > 0$. Then

$$\int_{\mathrm{i}y-\infty}^{\mathrm{i}y+\infty} z^{-\ell}\, e(-\beta z)\, dz = \begin{cases} (-2\pi\mathrm{i})^\ell\, \beta^{\ell-1}/(\ell-1)! & \beta > 0, \\ 0 & \beta \leq 0. \end{cases}$$

Problem 10.2.3. Let $\alpha > 0$, $\beta \in \mathbb{R}$ and $y > 0$. Then $\int_{\mathrm{i}y-\infty}^{\mathrm{i}y+\infty} z^{-k}\, e(-\alpha/z - \beta z)\, dz$ vanishes for $\beta \leq 0$, and for $\beta > 0$ equals

$$2\pi\mathrm{i}^{-k}\Big(\frac{\beta}{\alpha}\Big)^{(k-1)/2} J_{k-1}\big(4\pi\sqrt{\alpha\beta}\big).$$

Problem 10.2.4. $P_m(z) = \sum_{n\geq 1} p_m(n)\, e(nz)$, where

$$p_m(n) = \delta(m,n) + 2\pi\mathrm{i}^{-k}\Big(\frac{n}{m}\Big)^{(k-1)/2} \sum_{c\geq 1} \frac{S(m,n;c)}{c}\, J_{k-1}\Big(\frac{4\pi\sqrt{mn}}{c}\Big).$$

Problems 10.1.1 and 10.2.4 together give Petersson's formula [Pe], [Iw, §3.2], [ILS, §2]. Let

$$T_k(m,n) := 2\pi\mathrm{i}^{-k} \sum_{c\geq 1} \frac{S(m,n;c)}{c}\, J_{k-1}\Big(\frac{4\pi\sqrt{mn}}{c}\Big),$$

a real symmetric function of $m, n \geq 1$.

Theorem 10.2.1 (Petersson)**.** *For every orthonormal basis (f_j) of S_k and all $m, n \geq 1$,*

$$\frac{\Gamma(k-1)}{(4\pi\sqrt{mn})^{k-1}} \sum_j \overline{a_{f_j}(m)}\, a_{f_j}(n) = \delta(m,n) + T_k(m,n).$$

Problem 10.2.5. For $k \in \{4, 6, 8, 10, 14\}$ and all $m, n \geq 1$,

$$\sum_{c\geq 1} \frac{S(m,n;c)}{c}\, J_{k-1}\Big(\frac{4\pi\sqrt{mn}}{c}\Big) = -\frac{\mathrm{i}^k}{2\pi}\, \delta(m,n).$$

Numerically, for $m = n = 1$ the partial sums over $c \leq 800$ reproduce these values to within $3 \cdot 10^{-8}$ for $k = 4$ and 10^{-13} for $k \geq 6$. For $k = 12$ one finds $1 + T_{12}(1,1) = 2.84028\ldots$, which by Theorem 10.2.1 is $10!/\big((4\pi)^{11}\|\Delta\|^2\big)$, so that $\|\Delta\|^2 = 1.03536\ldots \cdot 10^{-6}$.

10.3. Near orthogonality

Normalize the Poincaré series by

$$\widetilde{P}_m := \frac{(4\pi m)^{(k-1)/2}}{\Gamma(k-1)^{1/2}}\, P_m,$$

and for each positive integer M let $G_M := \big(\langle \widetilde{P}_m, \widetilde{P}_n\rangle\big)_{1\le m,n\le M}$ be the $M \times M$ Gram matrix. We use the operator norm on $\mathbb{C}^M$ with its Euclidean inner product.

Problem 10.3.1. $\langle \widetilde{P}_m, \widetilde{P}_n\rangle = \delta(m,n) + T_k(m,n)$.

So G_M is the identity plus the matrix of Kloosterman terms, and the question is how small J_{k-1} is. We use Poisson's integral

$$J_\nu(x) = \frac{(x/2)^\nu}{\sqrt{\pi}\,\Gamma(\nu+\frac12)} \int_{-1}^{1} (1-t^2)^{\nu-1/2} \cos(xt)\, dt \qquad (\nu > -\tfrac12,\ x>0),$$

see [DLMF, (10.9.4)].

Problem 10.3.2. For $\nu > -\frac12$ and $x > 0$, $|J_\nu(x)| \le (x/2)^\nu/\Gamma(\nu+1)$.

Problem 10.3.3. $|T_k(m,n)| \le 2\pi\, \zeta(k-1)\, (2\pi\sqrt{mn})^{k-1}/(k-1)!$.

Problem 10.3.4. If $1 \le M \le (k-1)/(4\pi e)$, then every eigenvalue of G_M lies within $k\,2^{-k}$ of 1.

Problems 10.3.1–10.3.4 prove the following.

Theorem 10.3.1. *If $1 \le M \le (k-1)/(4\pi e)$, then $\|G_M - 1\| \le k\,2^{-k}$. In particular $P_1, \dots, P_M$ are linearly independent, and $\dim S_k \ge \lfloor (k-1)/(4\pi e)\rfloor$.*

Here $e = 2.718\ldots$ is Euler's number, and $4\pi e = 34.15\ldots$. The threshold is not the true one. For $0 < x \le r\nu$ with $0 < r < 1$ fixed, the function $J_\nu(x)$ is exponentially small in ν, and Siegel's inequality makes this precise: for $\nu \ge 0$ and $0 < x \le 1$,

$$|J_\nu(\nu x)| \le \Big(\frac{x\, e^{\sqrt{1-x^2}}}{1+\sqrt{1-x^2}}\Big)^\nu$$

[DLMF, (10.14.5)].

Problem 10.3.5. Let $0 < \theta < 1/(4\pi)$. There are constants $0 < \varrho < 1$ and $C > 0$, depending only on θ, such that $\|G_M - 1\| \le Ck\varrho^k$ for every even $k \ge 4$ and every integer M with $1 \le M \le \theta(k-1)$.

So for large k the $\widetilde{P}_m$ with $m \le \theta(k-1)$, for a fixed $\theta < 1/(4\pi)$, are almost orthonormal. For m near $(k-1)/(4\pi)$ the argument $4\pi m$ of the term $c = 1$ of $T_k(m,m)$ reaches the transition region $x \approx \nu$ of J_ν, where $J_\nu(x)$ is no longer exponentially small but of size up to about $\nu^{-1/3}$, and the diagonal entry is in general no longer exponentially close to 1. For $k = 100$, where $(k-1)/(4\pi) = 7.87\ldots$ and $\dim S_{100} = 8$, a computation of the Kloosterman terms gives the following. The eigenvalues of G_7 lie in $[0.99999, 1.0094]$. Those of G_8 lie in $[0.982, 1.808]$, so $P_1, \dots, P_8$ form a basis of S_{100}, and the Gram matrix of the normalized basis $\widetilde{P}_1, \dots, \widetilde{P}_8$ has an eigenvalue near 1.808. G_9 is singular, as it must be.

10.4. The dimension as formal degree times covolume

How large a proportion of S_k does Theorem 10.3.1 fill? Let $\Gamma\backslash\mathbb{H}$ carry the measure ν.

Problem 10.4.1. $\nu(\Gamma\backslash\mathbb{H}) = \pi/3$.

Problem 10.4.2. $\left|\dim S_k - \frac{k-1}{12}\right| \le \frac{13}{12}$ for every even $k \ge 4$.

For fixed $0 < \theta < 1/(4\pi)$, the first $\lfloor \theta(k-1) \rfloor$ series in Problem 10.3.5 span a proportion of S_k tending to 12θ as k tends to infinity through even weights. These limits approach $3/\pi = 0.954\ldots$ as θ increases to $1/(4\pi)$. The full initial segment in Theorem 10.3.1 gives limiting proportion $3/(\pi e) = 0.351\ldots$. Where does $(k-1)/12$ come from? It is the product of $\pi/3$ and a constant attached to the weight alone.

Let $G := \mathrm{PSL}_2(\mathbb{R})$ act on $\mathbb{H}$, and normalize Haar measure dg by $\int_G F(g\mathrm{i})\,dg = \int_{\mathbb{H}} F\,d\nu$ for compactly supported continuous F. With Haar probability on the stabilizer $\mathrm{PSO}(2)$ in the quotient integral formula, $\mathrm{vol}(\mathrm{PSL}_2(\mathbb{Z})\backslash G) = \pi/3$. Let $\mathcal{A}_k$ be the space of holomorphic functions f on $\mathbb{H}$ with $\|f\|^2 := \int_{\mathbb{H}} |f|^2 y^k\,d\nu < \infty$, on which G acts unitarily by $(\pi(g)f)(z) := f(g^{-1}z)\,j(g^{-1},z)^{-k}$. This is the holomorphic discrete series of weight k. For $w \in \mathbb{H}$ put

$$h_w(z) := \Big(\frac{z-\bar{w}}{2\mathrm{i}}\Big)^{-k}.$$

For a unit vector u of an irreducible unitary representation π with square-integrable matrix coefficients, the *formal degree* d_π is defined by $\int_G |\langle \pi(g)u, u\rangle|^2\,dg = 1/d_\pi$. It does not depend on u, by the Schur orthogonality relations for such representations [HC]. We compute it with u proportional to h_{i}.

Problem 10.4.3. For every $w \in \mathbb{H}$, $h_w \in \mathcal{A}_k$. For every $f \in \mathcal{A}_k$, $\langle f, h_{\mathrm{i}}\rangle = \frac{4\pi}{k-1} f(\mathrm{i})$.

Problem 10.4.4. $\pi(g)h_w = \overline{j(g,w)}^{-k} h_{gw}$ for $g \in \mathrm{SL}_2(\mathbb{R})$ and $w \in \mathbb{H}$.

Problem 10.4.5. Let $u := h_{\mathrm{i}}/\|h_{\mathrm{i}}\|$, and for $g \in G$ write $w := g\mathrm{i}$. Then $|\langle \pi(g)u, u\rangle|^2 = \big(4\,\mathrm{Im}\,w/|w+\mathrm{i}|^2\big)^k$, and the formal degree of π is $(k-1)/(4\pi)$.

With Problem 10.4.1 this gives

$$d_\pi \cdot \mathrm{vol}(\mathrm{PSL}_2(\mathbb{Z})\backslash G) = \frac{k-1}{4\pi}\cdot\frac{\pi}{3} = \frac{k-1}{12},$$

which is $\dim S_k$ up to the bounded error of Problem 10.4.2. This is not a coincidence. As in Problem 10.1.1, and using Problems 10.4.3 and 10.4.4, one checks that the reproducing kernel $B(z,w) := \sum_j f_j(z)\overline{f_j(w)}$ of S_k, for an orthonormal basis (f_j), is

$$B(z,w) = \frac{k-1}{4\pi} \sum_{\gamma \in \mathrm{PSL}_2(\mathbb{Z})} j(\gamma, z)^{-k}\, h_w(\gamma z).$$

Since $\dim S_k = \int_{\Gamma\backslash\mathbb{H}} B(z,z)\,y^k\,d\nu(z)$, the term $\gamma = 1$ contributes exactly the formal degree times the covolume, and by Problem 10.4.2 all other terms together contribute a bounded amount. For a compact unitary group with Haar probability, the formal degree of an irreducible representation is its dimension. In the definite example of Chapter 21, for rank $n \ge 1$ and weight λ with $4 \mid |\lambda|$, the central scalars contribute $4M_n \dim V_\lambda$, where M_n is the mass (Problem 21.3.4).

Theorem 10.3.1 says that the map $\mathbb{C}^M \to S_k$, $e_m \mapsto \widetilde{P}_m$, is almost an isometry when M is at most a fixed proportion of $\dim S_k$. Its image therefore occupies only part of S_k. Problem 10.3.5 extends near orthonormality to a longer initial segment, and Problem 10.1.2 shows that the full family spans S_k. In the setting of Chapter 9, a finite group acts on the ambient space. A near-isometry estimate for the projected map and a second-moment bound for the Gram operators of the unprojected map and its translates give a lower bound for the dimension spanned by a few projected translates in the target (Theorems 9.3.1 and 9.4.1).

The analogue in the proof. This chapter gives a classical model for the estimates in Chapter 36. In the proof, the principal-level forms on the unitary group of a hermitian space Y_0 over a CM field E play the role of S_k. Bessel periods play the role of Fourier coefficient extraction and are represented by a Poincaré map. Its values on the source coordinate basis are Bessel–Poincaré series. The two estimates below concern the map followed by the projector onto the good forms and the dimension of those forms. The next paragraph gives the declarations for these spaces, the period map and its values on the basis, and the two estimates. For the definition of Bessel periods see [GGP, §§12, 23].

In the Lean formalization. Fix admissible data D (`New.Data`) of the Lean proof [GL]. Write E for `Data.E`, Y_0 for `D.spaceY 0`, and r for the rank of Y_0 over E. Write S for the source forms `Data.SourceForm`, with coordinates `Data.sourceFormCoords`, and D_X for their complex dimension. The Poincaré map `Data.poincare` is `Data.poincareAt` at the chosen archimedean point `Data.besselPoint` and linear form `Data.besselForm`. By `Data.inner_poincareAt` it represents the Bessel period for each source form and each principal-level test form. By `Data.poincare_eq_poincareMap_comp` and `Filling.Fits.coe_poincareMap`, the inverse coordinate images of the standard basis vectors map to the corresponding Bessel–Poincaré series.

Let P be `Data.scaledPoincare`, the Poincaré map in these Euclidean coordinates multiplied by the positive factor `Data.poincareScale`. Its codomain is the space `Data.principalForms` on Y_0, of the specified discrete-series type at infinity and fixed by the kernel of reduction at the chosen finite places inside the standard finite level. Let e_0 denote the action of the group-algebra idempotent $\texttt{D.e}_0$ through `Data.principalRep` on this space. It projects onto the space T of good forms (`Data.targetForms`), of complex dimension d_T (`Data.targetDim`). Let b be the weight `D.b` at the infinite places `D.bPlaces`. For every complex subspace U of the source coordinate space, $\texttt{Data.isNearIsometry_e}_0\texttt{_comp_scaledPoincare}$ gives

$$\|e_0 P \,\mathrm{pr}_U\|_{\mathrm{HS}}^2 \geq \dim U - 5b^{-4} D_X,$$

where pr_U is the orthogonal projection and $\|\cdot\|_{\mathrm{HS}}$ is the Hilbert–Schmidt norm.

By `Data.targetDim_le_card_mul_besselDegree_mul_mass`,

$$d_T \leq \#\bar{G} \cdot \deg \cdot \mathrm{mass}(E, r).$$

Here $\bar{G}$ is `Data.chosenGL`, the product of GL_r over the residue fields at the chosen places above the two level primes. The constant deg is `D.filling.besselDegree`, the product of the degrees of the local Bessel systems over all infinite places of E. The factor $\mathrm{mass}(E, r)$ is `New.mass`, evaluated at E and r, the mass of the genus of the standard hermitian lattice $\mathcal{O}_E^r$. Both inequalities are in `grh/src/New/Spanning/SecondMoment/SpanningTheorem.lean`.

Hints

§10.1.

10.1.1: Unfold the sum over $\Gamma_\infty\backslash\Gamma$ to the strip $0 \le x \le 1$, $y > 0$, and integrate in x first.

10.1.2: Problem 10.1.1.

10.1.3: Expand P_m in the basis Δ and use Problem 10.1.1. Note that $\tau(1) = 1$, $\tau(2) = -24$.

§10.2.

10.2.1: The bottom row of a matrix in Γ is coprime, and two matrices with the same bottom row differ by left multiplication by an element of Γ_∞.

10.2.2: For $\beta \neq 0$, close the contour in the half-plane where $e(-\beta z)$ decays. For $\beta = 0$, use a primitive of $z^{-\ell}$.

10.2.3: Expand $e(-\alpha/z)$ in its power series and apply Problem 10.2.2 term by term. For $\beta \le 0$, $|e(-\alpha/z)| \le 1$ in $\mathbb{H}$.

10.2.4: The terms with $c > 0$ and fixed c are indexed by $d \in \mathbb{Z}$ coprime to c; group them by d mod c. Each group is a sum over translates $z \mapsto z + r$, $r \in \mathbb{Z}$, so its n-th Fourier coefficient is an integral over a whole horizontal line. Use Problems 10.2.1 and 10.2.3.

10.2.5: Theorem 10.2.1.

§10.3.

10.3.1: Problem 10.1.1 with $f = P_m$, and Problem 10.2.4.

10.3.2: Bound $|\cos(xt)|$ by 1 and evaluate the Beta integral.

10.3.3: $|S(m, n; c)| \le c$.

10.3.4: $(k-1)! \ge ((k-1)/e)^{k-1}$. Then Gershgorin's theorem.

10.3.5: Treat the term $c = 1$ with Siegel's inequality. The base on its right is increasing in x and equals 1 at $x = 1$. For the terms $c \ge 2$, use Problem 10.3.2.

§10.4.

10.4.1: The standard fundamental domain $|x| \le \frac{1}{2}$, $|z| \ge 1$; integrate in y first.

10.4.2: Write $k = 12j + r$ with $0 \le r < 12$ and use the dimension formula.

10.4.3: Put $\zeta := (z - \mathrm{i})/(z + \mathrm{i})$ and $F(\zeta) := f(z)\big((z + \mathrm{i})/2\mathrm{i}\big)^k$. Express $|f|^2 y^k \, d\nu$ in terms of F and ζ, and use the mean value property on the circles $|\zeta| = r$. For $h_w \in \mathcal{A}_k$, use $4 \operatorname{Im} z \operatorname{Im} w/|z - \bar{w}|^2 = 1 - |\zeta_w|^2$ with $\zeta_w := (z - w)/(z - \bar{w})$.

10.4.4: $gz - \overline{gw} = (z - \bar{w})/\big(j(g, z)\overline{j(g, w)}\big)$.

10.4.5: Problems 10.4.3 and 10.4.4. For the integral, use geodesic polar coordinates about i, in which $4 \operatorname{Im} w/|w + \mathrm{i}|^2 = \cosh^{-2}(\rho/2)$.

References

[DLMF] F. W. J. Olver, D. W. Lozier, R. F. Boisvert and C. W. Clark (eds.), *NIST Handbook of Mathematical Functions*, Cambridge Univ. Press, 2010; `https://dlmf.nist.gov`, Ch. 10.

[GGP] W. T. Gan, B. H. Gross and D. Prasad, *Symplectic local root numbers, central critical L-values, and restriction problems in the representation theory of classical groups*, Astérisque **346** (2012), 1–109.

[GL] L. Sernau, *GRH for Dirichlet L-functions, in Lean 4*, a shorter rewriting of the Lean proof, text by Claude, `https://github.com/lsernau/grh-lean`, commit `72fead1`, readable edition `grh/`.

[HC] Harish-Chandra, *Harmonic analysis on semisimple Lie groups*, Bull. Amer. Math. Soc. **76** (1970), 529–551.

[ILS] H. Iwaniec, W. Luo and P. Sarnak, *Low lying zeros of families of L-functions*, Publ. Math. IHÉS **91** (2000), 55–131.

[Iw] H. Iwaniec, *Topics in Classical Automorphic Forms*, Grad. Stud. Math. **17**, Amer. Math. Soc., Providence, 1997.

[Pe] H. Petersson, *Über die Entwicklungskoeffizienten der automorphen Formen*, Acta Math. **58** (1932), 169–215.

[SeA] J.-P. Serre, *A Course in Arithmetic*, Grad. Texts in Math. 7, Springer, 1973.

COMPLEX TORI, THETA FUNCTIONS AND PERIODS

Prerequisites. Complex analysis: Liouville's theorem, the argument principle, Weierstrass products, and Euler's Gamma function with the Beta integral and the reflection formula. The Gaussian integers. Elliptic curves over $\mathbb{C}$ at the level of the statements of [Si1, Ch. VI]. No earlier chapter is used. Chapter 13, *Complex multiplication and reduction at an inert prime*, continues this one.

11.1. Complex tori

How does one compute on a curve of genus one over $\mathbb{C}$? One uniformizes it. Let $\Lambda \subset \mathbb{C}$ be a lattice, and for integers $k \geq 3$ let $G_k(\Lambda) := \sum'_{\omega\in\Lambda} \omega^{-k}$, where the prime means that $\omega = 0$ is omitted. The Weierstrass function

$$\wp(u) := \frac{1}{u^2} + \sum_{\omega\in\Lambda}{}' \Big(\frac{1}{(u-\omega)^2} - \frac{1}{\omega^2} \Big)$$

is elliptic, that is meromorphic and Λ-periodic. Let $g_2 := 60G_4(\Lambda)$ and $g_3 := 140G_6(\Lambda)$. The map $u \mapsto (\wp(u), \wp'(u))$ for $u \notin \Lambda$, extended by sending the zero class to the point at infinity, is an analytic isomorphism of groups from $\mathbb{C}/\Lambda$ onto the smooth projective cubic with affine equation $y^2 = 4x^3 - g_2 x - g_3$, and every elliptic curve over $\mathbb{C}$ arises in this way [Si1, §§VI.3–VI.5].

Problem 11.1.1. Let $r := \min_{\omega\in\Lambda\setminus\{0\}} |\omega|$. For $0 < |u| < r$, $\wp(u) = u^{-2} + \sum_{k\geq 1} (2k+1) G_{2k+2}(\Lambda)\, u^{2k}$. As meromorphic functions, $\wp'^2 = 4\wp^3 - g_2\wp - g_3$.

Let

$$\zeta(u) := \frac{1}{u} + \sum_{\omega\in\Lambda}{}' \Big(\frac{1}{u-\omega} + \frac{1}{\omega} + \frac{u}{\omega^2} \Big), \qquad \sigma(u) := u \prod_{\omega\in\Lambda}{}' \Big(1 - \frac{u}{\omega}\Big) e^{u/\omega + \frac{u^2}{2\omega^2}}.$$

Then $\zeta' = -\wp$ and $\sigma'/\sigma = \zeta$. The function σ is entire and odd, with simple zeros exactly at the points of Λ.

Problem 11.1.2. There is a $\mathbb{Z}$-linear map $\eta\colon \Lambda \to \mathbb{C}$ with $\zeta(u+\omega) = \zeta(u) + \eta(\omega)$.

Problem 11.1.3. If ω_1, ω_2 is a basis of Λ with $\operatorname{Im}(\omega_2/\omega_1) > 0$, then $\eta(\omega_1)\omega_2 - \eta(\omega_2)\omega_1 = 2\pi\mathrm{i}$.

This is Legendre's relation.

Problem 11.1.4. $\sigma(u+\omega) = \psi(\omega)\, e^{\eta(\omega)(u+\omega/2)} \sigma(u)$ for $\omega \in \Lambda$, where $\psi(\omega) = 1$ if $\omega \in 2\Lambda$ and $\psi(\omega) = -1$ otherwise.

Problem 11.1.5. As a meromorphic identity, $\dfrac{\sigma(u+v)\,\sigma(u-v)}{\sigma(u)^2\,\sigma(v)^2} = \wp(v) - \wp(u)$.

Problem 11.1.6. As a meromorphic identity, $\zeta(u+v) - \zeta(u) - \zeta(v) = \dfrac{1}{2}\,\dfrac{\wp'(u) - \wp'(v)}{\wp(u) - \wp(v)}$. Consequently, as meromorphic functions,

$$\wp(u+v) = \frac{1}{4}\Big(\frac{\wp'(u) - \wp'(v)}{\wp(u) - \wp(v)}\Big)^2 - \wp(u) - \wp(v).$$

Date: November 24, 2026.

Now let Λ be *square*, that is $\mathrm{i}\Lambda = \Lambda$.

Problem 11.1.7. If $\mathrm{i}\Lambda = \Lambda$, then $\wp(\mathrm{i}u) = -\wp(u)$, $g_3 = 0$, and $\eta(\mathrm{i}\omega) = -\mathrm{i}\,\eta(\omega)$.

Problem 11.1.8. There is exactly one real $\lambda > 0$ with $g_2(\lambda\mathbb{Z}[\mathrm{i}]) = 4$.

Let $\varpi := 2\int_0^1 (1-t^4)^{-1/2}\,dt = 2.62205\ldots$ be the lemniscate constant.

Problem 11.1.9. The lattice $\varpi\mathbb{Z}[\mathrm{i}]$ has $g_2 = 4$ and $g_3 = 0$. Moreover $\varpi = \Gamma(\frac{1}{4})^2/(2\sqrt{2\pi})$.

From now on, *the lemniscatic lattice* is $\varpi\mathbb{Z}[\mathrm{i}]$, and $\wp$, ζ, σ without further mention are its Weierstrass functions. With $x = \wp$ and $y = \wp'/2$ it is the lattice of the curve $y^2 = x^3 - x$, and $dx/2y$ pulls back to du.

11.2. Theta functions

The function σ is not periodic, but by Problem 11.1.4 it changes by an exponential factor under the lattice. Entire functions with such a law are theta functions. How many are there, and how are they made?

Let τ lie in the upper half-plane, and let $\vartheta(z) := \sum_{n\in\mathbb{Z}} e^{\pi\mathrm{i}n^2\tau + 2\pi\mathrm{i}nz}$.

Problem 11.2.1. $\vartheta(z+1) = \vartheta(z)$, $\vartheta(z+\tau) = e^{-\pi\mathrm{i}\tau - 2\pi\mathrm{i}z}\vartheta(z)$, and $\vartheta(-z) = \vartheta(z)$.

Problem 11.2.2. Modulo $\mathbb{Z} + \mathbb{Z}\tau$, the only zero of ϑ is $(1+\tau)/2$, and it is simple.

Problem 11.2.3. Let σ and η belong to $\Lambda = \mathbb{Z} + \mathbb{Z}\tau$. Then there is a constant c with

$$\sigma(u) = c\,e^{\eta(1)u^2/2 + \pi\mathrm{i}u}\,\vartheta\big(u + \tfrac{1+\tau}{2}\big).$$

The theta functions of Chapter 15 are built from the Gaussian integers:

$$\Theta(z) := \sum_{\lambda\in\mathbb{Z}[\mathrm{i}]} e^{-\pi|\lambda|^2 + \lambda z}, \qquad \theta(z) := \sum_{a\in\mathbb{Z}} e^{-\pi a^2 + az}.$$

Problem 11.2.4. $\Theta(z) = \theta(z)\,\theta(\mathrm{i}z)$, $\Theta(\mathrm{i}z) = \Theta(z)$, and for $\beta \in \mathbb{Z}[\mathrm{i}]$

$$\Theta(z + 2\pi\beta) = e_\beta(z)\,\Theta(z), \qquad e_\beta(z) := e^{\pi|\beta|^2 + \bar\beta z}.$$

Let T be the space of entire functions f with $f(z + 2\pi\beta) = e_\beta(z)f(z)$ for all $\beta \in \mathbb{Z}[\mathrm{i}]$.

Problem 11.2.5. $\dim T = 2$, and every $f \in T$ is even.

Problem 11.2.6. A nonzero $f \in T$ has exactly two zeros modulo $2\pi\mathbb{Z}[\mathrm{i}]$, counted with multiplicity.

Problem 11.2.7. If $f \in T$, then $f(\mathrm{i}z) \in T$. The $f \in T$ with $f(\mathrm{i}z) = f(z)$ form the line $\mathbb{C}\,\Theta$.

The last fact about σ that we need concerns a sigma quotient associated with the theorem of the cube [Mu, §6, §10].

Problem 11.2.8. The quotient

$$\Xi(x,y,w) := \frac{\sigma(x+y+w)\,\sigma(x)\,\sigma(y)\,\sigma(w)}{\sigma(x+y)\,\sigma(y+w)\,\sigma(w+x)}$$

defines a meromorphic function on $\mathbb{C}^3$ that is Λ-periodic in each variable. As a meromorphic identity, $1/\Xi = \zeta(x) + \zeta(y) + \zeta(w) - \zeta(x+y+w)$.

Chapter 15 expresses Θ through σ and $\wp$ (Problem 15.1.3); then the nth derivative at 0 is $\Theta(0)$ times a rational multiple of $(\varpi/2\pi)^n$. So one needs to know ϖ, and the rational numbers that $\wp$ produces.

11.3. Periods

By Problem 11.1.1, the coefficient of u^{2k} in the Laurent expansion of $\wp$ is $(2k+1)G_{2k+2}(\Lambda)$ for $k \geq 1$. For the lemniscatic lattice these coefficients are rational. Write μ for an element of $\mathbb{Z}[\mathrm{i}]$.

Problem 11.3.1. $G_k(\varpi\mathbb{Z}[\mathrm{i}]) \in \mathbb{Q}$ for every integer $k \geq 3$, and $G_k = 0$ unless $4 \mid k$. For each integer $k \geq 1$, define the Hurwitz number H_{4k} by

$$\sum_{\mu}{}' \mu^{-4k} = \frac{(2\varpi)^{4k}}{(4k)!}\, H_{4k}.$$

Then $H_4 = \frac{1}{10}$ and $H_8 = \frac{3}{10}$.

When $\bar{\mu}$ also appears, π enters. Summed first over m and then over n, Eisenstein's series $G_2(\tau) := \sum_n \sum_m{}'(m+n\tau)^{-2}$ satisfies $G_2(-1/\tau) = \tau^2 G_2(\tau) - 2\pi\mathrm{i}\tau$ [We].

Problem 11.3.2. $G_2(\mathrm{i}) = \pi$.

For integers $j \geq 0$ and $k > j+2$, let $S(j,k) := \sum'_\mu \bar{\mu}^j \mu^{-k}$.

Problem 11.3.3. $S(j,k) = 0$ unless $j + k \equiv 0 \pmod 4$, and $S(0,k) = \varpi^k G_k(\varpi\mathbb{Z}[\mathrm{i}])$.

Damerell proved that $S(j,k)$ is an algebraic multiple of $\varpi^{j+k}\pi^{-j}$ [Dam]; for instance $S(1,7) = \frac{2}{315}\varpi^8/\pi$.

How big is ϖ in terms of classical constants? Let χ be the non-trivial character modulo 4. In the rest of this section, $\eta(\tau) := e^{\pi\mathrm{i}\tau/12}\prod_{n\geq 1}(1-e^{2\pi\mathrm{i}n\tau})$ is Dedekind's function, and $\zeta(s)$, with argument s, is Riemann's.

Problem 11.3.4. For $\operatorname{Re} s > 1$, $\sum'_\mu |\mu|^{-2s} = 4\,\zeta(s)\,L(s,\chi)$.

Let γ be Euler's constant. Kronecker's first limit formula states that for $\tau = x+\mathrm{i}y$ with $y > 0$, as $s \to 1$ from $\operatorname{Re} s > 1$,

$$\sum_{(m,n)\neq(0,0)} \frac{y^s}{|m+n\tau|^{2s}} = \frac{\pi}{s-1} + 2\pi\big(\gamma - \log 2 - \log(\sqrt{y}\,|\eta(\tau)|^2)\big) + O(s-1)$$

[La, Ch. 20]; Theorem 20.1.1 of Chapter 20 proves it.

Problem 11.3.5. $L'(1,\chi)/L(1,\chi) = \gamma - 2\log 2 - 4\log\eta(\mathrm{i})$.

The discriminant $\Delta(\Lambda) := g_2^3 - 27g_3^2$ satisfies $\Delta(\lambda\Lambda) = \lambda^{-12}\Delta(\Lambda)$ and $\Delta(\mathbb{Z}+\mathbb{Z}\tau) = (2\pi)^{12}\eta(\tau)^{24}$ [SeA, §VII.4.4].

Problem 11.3.6. $\eta(\mathrm{i})^2 = \varpi/(\sqrt{2}\,\pi)$, and so $\eta(\mathrm{i}) = \Gamma(\frac{1}{4})/(2\pi^{3/4})$.

Problems 11.1.9, 11.3.5 and 11.3.6 prove the following.

Theorem 11.3.1. $\dfrac{L'(1,\chi)}{L(1,\chi)} = \gamma + 2\log 2 + 3\log\pi - 4\log\Gamma(\frac{1}{4}) = 0.24560\ldots$

Chowla and Selberg found the general form [CS]. Chapter 20 proves it, together with Kronecker's limit formula, and states the period relation of Gross [Gr]: for an elliptic curve over $\bar{\mathbb{Q}}$ with complex multiplication by $\mathcal{O}_K$, every nonzero period of a holomorphic differential defined over $\bar{\mathbb{Q}}$ is a nonzero algebraic multiple of an explicit product Ω_K of values of Γ. For $K = \mathbb{Q}(\mathrm{i})$ this product is $\sqrt{\pi}\,\Gamma(\frac{1}{4})/\Gamma(\frac{3}{4})$.

Problem 11.3.7. $\sqrt{\pi}\,\Gamma(\frac{1}{4})/\Gamma(\frac{3}{4}) = 2\varpi$. Moreover

$$\Omega := \frac{2\varpi^2}{\pi} = \frac{\Gamma(\frac{1}{4})^4}{4\pi^2} = 4\pi\,\eta(\mathrm{i})^4.$$

For an imaginary quadratic field K with quadratic character χ_K, Chapter 20 relates $L'(1,\chi_K)/L(1,\chi_K)$ to the period product Ω_K, and Theorem 11.3.1 is its value for $K = \mathbb{Q}(\mathrm{i})$. Chapter 33 defines the period constant $\Omega = \exp\Big(\gamma - \mathrm{Re}\Big(\frac{L'(1,\chi_K)}{L(1,\chi_K)}\Big)\Big)\cdot 2\pi/\mathrm{rd}_E$, where E is the CM field of the data and rd_E its root discriminant. It also defines $s_\infty(j) = \log(j!) + j\log(M/\Omega)$ for integers $j \geq 0$, where $M = p_0p_1$ is the product of the two primes of the principal level. For $E = K = \mathbb{Q}(\mathrm{i})$, which is not a field of the data, $\mathrm{rd}_E = 2$, and Theorem 11.3.1 shows that the same expression is the Ω of Problem 11.3.7.

In the Lean formalization. The corresponding statements of the Lean proof [GL] are the definitions `Parameters.bigOmega` (in `grh/src/New/Reduction/Data/FieldsAndPlaces.lean`), `Data.M` and `Data.jetSize` (in `grh/src/New/Reduction/Data/AdmissibleData.lean`); `bigOmega` at the tower exponent of the data is Ω, and `jetSize`, which the code describes as the size of a derivative of order j, is s_∞.

Hints

§11.1.

11.1.1: Expand $(u-\omega)^{-2} - \omega^{-2}$ in powers of u. The function $\wp'^2 - 4\wp^3 + g_2\wp + g_3$ is elliptic, has no poles, and vanishes at 0.

11.1.2: The derivative of $\zeta(u+\omega) - \zeta(u)$ is 0.

11.1.3: Integrate ζ around a period parallelogram whose boundary avoids Λ.

11.1.4: The logarithmic derivative of $\sigma(u+\omega)/\sigma(u)$ is $\eta(\omega)$. To find the constant for $\omega \notin 2\Lambda$, use that σ is odd; for nonzero $\omega \in 2\Lambda$, apply the law twice with $\omega/2$, by induction on the power of 2 dividing ω.

11.1.5: For $v \notin \Lambda$, both sides are elliptic in u with the same zeros and poles. Compare the leading terms at $u = 0$.

11.1.6: Take the logarithmic derivative of Problem 11.1.5 in u and in v, and add. For the second formula, differentiate the first in u.

11.1.7: $G_k(\mathrm{i}\Lambda) = \mathrm{i}^{-k}G_k(\Lambda)$.

11.1.8: $g_2(\lambda\Lambda) = \lambda^{-4}g_2(\Lambda)$, and the values of $\wp$ at the three nonzero half-period classes of $\mathbb{Z}[\mathrm{i}]$ are real, distinct, and are the roots of $4x^3 - g_2x - g_3$.

11.1.9: Let λ be as in Problem 11.1.8. Then $\wp(\mathrm{i}\lambda/2) = -\wp(\lambda/2)$ and $\wp((1+\mathrm{i})\lambda/2) = 0$. On $(0,\lambda/2]$, $\wp$ is real and decreasing, and $\wp'^2 = 4\wp^3 - 4\wp$. Substitute $x = t^{-2}$. For the Gamma value use the Beta integral and $\Gamma(\frac{1}{4})\Gamma(\frac{3}{4}) = \pi\sqrt{2}$.

§11.2.

11.2.1: Replace n by $n+1$ and by $-n$.

11.2.2: Argument principle, as in Problem 11.1.3. At $z = (1+\tau)/2$, pair the terms n and $-1-n$.

11.2.3: Both sides have simple zeros exactly at Λ, and the same law under $u \mapsto u+1$ and $u \mapsto u+\tau$, by Problem 11.1.4 and Legendre's relation.

11.2.4: Write $\lambda = a+b\mathrm{i}$. For the law, substitute $\lambda = \mu+\bar{\beta}$ and note $\mathrm{Im}(\mu\beta) \in \mathbb{Z}$.

11.2.5: $e^{-z^2/4\pi} f(z)$ has period 2π. Expand it in a Fourier series $\sum_n a_n e^{\mathrm{i}nz}$, and use $\beta = \mathrm{i}$.

11.2.6: Integrate f'/f around a parallelogram with sides 2π and $2\pi\mathrm{i}$ whose boundary contains no zero of f.

11.2.7: If $f(\mathrm{i}z) = f(z)$, only powers z^{4k} occur in the Taylor series of f. Use Problem 11.2.6 and $\Theta(0) > 0$.

11.2.8: Use Problem 11.1.4 in x. For fixed y, w such that 0, $-y-w$, $-y$, $-w$ are distinct modulo Λ, compare the zeros and poles in x of Ξ and $1/(\zeta(x)+\zeta(y)+\zeta(w)-\zeta(x+y+w))$, then compare their leading terms at $x = 0$.

§11.3.

11.3.1: $g_2 = 4$ and $g_3 = 0$. Differentiate $\wp'^2 = 4\wp^3 - 4\wp$ to get $\wp'' = 6\wp^2 - 2$, and compare coefficients in Problem 11.1.1.

11.3.3: Replace μ by $\mathrm{i}\mu$.

11.3.4: Count the μ of norm n by unique factorization in $\mathbb{Z}[\mathrm{i}]$.

11.3.5: Take $\tau = \mathrm{i}$, and compare with the Laurent expansion of $4\zeta(s)L(s,\chi)$ at $s = 1$. $L(1,\chi) = \pi/4$.

11.3.6: $\Delta(\varpi\mathbb{Z}[\mathrm{i}]) = 64$, and $\eta(\mathrm{i}) > 0$.

11.3.7: $\Gamma(\frac{1}{4})\Gamma(\frac{3}{4}) = \pi\sqrt{2}$, and Problems 11.1.9 and 11.3.6.

References

[CS] A. Selberg and S. Chowla, *On Epstein's zeta-function*, J. reine angew. Math. **227** (1967), 86–110.

[Dam] R. M. Damerell, *L-functions of elliptic curves with complex multiplication. I*, Acta Arith. **17** (1970), 287–301.

[GL] L. Sernau, *GRH for Dirichlet L-functions, in Lean 4*, a shorter rewriting of the Lean proof, text by Claude, `https://github.com/lsernau/grh-lean`, commit `72fead1`, readable edition `grh/`.

[Gr] B. H. Gross, *On the periods of abelian integrals and a formula of Chowla and Selberg*, Invent. Math. **45** (1978), 193–211.

[La] S. Lang, *Elliptic Functions*, 2nd ed., Grad. Texts in Math. 112, Springer, 1987.

[Mu] D. Mumford, *Abelian Varieties*, Tata Inst. Fund. Res. Stud. Math. 5, Oxford Univ. Press, 1970.

[SeA] J.-P. Serre, *A Course in Arithmetic*, Grad. Texts in Math. 7, Springer, 1973.

[Si1] J. H. Silverman, *The Arithmetic of Elliptic Curves*, 2nd ed., Grad. Texts in Math. 106, Springer, 2009.

[We] A. Weil, *Elliptic Functions according to Eisenstein and Kronecker*, Ergeb. Math. Grenzgeb. 88, Springer, 1976.

THE FOCK MODEL AND THETA INTERTWINERS

Prerequisites. Fourier series of entire periodic functions. Quadratic Gauss sums: for an odd prime p and $p \nmid a$, $\sum_{t \bmod p} e^{2\pi i a t^2/p} = \left(\frac{a}{p}\right)\varepsilon_p\sqrt{p}$, with $\varepsilon_p = 1$ for $p \equiv 1 \pmod 4$ and $\varepsilon_p = \mathrm{i}$ for $p \equiv 3 \pmod 4$ [Dav, Ch. 2]. From Chapter 11, *Complex tori, theta functions and periods*: Jacobi's function and its quasi-periodicity (Section 11.2, Problem 11.2.1).

The kernels of the definite theta lifts of later chapters are built from theta functions of lattices of homomorphisms. Here we ask how a theta function of one lattice becomes a theta function of another, and what is lost when one does this twice. For compatible lattices a finite sum of translation operators does this, and for the neighbours below the loss is a root of unity given by a Gauss sum. We work in one complex variable, with $\mathbb{Z}[\mathrm{i}]$ and its neighbours of index 2 and p.

12.1. The Heisenberg group and the Fock model

On $V = \mathbb{C}$ let $H(z,w) := z\bar{w}$ and $E := \operatorname{Im} H$, so that $E(x+\mathrm{i}y, x'+\mathrm{i}y') = yx' - xy'$ is a symplectic form. For $x \in \mathbb{C}$ and a function G on $\mathbb{C}$ put

$$(U_x G)(z) := G(z+x)\, e^{-\pi H(z,x) - \frac{\pi}{2}H(x,x)}.$$

Let $\mathcal{F}$ be the *Fock space* of entire functions with $\|G\|^2 := \int_{\mathbb{C}} |G(z)|^2 e^{-\pi|z|^2}\, dA(z) < \infty$. The operators $e^{\mathrm{i}s}U_x$ with $s \in \mathbb{R}$ form a Heisenberg group, and $\mathcal{F}$ is its Fock model [Fo, Ch. 1], [Pol, Ch. 2]; for theta functions in one variable from this point of view, see [Mu, Ch. I, §3].

Problem 12.1.1. Each U_x is a unitary operator on $\mathcal{F}$, and

$$U_x U_y = e^{-\pi \mathrm{i} E(x,y)}\, U_{x+y}.$$

Problem 12.1.2. The monomials z^n are orthogonal in $\mathcal{F}$, with $\|z^n\|^2 = n!/\pi^n$.

So $f \mapsto f(\sqrt{\pi}\, z)$ is an isometry from $\mathbb{C}[z]$ with the Gaussian norm $\|f\|^2 := \pi^{-1}\int_{\mathbb{C}} |f(z)|^2 e^{-|z|^2}\, dA(z)$, for which $\|z^n\|^2 = n!$, into $\mathcal{F}$.

The representation of the Heisenberg group on $\mathcal{F}$ is irreducible. By the Stone–von Neumann theorem, every strongly continuous irreducible unitary representation on which $e^{\mathrm{i}s}$ acts by $e^{\mathrm{i}s}$ is unitarily equivalent to it [LV], [Pol, Ch. 2]. The inverse image of a self-dual lattice in the Heisenberg group is maximal abelian. A theta function is a joint eigenfunction for this group; the centre acts by its given character and the lattice eigenvalues are specified by a semicharacter.

A lattice $\Lambda \subset \mathbb{C}$ is *self-dual* if $E(\Lambda,\Lambda) \subset \mathbb{Z}$ and $\mathbb{C}/\Lambda$ has area 1. A *semicharacter* of Λ is a function $\alpha\colon \Lambda \to \{\pm 1\}$ with

$$\alpha(\lambda+\mu) = \alpha(\lambda)\alpha(\mu)(-1)^{E(\lambda,\mu)} \qquad (\lambda,\mu \in \Lambda).$$

For such a pair let $\mathcal{T}(\Lambda,\alpha)$ be the space of entire functions G with $\alpha(\lambda)U_\lambda G = G$ for all $\lambda \in \Lambda$, that is,

$$G(z+\lambda) = \alpha(\lambda)\, e^{\pi z\bar{\lambda} + \frac{\pi}{2}|\lambda|^2}\, G(z).$$

Date: November 25, 2026.

These are the classical theta functions of the line bundle on $\mathbb{C}/\Lambda$ with Hermitian form H and semicharacter α [Pol, Ch. 1]. Let $\alpha_0(m+n\mathrm{i}) := (-1)^{mn}$ on $\mathbb{Z}[\mathrm{i}]$.

Problem 12.1.3. The semicharacters of $\mathbb{Z}[\mathrm{i}]$ are the four functions $(-1)^{mn+am+bn}$ with $a, b \in \{0,1\}$. Exactly two of them, α_0 and $(-1)^{mn+m+n}$, are invariant under $v \mapsto \mathrm{i}v$.

Problem 12.1.4. Let α be a semicharacter of a self-dual Λ. Then $\lambda \mapsto \alpha(\lambda)U_\lambda$ is a homomorphism, and for $w \in \mathbb{C}$ and $G \in \mathcal{T}(\Lambda, \alpha)$,

$$\alpha(\lambda)U_\lambda\,(U_w G) = e^{-2\pi\mathrm{i}E(\lambda,w)}\,U_w G \qquad (\lambda \in \Lambda).$$

Problem 12.1.5. For $G \in \mathcal{T}(\Lambda, \alpha)$ the function $z \mapsto |G(z)|^2 e^{-\pi|z|^2}$ is Λ-periodic. Moreover $\mathcal{T}(\Lambda, \alpha) \cap \mathcal{F} = 0$.

So no nonzero theta function lies in $\mathcal{F}$. For $G \in \mathcal{T}(\Lambda, \alpha)$ we use the norm

$$\|G\|_\Lambda^2 := \int_{\mathbb{C}/\Lambda} |G(z)|^2 e^{-\pi|z|^2}\,dA(z).$$

12.2. Theta functions of $\mathbb{Z}[\mathrm{i}]$

How many theta functions does $\mathbb{Z}[\mathrm{i}]$ carry? For $\operatorname{Im}\tau > 0$ let $\vartheta_\tau(z) := \sum_{n\in\mathbb{Z}} e^{\pi\mathrm{i}n^2\tau + 2\pi\mathrm{i}nz}$, the function ϑ of Chapter 11, and let

$$G(z) := e^{\pi z^2/2}\,\vartheta_{\mathrm{i}}(z) = e^{\pi z^2/2} \sum_{n\in\mathbb{Z}} e^{-\pi n^2 + 2\pi\mathrm{i}nz}.$$

Problem 12.2.1. $\mathcal{T}(\mathbb{Z}[\mathrm{i}], \alpha_0) = \mathbb{C}G$.

Problem 12.2.2. $G(\mathrm{i}z) = G(z)$.

Problem 12.2.3. $\|G\|^2_{\mathbb{Z}[\mathrm{i}]} = 2^{-1/2}$.

For $t > 0$ let $\Lambda_t := t\mathbb{Z} + t^{-1}\mathrm{i}\mathbb{Z}$, a self-dual lattice, with the semicharacter $\alpha_t(ta + t^{-1}b\mathrm{i}) := (-1)^{ab}$.

Problem 12.2.4. $\mathcal{T}(\Lambda_t, \alpha_t) = \mathbb{C}\,e^{\pi z^2/2}\,\vartheta_{\mathrm{i}/t^2}(z/t)$.

For every self-dual Λ and every semicharacter α of it, $\mathcal{T}(\Lambda, \alpha)$ is a line. More generally, for a positive definite Hermitian form in g variables whose imaginary part E is integral on a full lattice Λ, the dimension is the absolute value of the Pfaffian of the matrix of E in a lattice basis [Pol, Ch. 3]. Section 12.3 deduces the line statement from Problem 12.2.1 for pairs compatible with $(\mathbb{Z}[\mathrm{i}], \alpha_0)$.

12.3. Intertwiners

Two pairs (Λ_1, α_1) and (Λ_2, α_2) as in Section 12.1 are *compatible* if Λ_1 and Λ_2 are commensurable and $\alpha_1 = \alpha_2$ on $\Lambda_{12} := \Lambda_1 \cap \Lambda_2$. Since both lattices have covolume 1, $n_{12} := [\Lambda_2 : \Lambda_{12}]$ equals $[\Lambda_1 : \Lambda_{12}]$. The *intertwiner* is

$$I_{12}\,G := n_{12}^{-1/2} \sum_{y \in \Lambda_2/\Lambda_{12}} \alpha_2(y)\,U_y G \qquad (G \in \mathcal{T}(\Lambda_1, \alpha_1)).$$

It is a finite sum of translation operators. The theory goes back to Weil [We]; see [Pol, Ch. 4] and [LV].

Problem 12.3.1. Each summand of $I_{12}G$ depends only on the class of y modulo Λ_{12}, and I_{12} maps $\mathcal{T}(\Lambda_1, \alpha_1)$ into $\mathcal{T}(\Lambda_2, \alpha_2)$.

Problem 12.3.2. $I_{21}I_{12}$ is the identity of $\mathcal{T}(\Lambda_1,\alpha_1)$.

Problem 12.3.3. $\|I_{12}G\|_{\Lambda_2} = \|G\|_{\Lambda_1}$.

By Problems 12.2.1 and 12.3.2, $\mathcal{T}(\Lambda,\alpha)$ is a line, spanned by IG for the intertwiner I from $\mathbb{Z}[\mathrm{i}]$, whenever (Λ,α) is compatible with $(\mathbb{Z}[\mathrm{i}],\alpha_0)$.

Problem 12.3.4. Let p be a prime, and let I_{12} be the intertwiner from $(\mathbb{Z}[\mathrm{i}],\alpha_0)$ to $(\Lambda_{1/p},\alpha_{1/p})$. Then

$$I_{12}\,G = \sqrt{p}\;e^{\pi z^2/2}\,\vartheta_{p^2\mathrm{i}}(pz),$$

and Problem 12.3.2 for this pair is the splitting of $\vartheta_{\mathrm{i}}(z)$ according to the class of n modulo p.

12.4. Composition

Is $I_{23}I_{12}$ equal to I_{13}? Let (Λ_i,α_i), $i=1,2,3$, be pairwise compatible pairs, each compatible with $(\mathbb{Z}[\mathrm{i}],\alpha_0)$. For $z\in\Lambda_3$ and $y\in\Lambda_2$ with $z+y\in\Lambda_1$ put

$$\psi(z,y) := \alpha_3(z)\,\alpha_2(y)\,\alpha_1(z+y)\,e^{-\pi\mathrm{i}E(z,y)}.$$

Problem 12.4.1. Let S_2 and S_3 be sets of representatives of Λ_2/Λ_{12} and Λ_3/Λ_{23}. There is a unique scalar $\mu=\mu(\Lambda_1,\Lambda_2,\Lambda_3)$, with the three semicharacters understood, for which

$$I_{23}I_{12} = \mu\, I_{13}, \qquad \mu = \Big(\frac{n_{13}}{n_{12}\,n_{23}}\Big)^{1/2} \sum_{\substack{z\in S_3,\ y\in S_2\\ z+y\in\Lambda_1}} \psi(z,y).$$

Problem 12.4.2. $|\mu|=1$, $\mu(\Lambda_1,\Lambda_2,\Lambda_1)=1$, and $\mu(\Lambda_1,\Lambda_3,\Lambda_2)=\overline{\mu(\Lambda_1,\Lambda_2,\Lambda_3)}$.

Problem 12.4.3. For four pairwise compatible pairs, each compatible with $(\mathbb{Z}[\mathrm{i}],\alpha_0)$,

$$\mu(\Lambda_1,\Lambda_2,\Lambda_3)\,\mu(\Lambda_1,\Lambda_3,\Lambda_4) = \mu(\Lambda_2,\Lambda_3,\Lambda_4)\,\mu(\Lambda_1,\Lambda_2,\Lambda_4).$$

Problems 12.3.2, 12.3.3, 12.4.1 and 12.4.2 prove the following. Weil computes the factor system for his projective representation [We]. The formula for μ appears in [Adr, Lemma 7.3(ii)] with a single semicharacter on all three lattices.

Theorem 12.4.1. *The intertwiners are isometries, $I_{21}=I_{12}^{-1}$, and $I_{23}I_{12}=\mu\,I_{13}$ with $|\mu|=1$ given by the sum of Problem 12.4.1.*

The constant μ is a normalized quadratic Gauss sum. For the Weil representation, Lion and Vergne express the analogous constant through the Maslov index of three Lagrangian subspaces [LV]; Gauss sums of integral quadratic forms are treated in [Pol, App. B]. The next section computes μ in the smallest cases.

12.5. Neighbours of index p and 2

Odd index. Let $R\subset\mathbb{Q}$ be the ring of fractions with odd denominator, so that $R/2R=\mathbb{Z}/2$, and for $r\in R$ let $(-1)^r := (-1)^n$ for any integer $n\equiv r \pmod{2R}$. For $v=x+\mathrm{i}y$ with $x,y\in R$ put $\alpha_R(v):=(-1)^{xy}$.

Problem 12.5.1. α_R is a semicharacter of every self-dual lattice contained in $R+R\mathrm{i}$. It equals α_0 on $\mathbb{Z}[\mathrm{i}]$ and $\alpha_{1/p}$ on $\Lambda_{1/p}$ for p odd.

So all self-dual lattices in $R + R\mathrm{i}$, with α_R, are pairwise compatible. Fix an odd prime p, and let $N := \mathbb{Z} + p\mathbb{Z}\mathrm{i}$.

Problem 12.5.2. The self-dual lattices Λ with $N \subset \Lambda$ are $\Lambda^{(\infty)} := \mathbb{Z}[\mathrm{i}]$ and $\Lambda^{(c)} := N + \mathbb{Z}(\frac{1}{p} + c\mathrm{i})$ for $c \in \mathbb{Z}/p$. Moreover $\Lambda^{(0)} = \Lambda_{1/p}$, and any two of these $p+1$ lattices intersect in N.

Problem 12.5.3. For $b \neq c$ in $\mathbb{Z}/p$, with $\bar{2} := (p+1)/2$,

$$\mu(\Lambda^{(\infty)}, \Lambda^{(b)}, \Lambda^{(c)}) = \frac{1}{\sqrt{p}} \sum_{t \bmod p} e^{2\pi\mathrm{i}\,\bar{2}(c-b)t^2/p} = \Big(\frac{2(c-b)}{p}\Big)\,\varepsilon_p.$$

For $p = 3$, $b = 0$, $c = 1$ this is $-\mathrm{i}$.

Problem 12.5.4. For distinct $a, b, c \in \mathbb{Z}/p$,

$$\mu(\Lambda^{(a)}, \Lambda^{(b)}, \Lambda^{(c)}) = \Big(\frac{2(b-a)(c-b)(c-a)}{p}\Big)\,\varepsilon_p.$$

Index 2. Here α_R is not available, and the semicharacters must be chosen. Let $N_2 := \mathbb{Z} + 2\mathbb{Z}\mathrm{i}$, let $\Lambda' := \Lambda_{1/2} = \frac{1}{2}\mathbb{Z} + 2\mathbb{Z}\mathrm{i}$ with $\alpha' := \alpha_{1/2}$, and let $\Lambda'' := \mathbb{Z}(\frac{1}{2} + \mathrm{i}) + \mathbb{Z}$ with $\alpha''(a(\frac{1}{2} + \mathrm{i}) + m) := (-1)^{am}$.

Problem 12.5.5. $\mathbb{Z}[\mathrm{i}]$, Λ' and Λ'' are the self-dual lattices containing N_2, and any two of them intersect in N_2. The pairs $(\mathbb{Z}[\mathrm{i}], \alpha_0)$, (Λ', α') and (Λ'', α'') are pairwise compatible, and each of Λ', Λ'' has exactly two semicharacters compatible with α_0.

Problem 12.5.6. $\mu(\mathbb{Z}[\mathrm{i}], \Lambda', \Lambda'') = 2^{-1/2} \sum_{t \bmod 2} e^{\pi\mathrm{i}t^2/2} = e^{\pi\mathrm{i}/4}$. If α'' is replaced by the other semicharacter compatible with α_0, then $\mu = e^{-\pi\mathrm{i}/4}$.

For the distinct neighbours above, the composition scalar is a fourth root of unity at an odd prime and a primitive eighth root of unity at index 2. In both calculations the phase $\psi(z, y)$ contains the semicharacter values and the factor $e^{-\pi\mathrm{i}E(z,y)}$. At index 2 the choice of compatible semicharacter distinguishes the two eighth roots in Problem 12.5.6.

Unitary changes of variable. Constants of the same kind appear when a lattice is moved by a unitary map ϱ of V. Let $G' \in \mathcal{T}(\Lambda, \alpha)$. If ϱ preserves Λ and α, then $G' \circ \varrho^{-1}$ lies in the same line. For $z \mapsto \mathrm{i}z$ on $(\mathbb{Z}[\mathrm{i}], \alpha_0)$ the scalar is 1 by Problem 12.2.2. If the transported pair $(\varrho\Lambda, \alpha \circ \varrho^{-1})$ is compatible with (Λ, α), then $G' \circ \varrho^{-1}$ and $I_{\Lambda \to \varrho\Lambda}\, G'$ belong to the same theta line and have the same norm. For $G' \neq 0$ they differ by a scalar of absolute value one. Related composition factors occur in Weil's construction of the metaplectic cover [We]. For a completion $F \neq \mathbb{C}$ of a number field containing the n-th roots of unity, Kubota gives a factor set for an n-fold cover of $\mathrm{SL}_2(F)$ in terms of Hilbert symbols [Kub].

In the Lean formalization. In the Lean proof [GL], the kernel of the definite lift from X_j to X_{j+1} for a tame character (`liftKernel`) takes data in the finite part (`finitePart`) for the Hermitian space of maps from X_j to X_{j+1}. This is the complex span of the finite Heisenberg translates of that space's vacuum. A translation tuple x (`Translations`) consists, for every $j \in \mathbb{N}$, of a matrix x_j over the finite adeles of the CM field, with rows indexed by the basis of X_{j+1} and columns by the basis of X_j. The value `translateDatum` $x\, j$ is the translate by x_j of the integral vacuum of that Hermitian space (Chapter 34).

The corresponding statements of the Lean proof for the data of the composite lift are `gluedDoubleLiftDatum`, `doubleLiftGluing`, `gluedVacuum` and `gluedTensor`, and for the composite lift itself `compositeLift` and `restrictToY`.

These declarations are in `grh/src/New/UpperBound/Objects/Columns.lean`, with `finitePart` in `grh/src/Lib/Weil/Construction/VacuumProjections.lean`.

Hints

§12.1.

12.1.1: $|(U_xG)(z)|^2e^{-\pi|z|^2} = |G(z+x)|^2e^{-\pi|z+x|^2}$. For the product, compare exponents; $H(x,y) - \operatorname{Re} H(x,y) = \mathrm{i}E(x,y)$.

12.1.2: Polar coordinates.

12.1.3: Two semicharacters differ by a character of Λ with values ±1. For α_0 check the identity on the basis $1, \mathrm{i}$ and extend.

12.1.4: The first statement is the definition of a semicharacter together with Problem 12.1.1. For the second, commute U_λ past U_w.

12.1.5: Compare the Gaussian integrals over translates of one fundamental parallelogram.

§12.2.

12.2.1: For $F \in \mathcal{T}(\mathbb{Z}[\mathrm{i}], \alpha_0)$, $e^{-\pi z^2/2}F$ has period 1; expand it in a Fourier series and use the law under $z \mapsto z + \mathrm{i}$ to relate consecutive coefficients.

12.2.2: Apply Problem 12.2.1 to $G(\mathrm{i}z)$.

12.2.3: Integrate first over $x \in [0,1]$; the remaining sum over n unfolds $[0,1]$ in y to $\mathbb{R}$.

12.2.4: As in Problem 12.2.1, after the substitution $z = tw$.

§12.3.

12.3.1: Use the homomorphism in Problem 12.1.4 for (Λ_2, α_2). First compare the summands at y and $y+\lambda$ for $\lambda \in \Lambda_{12}$. Then apply $\alpha_2(w)U_w$ for $w \in \Lambda_2$ and inspect its effect on the cosets.

12.3.2: By Problem 12.1.4, $\sum_{x \in \Lambda_1/\Lambda_{12}} \alpha_1(x)U_x$ multiplies U_yG by a character sum. The character $x \mapsto e^{-2\pi\mathrm{i}E(x,y)}$ of Λ_1/Λ_{12} is trivial exactly when $y \in \Lambda_1$, since Λ_1 is self-dual.

12.3.3: Integrate over $\mathbb{C}/\Lambda_{12}$, an n_{12}-fold cover of both tori. A cross term $U_yG\,\overline{U_{y'}G}\,e^{-\pi|z|^2}$ with $y \not\equiv y'$ is Λ_{12}-periodic and changes by a nontrivial character under Λ_1.

12.3.4: Representatives s/p, $0 \le s < p$. Then $\sum_s e^{2\pi\mathrm{i}ns/p}$ picks out $p \mid n$.

§12.4.

12.4.1: Use Problems 12.2.1 and 12.3.2 to compare the two maps between the source and target theta spaces. Apply $\sum_x \alpha_1(x)U_x$ to both sides of $I_{23}I_{12}G = \mu\, I_{13}G$, with x running over $\Lambda_1/(\Lambda_1 \cap \Lambda_2 \cap \Lambda_3)$, and use Problem 12.1.4.

12.4.2: For the modulus use Problem 12.3.3. Then compute $I_{32}I_{23}I_{12}$ in two ways.

12.4.3: Compute $I_{34}I_{23}I_{12}$ in two ways.

§12.5.

12.5.1: $(x+x')(y+y') - xy - x'y' - E(v,v') = 2xy'$.

12.5.2: The dual of N for E is $N^\perp = \frac{1}{p}\mathbb{Z} + \mathbb{Z}\mathrm{i}$, and $N^\perp/N \cong (\mathbb{Z}/p)^2$. A self-dual $\Lambda \supset N$ lies in $N^\perp$ and corresponds to a line in $N^\perp/N$.

12.5.3: Take $z = t(\frac{1}{p} + c\mathrm{i})$ and $y = -t(\frac{1}{p} + b\mathrm{i})$. Then $z + y \in \mathbb{Z}[\mathrm{i}]$, and $\psi(z,y)$ depends only on the classes of z and y modulo N.

12.5.4: Problem 12.4.3 with $\Lambda_1 = \mathbb{Z}[\mathrm{i}]$, and Problem 12.5.3.

12.5.5: As in Problem 12.5.2 with $p = 2$. Note that $\alpha_0 = 1$ on N_2, and apply Problem 12.1.3's argument to Λ' and Λ''.

12.5.6: One term has $z = y = 0$. In the other, z represents the nonzero class of Λ''/N_2.

References

[Adr] J. Adriazola, *The Alpöge proof of the Riemann hypothesis*, manuscript, revised 24 November 2026, `https://github.com/jimjamzola/RH-Alpoge-Reconstruction`.

[Dav] H. Davenport, *Multiplicative Number Theory*, 3rd ed., Grad. Texts in Math. 74, Springer, 2000.

[Fo] G. B. Folland, *Harmonic Analysis in Phase Space*, Ann. of Math. Stud. 122, Princeton Univ. Press, 1989.

[GL] L. Sernau, *GRH for Dirichlet L-functions, in Lean 4*, a shorter rewriting of the Lean proof, text by Claude, `https://github.com/lsernau/grh-lean`, commit `72fead1`, readable edition `grh/`.

[Kub] T. Kubota, *Topological covering of $SL(2)$ over a local field*, J. Math. Soc. Japan **19** (1967), 114–121.

[LV] G. Lion and M. Vergne, *The Weil Representation, Maslov Index and Theta Series*, Progr. Math. 6, Birkhäuser, 1980.

[Mu] D. Mumford, *Tata Lectures on Theta I*, Progr. Math. 28, Birkhäuser, 1983.

[Pol] A. Polishchuk, *Abelian Varieties, Theta Functions and the Fourier Transform*, Cambridge Tracts in Math. 153, Cambridge Univ. Press, 2003.

[We] A. Weil, *Sur certains groupes d'opérateurs unitaires*, Acta Math. **111** (1964), 143–211.

COMPLEX MULTIPLICATION AND REDUCTION AT AN INERT PRIME

Prerequisites. Chapter 11, *Complex tori, theta functions and periods*, Section 11.1: the Weierstrass functions, Problems 11.1.6 and 11.1.7, and the lemniscatic lattice $\varpi\mathbb{Z}[\mathrm{i}]$ of the curve $E\colon y^2 = x^3 - x$. Orders in imaginary quadratic fields. Elliptic curves over a field at the level of [Si1, Ch. III], and the statements, not the proofs, of [Si1, Ch. IV, §§V.1–V.4, Ch. VI].

13.1. Complex multiplication

Which tori have endomorphisms other than $u \mapsto nu$? Every holomorphic map $\mathbb{C}/\Lambda \to \mathbb{C}/\Lambda$ that fixes 0 is $u \mapsto \alpha u$ with $\alpha\Lambda \subseteq \Lambda$ [Si1, Thm. VI.4.1]. So if E corresponds to Λ, then $\mathrm{End}(E) = \{\alpha \in \mathbb{C} : \alpha\Lambda \subseteq \Lambda\}$, and we write $[\alpha]$ for $u \mapsto \alpha u$.

Problem 13.1.1. If $\mathrm{End}(E) \neq \mathbb{Z}$, then $K := \mathbb{Q}(\alpha)$ is imaginary quadratic for every $\alpha \in \mathrm{End}(E) \smallsetminus \mathbb{Z}$, $\mathrm{End}(E)$ is an order in K, and Λ is homothetic to a lattice contained in K.

We then say that E has *complex multiplication* by that order.

Problem 13.1.2. $\mathrm{End}(\mathbb{C}/\mathbb{Z}[\mathrm{i}]) = \mathbb{Z}[\mathrm{i}]$, $\mathrm{End}(\mathbb{C}/\mathbb{Z}[2\mathrm{i}]) = \mathbb{Z}[2\mathrm{i}]$, and $\mathrm{End}(\mathbb{C}/\mathbb{Z}[\rho]) = \mathbb{Z}[\rho]$ with $\rho = e^{2\pi\mathrm{i}/3}$.

Problem 13.1.3. For $\alpha \in \mathrm{End}(E)$, $\alpha \neq 0$, the kernel of $[\alpha]$ on $\mathbb{C}/\Lambda$ has $|\alpha|^2$ elements.

For each nonzero $\alpha \in \mathrm{End}(E)$, the function $\wp(\alpha u)$ is even and elliptic for Λ, so it is a rational function of $\wp(u)$, and $[\alpha]$ is a rational map of the curve.

Problem 13.1.4. For the lemniscatic lattice, $\wp((1+\mathrm{i})u) = \dfrac{\wp(u)^2 - 1}{2\mathrm{i}\,\wp(u)}$.

Problem 13.1.5. On $E\colon y^2 = x^3 - x$, $[\mathrm{i}](x, y) = (-x, \mathrm{i}y)$. For every $\alpha \in \mathrm{End}(E)$, $[\alpha]^*(dx/2y) = \alpha\, dx/2y$.

Problem 13.1.6. For $a, b \in \mathbb{C}^\times$, the curve $y^2 = x^3 + ax$ has complex multiplication by $\mathbb{Z}[\mathrm{i}]$, and $y^2 = x^3 + b$ has complex multiplication by $\mathbb{Z}[\rho]$.

The endomorphisms of $E\colon y^2 = x^3 - x$ extend to its elliptic curve model over $\mathbb{Z}[\mathrm{i}, \frac{1}{2}]$, so they can be reduced at each prime of this ring above an odd prime p. What do they look like near the origin? In a local parameter at the origin, addition gives a formal group law, and each endomorphism acts on it by a power series.

13.2. The formal group

Let E be given by a Weierstrass equation over a ring R, and let $z := -x/y$. The group law, written in z, is a formal group law $F(z_1, z_2) \in R[[z_1, z_2]]$, and every endomorphism defined over R becomes a series $[\alpha](z) \in R[[z]]$ [Si1, §§IV.1–IV.2].

Date: November 24, 2026.

The invariant differential becomes $\omega(z) = \sum_{n\geq 1} c_n z^{n-1}\,dz$ with $c_1 = 1$ and $c_n \in R$. If R is torsion-free, then over $R \otimes_{\mathbb{Z}} \mathbb{Q}$ the *logarithm* $\ell(z) := \sum_{n\geq 1} c_n z^n/n$ satisfies $F(z_1, z_2) = \ell^{-1}(\ell(z_1) + \ell(z_2))$ [Si1, §§IV.4–IV.5]. Over $\mathbb{C}$, take the uniformizing coordinate u for which ω pulls back to du. Then $\ell(z(u)) = u$ near the origin. The *invariant derivation* is $D := \ell'(z)^{-1}\,d/dz$, where $\ell'(z) = \sum_{n\geq 1} c_n z^{n-1}$ has the coefficients of ω; over $\mathbb{C}$, $D = d/du$.

For a one-parameter formal group over $\mathbb{Z}_p$, either $[p](z) \equiv 0 \pmod p$ or $[p](z) \equiv g(z^{p^h}) \pmod p$ with $g'(0) \not\equiv 0$; the integer h is the *height* [Si1, §IV.7]. For an elliptic curve with good reduction at p, $h \in \{1, 2\}$, and $h = 2$ exactly when the reduction is supersingular [Si1, Thm. V.3.1]. The two extreme models are $\hat{G}_a(X, Y) = X + Y$ and $\hat{G}_m(X, Y) = X + Y + XY$.

Problem 13.2.1. For $\hat{G}_m$, $\ell(X) = \log(1 + X)$, $[p](X) \equiv X^p \pmod p$, and the height is 1.

Problem 13.2.2. As operators on $\mathbb{Z}_p[[X]]$ modulo p: for $\hat{G}_a$, $D^p \equiv 0$; for $\hat{G}_m$, $D = (1 + X)\,d/dX$ and $D^p \equiv D$.

For a one-parameter formal group over $\mathbb{Z}_p$, its normalized invariant derivation satisfies $D^p \equiv \lambda D \pmod p$ for some $\lambda \in \mathbb{F}_p$. Problems 15.3.1 and 15.3.2 of Chapter 15 give the argument for the lemniscate, and the same argument applies to every one-parameter formal group over $\mathbb{Z}_p$. Which constant is λ?

Problem 13.2.3. Let $\hat{G}$ be the formal group of a Weierstrass equation over $\mathbb{Z}_{(p)}$, with $D^p \equiv \lambda D \pmod p$. Then $(D^n z)(0) = n!\,[u^n]\,\ell^{-1}(u)$ for every n, and $\lambda \equiv c_p \pmod p$.

Problem 13.2.4. For $\hat{G}$ as in Problem 13.2.3, the coefficient of z^p in $[p](z)$ is congruent to c_p modulo p. Hence the height is 1 exactly when $p \nmid c_p$.

Now we compute c_n for $E\colon y^2 = x^3 - x$. Let $w := -1/y$.

Problem 13.2.5. For $y^2 = x^3 - x$, $w + zw^2 = z^3$, and $\omega(z) = dz/\sqrt{1 + 4z^4}$.

Problem 13.2.6. For $y^2 = x^3 - x$, $\ell(z) = \sum_{m\geq 0} (-1)^m \binom{2m}{m} z^{4m+1}/(4m + 1)$. For odd n, c_n is the coefficient of x^{n-1} in $(x^3 - x)^{(n-1)/2}$.

For odd p and a curve $y^2 = f(x)$ over $\mathbb{F}_p$ with f a cubic with distinct roots over $\overline{\mathbb{F}}_p$, the coefficient A_p of x^{p-1} in $f^{(p-1)/2}$ is the *Hasse invariant*, and the curve is supersingular exactly when $A_p = 0$ [Si1, Thm. V.4.1(a)]. By Problem 13.2.6, A_p is the reduction of c_p modulo p for $y^2 = x^3 - x$, and Problems 13.2.3 and 13.2.4 recover the criterion for this curve. When $p \mid c_p$, the first term of $[p](z)$ modulo p lies beyond z^p. What is its first nonzero term?

13.3. Reduction at an inert prime

Which primes are supersingular for a curve with complex multiplication? Deuring's answer [Deu]: if E has complex multiplication by an order in K and good reduction at a prime above p, the reduction is supersingular if and only if p does not split in K. For $y^2 = x^3 - x$ these are the $p \equiv 3 \pmod 4$. We check this by hand.

Problem 13.3.1. Let $p \equiv 3 \pmod 4$. Then $\#E(\mathbb{F}_p) = p + 1$, that is, $a_p := p + 1 - \#E(\mathbb{F}_p) = 0$.

Problem 13.3.2. For $p = 4m+1$, $A_p = (-1)^m \binom{2m}{m} \not\equiv 0 \pmod p$. For $p \equiv 3 \pmod 4$, $A_p = 0$.

For $p \equiv 1 \pmod 4$ one has $a_p = \gamma + \bar\gamma$, where $\gamma \in \mathbb{Z}[\mathrm{i}]$ has $\gamma\bar\gamma = p$ and $\gamma \equiv 1 \pmod{2+2\mathrm{i}}$ [IR, Ch. 18].

Problem 13.3.3. $a_5 = -2$ and $a_{13} = 6$, in agreement with $\gamma = -1+2\mathrm{i}$ and $\gamma = 3+2\mathrm{i}$.

Now let $p \equiv 3 \pmod 4$, let $\phi(x,y) := (x^p, y^p)$ be the Frobenius endomorphism of E over $\mathbb{F}_p$, and reduce [i] modulo p into $\mathbb{F}_{p^2}$.

Problem 13.3.4. $\phi^2 = [-p]$ and $\phi \circ [\mathrm{i}] = [-\mathrm{i}] \circ \phi$. Hence $\mathrm{End}(E_{\bar{\mathbb{F}}_p})$ is not commutative.

Problem 13.3.5. Let $p \equiv 3 \pmod 4$. In the parameter $z = -x/y$, $[p](z) \equiv -z^{p^2} \pmod p$, and $[\mathrm{i}](z) = \mathrm{i}z$.

For instance $[3](z) \equiv -z^9 \pmod 3$. To describe the formal group at these primes, we use a theorem of Lubin and Tate [LT]. Let $\mathcal{O}$ be the ring of integers of a finite extension of $\mathbb{Q}_p$, with uniformizer π and residue field of order q. Lubin and Tate prove: (i) each $f \in \mathcal{O}[[X]]$ with $f(X) \equiv \pi X \bmod X^2$ and $f(X) \equiv X^q \bmod \pi$ is an endomorphism of a unique formal group F_f over $\mathcal{O}$; (ii) each $a \in \mathcal{O}$ gives a unique endomorphism $[a]_f$ of F_f with linear term aX, and $a \mapsto [a]_f$ is a ring homomorphism; (iii) for two such f, g there is a unique isomorphism $\theta\colon F_f \to F_g$ over $\mathcal{O}$ with linear term X, and it commutes with the $[a]$. By Hazewinkel's functional-equation lemma [Ha, I.2.2], the *model logarithm* $\ell_\pi(X) := X + X^q/\pi + X^{q^2}/\pi^2 + \cdots$ is the logarithm of such an F_f.

Let $p \equiv 3 \pmod 4$ and $\mathcal{O} := \mathbb{Z}_p[\mathrm{i}]$, so that $\pi := -p$ is a uniformizer and $q = p^2$.

Problem 13.3.6. The series $f := [-p]$ satisfies the hypotheses of (i), the formal group $\hat E$ of $y^2 = x^3 - x$ is F_f, and $[a]_f$ extends $\alpha \mapsto [\alpha]$ from $\mathbb{Z}[\mathrm{i}]$ to $\mathcal{O}$.

Problem 13.3.7. There is $\theta \in z + z^2\mathcal{O}[[z]]$ with $\ell = \ell_{-p} \circ \theta$. Consequently the coefficients of ℓ in degrees less than p^2 are p-integral, and $p \cdot [z^{p^2}]\,\ell \equiv -1 \pmod p$.

For $p = 3$: $[z^9]\,\ell = \frac{2}{3}$, and $3 \cdot \frac{2}{3} \equiv -1 \pmod 3$. Chapter 15 proves the same congruence for the lemniscate with binomial coefficients (Problem 15.4.2).

In the model logarithm the denominators occur only in the degrees $q, q^2, \ldots$, and there they are $p, p^2, \ldots$. For the lemniscate, Theorem 15.4.1 of Chapter 15 gives a divisibility bound for the invariant derivatives of series integral in the formal parameter. Problem 15.5.3 of that chapter gives a theta function whose fourth derivative at the origin is 4 when $p = 3$. Chapter 14 uses D^p in a single determinant; theta functions are the subject of Chapters 15 and 16. These four chapters prepare the study of derivatives of theta functions at primes that do not split in the imaginary quadratic field of the proof. The corresponding statement in the Lean formalization is `Parameters.norm_jet_minorProd_jetSeries_le`; its proof uses `CMLattice.exists_exponent_tsum`.

Hints

§13.1.

13.1.1: Write $\alpha\omega_1 = a\omega_1 + b\omega_2$ and $\alpha\omega_2 = c\omega_1 + d\omega_2$ with integers a, b, c, d. Then α is a root of $x^2 - (a+d)x + ad - bc$. If $\alpha \notin \mathbb{R}$, then $\omega_2/\omega_1 \in \mathbb{Q}(\alpha)$; if $\alpha \in \mathbb{R}$, then $b = c = 0$.

13.1.2: $\alpha \cdot 1 \in \Lambda$.

13.1.3: Compare the areas of fundamental parallelograms for Λ and $\alpha\Lambda$.

13.1.4: Apply Problem 11.1.6 with $v = \mathrm{i}u$, using Problem 11.1.7 and $\wp'^2 = 4\wp^3 - 4\wp$.

13.1.5: $x = \wp(u)$ and $y = \wp'(u)/2$.

13.1.6: Find automorphisms of the curves of order 4 and 3.

§13.2.

13.2.1: $[p](X) = (1+X)^p - 1$.

13.2.2: $D(1+X)^k = k(1+X)^k$. For $\hat{G}_a$ and $n \geq p$, $(d/dX)^p X^n = n(n-1)\cdots(n-p+1)X^{n-p}$. For $0 \leq n < p$, the derivative is zero.

13.2.3: Use the coordinate $u = \ell(z)$ for the first assertion. For the second, apply the operator congruence to the truncation of ℓ in degrees less than p.

13.2.4: Compare $\ell([p](z)) = p\,\ell(z)$ modulo (p, z^{p+1}).

13.2.5: Substitute $x = z/w$ and $y = -1/w$. Solve the quadratic for w, and compute $dx/2y = -\frac{z}{2}\,d\log x$.

13.2.6: The binomial series of $(1+4z^4)^{-1/2}$. For the second statement, $(x^3 - x)^{2m} = x^{2m}(x^2-1)^{2m}$.

§13.3.

13.3.1: $x^3 - x$ is odd, and -1 is not a square modulo p.

13.3.2: Problem 13.2.6. For the non-vanishing, $2m < p$.

13.3.3: Count the solutions of $y^2 = x^3 - x$ over $\mathbb{F}_5$ and $\mathbb{F}_{13}$.

13.3.4: $\phi^2 - a_p\phi + p = 0$ in $\mathrm{End}(E)$ [Si1, §V.2], and Problem 13.3.1. For the second relation, $\mathrm{i}^p = -\mathrm{i}$ in $\mathbb{F}_{p^2}$.

13.3.5: In the parameter z, ϕ acts on the formal group over $\mathbb{F}_p$ by $z \mapsto z^p$, and $[-1](z) = -z$.

13.3.6: Problem 13.3.5. For the last statement, use the uniqueness in (ii).

13.3.7: Use (iii). A formal group over a $\mathbb{Q}$-algebra has only one logarithm with linear term z. For the consequence, expand $\ell_{-p}(\theta(z))$ up to degree q.

References

[Deu] M. Deuring, *Die Typen der Multiplikatorenringe elliptischer Funktionenkörper*, Abh. Math. Sem. Hansischen Univ. **14** (1941), 197–272.

[Ha] M. Hazewinkel, *Formal Groups and Applications*, Academic Press, 1978.

[IR] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, 2nd ed., Grad. Texts in Math. 84, Springer, 1990.

[LT] J. Lubin and J. Tate, *Formal complex multiplication in local fields*, Ann. of Math. **81** (1965), 380–387.

[Si1] J. H. Silverman, *The Arithmetic of Elliptic Curves*, 2nd ed., Grad. Texts in Math. 106, Springer, 2009.

ONE CM DETERMINANT: MERTENS MODULO 4

Prerequisites. Legendre's formula $v_p(r!) = \sum_{e\ge 1} \lfloor r/p^e \rfloor$, Stirling's formula, Chebyshev's bound (Problem 5.1.1 in Chapter 5), and the arithmetic of $\mathbb{Z}[i]$. The invariant differential and complex uniformization of an elliptic curve [Si1, §III.5, Ch. VI], and supersingular reduction [Si1, §V.4]. The Jacobi theta function θ_1 [DLMF, §20.2], Cauchy's inequality and the argument principle. Section 14.6 also uses the prime number theorem for arithmetic progressions [MV, §11.3]. From Chapter 11, *Complex tori, theta functions and periods*: Jacobi's function ϑ (Section 11.2). From Chapter 13, *Complex multiplication and reduction at an inert prime*: the congruence $D^p \equiv \lambda D \pmod p$ for the invariant derivation of a one-dimensional formal group over $\mathbb{Z}_p$ (Section 13.2) and the supersingular reduction of $y^2 = x^3 - x$ at the primes inert in $\mathbb{Z}[i]$ (Section 13.3). Chapter 15, *The invariant derivation at a supersingular prime*, treats the derivation D^p for the lemniscate.

14.1. Mertens from the factorial

Throughout, p denotes a prime. Let $\theta(X) := \sum_{p\le X} \log p$. How much of $\log r!$ comes from each prime? Chebyshev's bound $\theta(2n) - \theta(n) \le n \log 4$ is Problem 5.1.1 of Chapter 5.

Problem 14.1.1. $\theta(X) < 2X \log 4$ for $X \ge 1$.

Problem 14.1.2. For each integer $r \ge 1$, $-\theta(r) \le \log r! - r\sum_{p\le r} \frac{\log p}{p} \le r\sum_p \frac{\log p}{p(p-1)}$.

With Stirling's formula, Problems 14.1.1 and 14.1.2 prove the following [Mer].

Theorem 14.1.1 (Mertens)**.** $\sum_{p\le X} \log p/p = \log X + O(1)$ *for* $X \ge 2$.

How much of $\log r!$ comes from each odd class modulo 4? Let

$$S_a(X) := \sum_{p\le X,\ p\equiv a \pmod 4} \frac{\log p}{p}.$$

Theorem 14.1.2. $S_a(X) = \frac{1}{2}\log X + O(1)$ *for* $a = 1, 3$ *and* $X \ge 2$.

Let χ_{-4} be the primitive real Dirichlet character modulo 4. Theorem 14.1.2 is classical, and the usual proof rests on $L(1, \chi_{-4}) \ne 0$ [MV, Ch. 4]. We replace the factorial by one determinant for each class and take $r = \lfloor X \rfloor$.

14.2. The Gaussian Vandermonde

Let $r \ge 1$ be an integer, and let $z_1, \dots, z_r$ be distinct Gaussian integers with $0 \le \operatorname{Re} z_j, \operatorname{Im} z_j < \lceil \sqrt{r} \rceil$ for each j. Let $V := \prod_{j<k}(z_k - z_j)$.

Problem 14.2.1. $|V|^2$ is a positive integer, and $\log|V|^2 \le \binom{r}{2}\log(2r)$.

Problem 14.2.2. If $p \equiv 1 \pmod 4$, then $v_p(|V|^2) \ge r^2/p - r$.

Date: November 25, 2026.

Problems 14.2.2, 14.2.1 and 14.1.1 imply the following. The counting of coincident pairs follows [PV, §2].

Theorem 14.2.1. $S_1(X) \le \frac{1}{2}\log X + O(1)$.

Problem 14.2.3. If $p \equiv 3 \pmod 4$, then $v_p(|V|^2) \ge r^2/p^2 - r$.

The estimate in Problem 14.2.3 has the summable weights $\log p/p^2$. To obtain a weight of order $1/p$, we use derivatives of integral regular functions on $y^2 = x^3 - x$. Among the odd primes this curve has supersingular reduction precisely at the primes inert in $\mathbb{Z}[i]$.

14.3. The derivation at an inert prime

Let $E\colon y^2 = x^3 - x$, $A := \mathbb{Z}[x,y]/(y^2 - x^3 + x)$, $\omega := dx/(2y)$, and $P := (0,0)$. The derivation D of A dual to ω is

$$Dx = 2y, \qquad Dy = 3x^2 - 1.$$

The automorphism $[i](x,y) := (-x, iy)$ fixes P and pulls ω back to $i\omega$. Let $d_k := (D^k x)(P)$.

Problem 14.3.1. The d_k are integers, and $d_k = 0$ unless $k \equiv 2 \pmod 4$. Moreover $d_2 = -2$, $d_6 = 144$, $d_{10} = -96768$.

Let $s = 1 + \frac{1}{4}t^4 + \cdots$ be the root of $s^4 = 1 + t^4$ with constant term 1. For odd p it lies in $\mathbb{Z}_{(p)}[[t]]$.

Problem 14.3.2. The point $x = -t^2/s^2$, $y = -t/s^3$ lies on E, t is a parameter at P, and

$$\omega = \frac{dt}{s^3} = \sum_{h\ge 0} (-1)^h b_h\, t^{4h}\, dt, \qquad b_h := \frac{\prod_{j=1}^{h}(4j-1)}{4^h h!}.$$

Thus E is a quotient of the Fermat quartic $s^4 = 1 + t^4$, and its differential is a series in t^4.

Problem 14.3.3. Let p be an odd prime. On A/pA the operator D^p is a derivation, and $D^p = cD$ for a constant $c \in \mathbb{F}_p$.

Problem 14.3.4. If $p \equiv 3 \pmod 4$, then $c = 0$.

Problem 14.3.5. If $p \equiv 3 \pmod 4$, then $p^{\lfloor k/p \rfloor}$ divides $(D^k f)(P)$ for all $f \in A$ and $k \ge 0$. For instance $3^2 \mid d_6$ and $7^2 \mid d_{14} = 268240896$.

14.4. The determinant of derivatives

Write $E(\mathbb{C}) = \mathbb{C}/\Lambda$ with $dz = \omega$ [Si1, Ch. VI], and let $w(z)$ be the x-coordinate of $P + z$. Then $w(z) = \wp(z + u_0)$ for a lift $u_0 \notin \Lambda$ of P, $D = d/dz$, $d_k = w^{(k)}(0)$, and

$$(w')^2 = 4(w^3 - w), \qquad w(0) = w'(0) = 0, \qquad w''(0) = -2.$$

For an integer $r \ge 1$, let M be the matrix whose row of index $k \ge 0$ lists the kth derivatives at 0 of

$$\frac{z^j}{j!} \quad (0 \le j < r), \qquad \frac{z^j}{j!}\, w(z) \quad (0 \le j < r). \tag{1}$$

The first r columns are the identity followed by zeros.

Problem 14.4.1. The entry of M in row k and column $z^j w/j!$ is $\binom{k}{j} d_{k-j}$ for $k \ge j$, and 0 otherwise.

A relation among the columns, restricted to rows $0, \dots, 4r$, is a pair of polynomials a, b of degree $< r$, not both zero, with $a + bw = O(z^{4r+1})$.

Problem 14.4.2. Let $Q(a,b) := (a'b - ab')^2 + 4ab(a^2 - b^2)$. Then $Q(a,b) = b^4\big((h')^2 - 4(h^3 - h)\big)$ with $h = -a/b$, when $b \ne 0$. If $a + bw = O(z^{4r+1})$ with $\deg a, \deg b < r$, then $Q(a,b) = 0$.

Problem 14.4.3. No nonconstant rational function $h \in \mathbb{C}(z)$ satisfies $(h')^2 = 4(h^3 - h)$.

Problem 14.4.4. If $h \in \{0, \pm 1\}$ and $b \ne 0$ has degree $< r$, then $b(w - h)$ vanishes at 0 to order at most $r + 1$.

Problems 14.4.2–14.4.4 prove the following.

Theorem 14.4.1. *The rows of M of index $0, \dots, 4r$ have rank $2r$.*

In order of increasing k, keep each row of M that is independent of its predecessors, until $2r$ rows are kept. Their indices are $I = \{0, \dots, r-1, k_1, \dots, k_r\}$ with $r \le k_1 < \cdots < k_r \le 4r$. Expanding along the identity block,

$$N_r := \det M_I = \det\Big[\tbinom{k_i}{j} d_{k_i - j}\Big]_{1 \le i \le r,\ 0 \le j < r}$$

is a nonzero integer. Let $L := \sum_i k_i - \binom{r}{2}$, the total order $\sum_i (k_i - j_i)$ of the derivatives in each term of this determinant.

Problem 14.4.5. For $r = 1, 2, 3$ the new rows are $\{2\}$, $\{2, 3\}$, $\{3, 4, 6\}$, and $N_r = -2,\ 12,\ 2^7 3^4$.

Problem 14.4.6. $r^2 \le L \le 4r^2$, and $v_p(N_r) \ge L/p - r$ for $p \equiv 3 \pmod 4$.

14.5. The size of the determinant

If ρ is the distance from 0 to the nearest pole of w, then $\limsup_{k\to\infty} (|d_k|/k!)^{1/k} = \rho^{-1}$. To bound N_r we first remove the poles.

Problem 14.5.1. Let H be holomorphic near 0 with $H(0) = 1$. Multiplying all the functions (1) by H does not change $\det M_I = N_r$.

Write $\Lambda = \lambda(\mathbb{Z} + \tau\mathbb{Z})$ with $\operatorname{Im}\tau > 0$, and let

$$\theta_\tau(v) := 2 \sum_{n \ge 0} (-1)^n e^{\pi i \tau (n + 1/2)^2} \sin\big((2n+1)\pi v\big),$$

so that $\theta_\tau(v) = \theta_1(\pi v \mid \tau)$ [DLMF, (20.2.1)]. In terms of Jacobi's function ϑ of Section 11.2, $\theta_\tau(v) = -i\, e^{\pi i \tau/4 + \pi i v}\, \vartheta\big(v + \frac{1+\tau}{2}\big)$. It is odd, $\theta_\tau(v+1) = -\theta_\tau(v)$, and $\theta_\tau(v + \tau) = -e^{-\pi i \tau - 2\pi i v} \theta_\tau(v)$.

Problem 14.5.2. The zeros of θ_τ are the points of $\mathbb{Z} + \tau\mathbb{Z}$, and they are simple.

Let $H(z) := \theta_\tau\big((z + u_0)/\lambda\big)^2 / \theta_\tau(u_0/\lambda)^2$.

Problem 14.5.3. H and Hw are entire, and $|H(z)|, |H(z)w(z)| \le e^{C(1+|z|^2)}$ with C independent of z.

Problem 14.5.4. For every $R > 0$, $|N_r| \le (2r)!\,(4r/R)^L e^{2Cr(1+R^2)}$. Hence $\log|N_r| \le \frac{1}{2}L\log r + O(r^2)$.

Problems 14.4.6, 14.5.4 and 14.1.1 imply the following.

Theorem 14.5.1. $S_3(X) \le \frac{1}{2}\log X + O(1)$.

Theorems 14.1.1, 14.2.1 and 14.5.1 prove Theorem 14.1.2. The proof never uses $L(1,\chi_{-4}) \ne 0$.

14.6. The linear term

Both determinant bounds allow errors of order r^2. In the derivative estimate the floors $\lfloor k/p \rfloor$ cost at most $r\theta(r)$, and in the split estimate counting coincident pairs gives an error bounded by the same quantity. The upper bounds for $|V|$ and $|N_r|$ also allow errors of order r^2 in their logarithms. So they give S_a up to $O(1)$ and say nothing of the constant term. For $\chi = \chi_{-4}$ that term involves

$$c_\chi := \frac{L'}{L}(1,\chi) = \gamma + \log\frac{\pi^2}{2\varpi^2} = 0.2456\ldots, \qquad \varpi := 2\int_0^1 \frac{dt}{\sqrt{1-t^4}},$$

where the second expression follows from Kronecker's limit formula and the value of ϖ in terms of $\Gamma(\frac{1}{4})$ (Theorem 11.3.1); it is the case $\mathbb{Q}(i)$ of the formula of Chowla and Selberg [CS]. How close can a determinant come to c_χ?

On the Vandermonde side the floors can be kept exactly. For a prime power q let $w_q(k) := \sum_{e\ge1}\lfloor k/q^e \rfloor$, and let $k!_{\mathbb{Z}[i]} := \prod_{\mathfrak{p}} \mathfrak{p}^{w_{N\mathfrak{p}}(k)}$, the kth factorial of $\mathbb{Z}[i]$ in the sense of Pólya and Bhargava. For any n Gaussian integers the Vandermonde product is divisible by $\prod_{k<n} k!_{\mathbb{Z}[i]}$ [Bh]. Write $|k!_{\mathbb{Z}[i]}|$ for the absolute value of a generator.

Problem 14.6.1. $\log\dfrac{k!}{|k!_{\mathbb{Z}[i]}|} = \frac{1}{2}w_2(k)\log 2 + \sum_{p\equiv3\ (4)}\log p\sum_{e\ \text{odd}}\left\lfloor\dfrac{k}{p^e}\right\rfloor$. For $k = 6$ both sides are $\log 36$.

For an integer $n \ge 1$, let $\beta(n) := \sum_{0\le k<n}\log|k!_{\mathbb{Z}[i]}|$.

Problem 14.6.2. $\beta(n) = \frac{1}{2}\sum_{1\le N<n}(n-N)\big(\log N + \sum_{p^e\mid N}\chi(p^e)\log p\big)$, the inner sum over prime powers $p^e > 1$.

The prime number theorem for arithmetic progressions with its fixed-modulus error term [MV, §11.3], together with the Euler product for $L(s,\chi)$, gives $\sum_{p^e\le x}\chi(p^e)\log p = o(x)$ and $\sum_{p^e\le x}\chi(p^e)\log p/p^e = -c_\chi + o(1)$.

Problem 14.6.3. $\beta(n) = \frac{n^2}{4}\log n - \frac{n^2}{4}\big(\frac{3}{2} + c_\chi\big) + o(n^2)$.

We take the points in a disc.

Problem 14.6.4. Let $R > 0$, and let μ be the uniform probability measure on the disc $|z| \le R$. For $|z| \le R$, $\int\log|z-u|\,d\mu(u) = \log R - (R^2-|z|^2)/(2R^2)$, and hence $\iint\log|z-u|\,d\mu\,d\mu = \log R - \frac{1}{4}$.

Problem 14.6.5. Let V_n be the Vandermonde product of the n Gaussian integers nearest 0. Then $\log|V_n| = \frac{n^2}{4}\log\frac{n}{\pi} - \frac{n^2}{8} + o(n^2)$.

Problem 14.6.6. $\beta(n) \le \log|V_n|$ implies $c_\chi \ge \log\pi - 1 = 0.1447\ldots$.

So even with exact divisibility the Vandermonde loses $c_\chi - \log\pi + 1 = 0.1008\ldots$ in the linear term. On the side of derivatives one may build Padé-type determinants from the Taylor coefficients of the lemniscatic sine, whose poles are the points of $\varpi\big(\frac{1+i}{2} + \mathbb{Z}[i]\big)$. We expect, from computation, that they give $c_\chi \le \log(4\pi/\varpi^2) = 0.6031\ldots$, short by the absolute constant $\log(8/\pi) - \gamma = 0.3574\ldots$; we do not know a proof of the size estimate this needs. The Vandermonde calculation uses a disc of Gaussian nodes; for the proposed derivative estimate we expect a corresponding contribution from a disc in the translated lattice of poles. The determinant argument gives a bounded error in $S_a(X)$. Even the constant term appears to require more than one determinant. The Riemann hypotheses for $\zeta(s)$ and $L(s, \chi_{-4})$ predict finer error terms for these prime sums.

The comparison of size and divisibility in this chapter illustrates the comparison in the direction amount h_{dir} of Chapter 33 (Section 33.4). In the Lean proof [GL], `Data.jetSize` gives the size term $s_\infty(j)$ for an integer $j \ge 0$, `Data.primeSum` gives the prime sum $s_{\mathrm{fin}}(y, \sigma)$ for a real y and an infinite place σ, and `Data.directionAmount` is $h_{\mathrm{dir}} = \sum_{\sigma\in\Phi}\big(s_\infty(\kappa(\sigma)) - s_{\mathrm{fin}}(\kappa(\sigma), \sigma)\big)$, with Φ and κ as in Chapter 33. At the long order of that chapter, `Data.mainPrimeSum` gives the main term s_{main} of the mean of the prime sums over the a-places, and `Data.jetSize_sub_mainPrimeSum_le` bounds the size term at that order minus s_{main} from above. In its proof the two terms proportional to $c_1 = -1 - \gamma + \operatorname{Re} L'(1, \chi_K)/L(1, \chi_K)$ cancel; here χ_K is the character of the quadratic field K of Chapter 33. Chapter 20 explains how a period of an elliptic curve with complex multiplication involves $L'(1, \chi_K)/L(1, \chi_K)$.

Exercises.

(1) If $p \equiv 1 \pmod 4$ and $h = (p-1)/4$, then $c \equiv (-1)^h b_h \not\equiv 0 \pmod p$ in Problem 14.3.3. This is the coefficient of x^{p-1} in $(x^3 - x)^{(p-1)/2}$: $c = 3, 6, 2$ for $p = 5, 13, 17$.
(2) $N_4 = 2^{12}\,3^5 \cdot 5 \cdot 7$, with new rows $4, 5, 6, 7$.

Hints

§14.1.

14.1.1: Sum Problem 5.1.1 over n near $X/2^m$.
14.1.2: Expand $\log r!$ by Legendre's formula; compare $\lfloor r/p \rfloor$ with r/p, and bound the terms with $e \ge 2$ by a geometric series.

§14.2.

14.2.1: $|V|^2$ is the norm of V.
14.2.2: Let $(p) = \mathfrak{p}\bar{\mathfrak{p}}$, and count the pairs $j < k$ with $z_j \equiv z_k$ modulo $\mathfrak{p}$ and modulo $\bar{\mathfrak{p}}$.
14.2.3: Now $\mathbb{Z}[i]/p \cong \mathbb{F}_{p^2}$, and $p \mid z$ gives $p^2 \mid |z|^2$.

§14.3.

14.3.1: Compute $D^k x$ in A, using $y^2 = x^3 - x$. For the vanishing, compare D with its transform under the automorphism $[i]$, which fixes P.
14.3.2: Differentiate $s^4 = 1 + t^4$ and examine y to first order at $t = 0$.
14.3.3: Use Leibniz's rule in characteristic p, and consider regular vector fields on the smooth projective curve.

14.3.4: In the formal group at the identity the scalar is λ of Chapter 13, Section 13.2. Compare it with the Hasse invariant [Si1, Thm. V.4.1(a)].

14.3.5: What inclusion for $D^p A$ follows by reduction modulo p?

§14.4.

14.4.2: For the second part, substitute $a = -bw + O(z^{4r+1})$, and compare the order of vanishing at 0 with the degree.

14.4.3: The map $z \mapsto (h, h'/2)$ would extend to $\mathbb{P}^1 \to E$ and pull ω back to dz. Look at $z = \infty$.

14.4.4: w has a double zero at 0.

14.4.5: Use Problem 14.4.1 and the values in Problem 14.3.1.

14.4.6: Use $k_i \geq r + i - 1$. Apply Problem 14.3.5 to each term of the determinant, and use $\lfloor m/p \rfloor > m/p - 1$.

§14.5.

14.5.1: Leibniz's rule, and the way the rows I were chosen.

14.5.2: Integrate θ'_τ/θ_τ around a period parallelogram; the sides cancel up to the jump $-2\pi i$ under $v \mapsto v + \tau$. Use oddness for the location.

14.5.3: The double zeros of H sit at the double poles of w. Bound H, Hw on one parallelogram, and translate using the functional equation of θ_τ.

14.5.4: Apply Problem 14.5.1 and Cauchy's inequality to each entry, then choose R.

§14.6.

14.6.1: $2 = -i(1+i)^2$; a split p has two primes of norm p, and an inert p is prime of norm p^2.

14.6.2: Count the multiples of each prime power p^e among the integers from 1 to k, and interchange the two finite sums.

14.6.3: $\sum_{1 \leq m < x}(x - m) = \frac{x^2}{2} - \frac{x}{2} + \frac{1}{2}\{x\}(1 - \{x\})$. For the last term with $x = n/d$, treat $d \leq \delta n$ trivially, and use partial summation on each interval where $\lfloor n/d \rfloor$ is constant.

14.6.4: $\frac{1}{2\pi}\int_0^{2\pi} \log|z - \rho e^{i\phi}|\, d\phi = \log\max(|z|, \rho)$.

14.6.5: Write $z_1, \ldots, z_n$ for the chosen nodes, scale by $R = \sqrt{n/\pi}$, and compare $n^{-2}\sum_{j<k} \log(|z_j - z_k|/R)$ with half the double integral for the unit disc in Problem 14.6.4. For fixed $0 < \varepsilon < 1/2$ the contribution from $|z_j - z_k| < \varepsilon R$ to this sum is $O(\varepsilon^2 \log(1/\varepsilon))$ as $n \to \infty$.

14.6.6: Compare the coefficients of n^2.

References

[Bh] M. Bhargava, *P-orderings and polynomial functions on arbitrary subsets of Dedekind rings*, J. reine angew. Math. **490–491** (1997), 101–128.

[CS] A. Selberg and S. Chowla, *On Epstein's zeta-function*, J. reine angew. Math. **227** (1967), 86–110.

[DLMF] *NIST Digital Library of Mathematical Functions*, `https://dlmf.nist.gov/`, Chapter 20.

[GL] L. Sernau, *GRH for Dirichlet L-functions, in Lean 4*, a shorter rewriting of the Lean proof, text by Claude, `https://github.com/lsernau/grh-lean`, commit `72fead1`, readable edition `grh/`.

[Mer] F. Mertens, *Ein Beitrag zur analytischen Zahlentheorie*, J. reine angew. Math. **78** (1874), 46–62.

[MV] H. L. Montgomery and R. C. Vaughan, *Multiplicative Number Theory I. Classical Theory*, Cambridge Stud. Adv. Math. 97, Cambridge University Press, 2007.

[PV] V. V. Volkov and F. V. Petrov, *On the interpolation of integer-valued polynomials*, J. Number Theory **133** (2013), 4224–4232; arXiv:1108.3212.

[Si1] J. H. Silverman, *The Arithmetic of Elliptic Curves*, 2nd ed., Grad. Texts in Math. 106, Springer, 2009.

THE INVARIANT DERIVATION AT A SUPERSINGULAR PRIME

Prerequisites. Formal groups of elliptic curves, their height, and supersingular reduction [Si1, Ch. IV and §§V.3–V.4]. The Weierstrass functions $\wp$ and σ [Si2, §I.5]. Legendre's formula $v_p(n!) = \sum_{i\ge1}\lfloor n/p^i\rfloor$, Kummer's theorem that $v_p\binom{m+n}{m}$ is the number of carries in the base-p addition of m and n, and the Lagrange inversion formula. From Chapter 11, *Complex tori, theta functions and periods*, we use the lattice $\varpi\mathbb{Z}[\mathrm{i}]$ of Problem 11.1.9. From Chapter 13, *Complex multiplication and reduction at an inert prime*: formal groups, their height and the invariant derivation (Section 13.2), and Problem 13.2.3; Section 15.3 proves, for the lemniscate, the congruence $D^p \equiv \lambda D \pmod p$ stated there. Chapter 16, *The isotropic plane*, continues this one.

15.1. Gaussian moments

Let $\zeta = e^{2\pi\mathrm{i}/8}$, and for integers $a, w \ge 0$ consider the moments

$$m(a,w) := \sum_{x\in\mathbb{Z}[\mathrm{i}]^2} (x_1+\zeta x_2)^a\,(x_1-\zeta x_2)^w\,e^{-\pi(|x_1|^2+|x_2|^2)}.$$

After a normalization they are rational numbers. How divisible are they by a prime $p \equiv 3 \pmod 4$, that is, by a prime that is inert in $\mathbb{Q}(\mathrm{i})$?

Let sl be the lemniscate sine, the meromorphic function with $\mathrm{sl}(0)=0$, $\mathrm{sl}'(0)=1$ and $\mathrm{sl}'^2 = 1-\mathrm{sl}^4$, and let $\varpi := 2\int_0^1 (1-t^4)^{-1/2}\,dt$. Let $\wp$ and σ be the Weierstrass functions attached to $\Lambda = \varpi\mathbb{Z}[\mathrm{i}]$, whose invariants are $g_2 = 4$ and $g_3 = 0$ (Problem 11.1.9). Let

$$F := \sigma^2\wp.$$

Problem 15.1.1. $\wp = \mathrm{sl}^{-2}$.

Problem 15.1.2. F is entire and even, $F(\mathrm{i}u) = F(u)$, and $F(u) = 1 + \frac{1}{6}u^4 + \frac{17}{2520}u^8 + O(u^{12})$.

Problem 15.1.3. Let $\vartheta_0 := \sum_{\alpha\in\mathbb{Z}[\mathrm{i}]} e^{-\pi|\alpha|^2}$. For $z\in\mathbb{C}$,

$$\sum_{\alpha\in\mathbb{Z}[\mathrm{i}]} e^{-\pi|\alpha|^2+z\alpha} = \vartheta_0\,F\Big(\frac{\varpi z}{2\pi}\Big).$$

Let $\Theta(Z_1,Z_2) := F(Z_1)F(Z_2)$ on $\mathbb{C}^2$, let $e_\pm := (1,\pm\zeta)$, and let

$$t(a,w) := \partial_s^a\partial_t^w\,\Theta(se_+ + te_-)\big|_{s=t=0}, \qquad \Theta(se_+ + te_-) = F(s+t)\,F\big(\zeta(s-t)\big).$$

Problem 15.1.4. $m(a,w) = \vartheta_0^2\,(\varpi/2\pi)^{a+w}\,t(a,w)$.

Problem 15.1.5. The numbers $t(a,w)$ are rational, $t(a,w) = t(w,a)$, and $t(a,w) = 0$ unless $a + 5w \equiv 0 \pmod 8$.

Date: November 24, 2026.

For instance $t(3,1) = 8$, $t(4,4) = 448$ and $t(8,0) = -576$. The table lists $v_{11}(t(a,w))$ for $w \le 2$ and the first nine values of $a \ge 8$ allowed by Problem 15.1.5.

$w=0$, $a=$	8	16	24	32	40	48	56	64	72
v_{11}	0	1	2	2	3	4	5	5	6
$w=1$, $a=$	11	19	27	35	43	51	59	67	75
v_{11}	0	0	1	2	2	3	4	5	5
$w=2$, $a=$	14	22	30	38	46	54	62	70	78
v_{11}	0	0	0	1	2	2	3	4	5

In this range $v_{11}(t(a,w)) = \max(\lfloor a/11 \rfloor - w, 0)$. Each derivative in the second direction seems to cost one factor of 11. By contrast, $t(8,0) = -576$ is prime to 7. This chapter treats one variable: what p divides the derivatives of a function on the lemniscate, and why F alone does not gain. The sequel, *The isotropic plane*, proves a lower bound of the shape above at every prime $p \equiv 3 \pmod 8$.

15.2. The lemniscate and its formal group

Let E be the smooth projective model of $y^2 = 1 - X^4$, with origin $(0,1)$. It is a curve of genus one with good reduction at every odd prime. The map $u \mapsto (\operatorname{sl} u, \operatorname{sl}' u)$ identifies $\mathbb{C}/L$ with $E(\mathbb{C})$, where $L \subset \Lambda$ is the period lattice of sl. The function X is a parameter at the origin, $du = dX/y$ is an invariant differential, and the addition law is

$$\operatorname{sl}(u+v) = \frac{\operatorname{sl} u \operatorname{sl}' v + \operatorname{sl} v \operatorname{sl}' u}{1 + \operatorname{sl}^2 u \operatorname{sl}^2 v}.$$

Let $D := d/du = y\, d/dX$ be the invariant derivation, and let $\ell(X) := \int_0^X (1 - v^4)^{-1/2}\, dv$ be the logarithm, so that $\operatorname{sl}(\ell(X)) = X$.

Problem 15.2.1. $\operatorname{sl} u = u - \frac{1}{10}u^5 + \frac{1}{120}u^9 - \frac{11}{15600}u^{13} + \cdots$. Only exponents $\equiv 1 \pmod 4$ occur, $\operatorname{sl}(\mathrm{i}u) = \mathrm{i} \operatorname{sl} u$, and the lattice L satisfies $\mathrm{i}L = L$.

Problem 15.2.2. The formal group law $X \oplus X'$, defined by $\operatorname{sl} u \oplus \operatorname{sl} v = \operatorname{sl}(u+v)$, has coefficients in $\mathbb{Z}[\frac{1}{2}]$, and after extension of scalars to $\mathbb{Z}[\frac{1}{2}, \mathrm{i}]$ it has the endomorphism $X \mapsto \mathrm{i}X$.

Problem 15.2.3. D maps $\mathbb{Z}[\frac{1}{2}][[X]]$ into itself, and $(D^n f)(0) = n!\,[u^n]\, f(\operatorname{sl} u)$ for $f \in \mathbb{Q}[[X]]$.

Fix an odd prime p and an embedding $\mathbb{Q}(\zeta) \hookrightarrow \overline{\mathbb{Q}}_p$, and write ζ and $\mathrm{i} = \zeta^2$ also for their images. Let $\mathcal{O} := \mathbb{Z}_p[\mathrm{i}] \subseteq \overline{\mathbb{Q}}_p$, and let v_p be the p-adic valuation normalized by $v_p(p) = 1$. For $p \equiv 3 \pmod 4$, $\mathcal{O}$ is the ring of integers of the unramified quadratic extension of $\mathbb{Q}_p$, and it contains ζ, since 8 divides $p^2 - 1$. We write $\hat{E}$ for the formal group of Problem 15.2.2 over $\mathcal{O}$.

Problem 15.2.4. For each $\alpha \in \mathcal{O}$ the series $[\alpha](X) := \operatorname{sl}(\alpha \ell(X))$ lies in $\mathcal{O}[[X]]$. It is the unique endomorphism of $\hat{E}$ with $[\alpha](X) = \alpha X + O(X^2)$.

When $p \equiv 3 \pmod 4$, this action of $\mathcal{O}$ makes $\hat{E}$ a formal $\mathcal{O}$-module of the kind constructed by Lubin and Tate [LT]; we use only Problem 15.2.4. For these primes E is supersingular and $\hat{E}$ has height two [Si1, Thm. V.3.1]. Indeed E is isogenous to $y^2 = x^3 - x$ by $(X, y) \mapsto (X^{-2}, -yX^{-3})$, and that curve is supersingular exactly when $p \equiv 3 \pmod 4$ [Si1, §V.4]. Section 15.3 shows what height two does to D.

15.3. The pth power of the invariant derivation

Let f be a function on E, regular at the origin, with expansion in $\mathcal{O}[[X]]$. Its derivatives $(D^n f)(0)$ are integral by Problem 15.2.3. We show that they are divisible by $p^{\lfloor n/p \rfloor}$ when $p \equiv 3 \pmod 4$. The smallest case is $p = 3$: $DX = y$, $D^2X = -2X^3$ and $D^3X = -6X^2 y$.

For a series f, let $\tau_Y f(X) := f(X \oplus Y)$, a series in two variables.

Problem 15.3.1. The operator induced by D^p on $(\mathcal{O}/p\mathcal{O})[[X]]$ is a derivation.

Problem 15.3.2. Let k be a field of characteristic p, and write D and τ_Y for the operators obtained by reducing the coefficients of the invariant derivation and the formal group law from $\mathbb{Z}[\frac{1}{2}]$ to k. Let δ be a continuous k-linear derivation of $k[[X]]$, acting on $k[[X, Y]]$ with Y held fixed. If $\delta\tau_Y = \tau_Y\delta$, then $\delta = (\delta X)(0)\, D$. The operator D itself commutes with τ_Y.

Thus $D^p \equiv \lambda_p D \pmod p$, with $\lambda_p \equiv (D^p X)(0) = p!\,[u^p] \operatorname{sl} u$.

Problem 15.3.3. If $p \equiv 3 \pmod 4$, then $\lambda_p \equiv 0$, so that $D^p\,\mathcal{O}[[X]] \subseteq p\,\mathcal{O}[[X]]$.

Problem 15.3.4. Let $p \equiv 3 \pmod 4$, let $f \in \mathcal{O}[[X_1, X_2]]$, and let D_1, D_2 be the invariant derivations in the two variables. Then $(D_1^a D_2^w f)(0) \in p^{\lfloor a/p \rfloor}\mathcal{O}$.

At $p \equiv 1 \pmod 4$ there is no such gain: λ_p is then a unit, since $\lambda_p \equiv p\,[X^p]\,\ell = 4^{-m}\binom{2m}{m}$ for $p = 4m + 1$ by the argument of Problem 13.2.3, and for instance $(D^5X)(0) = -12$. Katz studies congruences for invariant differential operators on Lubin–Tate formal groups of arbitrary finite height [Ka, §II].

15.4. The higher odd levels

At $p = 3$, the integer $(D^{29}X)(0)$ is divisible exactly by 3^{10}, one more than $\lfloor 29/3 \rfloor = 9$. Where does the extra factor come from? Throughout this section $p \equiv 3 \pmod 4$ and $q := p^2$, and we write

$$E_p(n) := \sum_{\substack{i \geq 1 \\ i \text{ odd}}} \Big\lfloor \frac{n}{p^i} \Big\rfloor.$$

The answer is that D^n gains $p^{E_p(n)}$.

Problem 15.4.1. $[X^{4m+1}]\,\ell = \binom{2m}{m}\big/\big(4^m(4m+1)\big)$, and ℓ has p-integral coefficients in all degrees less than q.

Problem 15.4.2. $p\,[X^q]\,\ell \equiv -1 \pmod p$. (For $p = 3$: $[X^9]\,\ell = 1/24$.)

By Problems 15.4.1 and 15.4.2, the truncation T of $\ell(X) + X^q/p$ to degree at most q lies in $X + X^2\mathbb{Z}_{(p)}[X]$. It is therefore a parameter on $\hat{E}$ over $\mathbb{Z}_{(p)}$, and $\mathcal{O}[[T]] = \mathcal{O}[[X]]$. In this parameter

$$\ell = T - \frac{T^q}{p} + O(T^{q+1}), \qquad g(z) := \ell^{-1}(z) = z + \frac{z^q}{p} + O(z^{q+1}),$$

where $O(\cdot)$ allows arbitrary rational coefficients. Write the group law in T again as $\oplus$, and define operators Δ_j on $\mathcal{O}[[T]]$ by $f(T \oplus Y) = \sum_{j \geq 0} (\Delta_j f)(T)\, Y^j$. They commute with each other and with D, and $\Delta_1 = D$.

Problem 15.4.3. For $f \in \mathcal{O}[[T]]$, $f(T \oplus g(z)) = \sum_{n \geq 0} (D^n f)(T)\, z^n/n!$. Consequently $D^p = p!\,\Delta_p$ and $D^q = q!\,(\Delta_q + D/p)$.

Problem 15.4.4. $\varepsilon := q!/p^{p+1}$ is a p-adic unit, and $D^q = p^p \varepsilon\, H$ with $H := D + p\Delta_q$.

Problem 15.4.5. Let A, B be commuting $\mathcal{O}$-linear operators on a torsion-free $\mathcal{O}$-module V with $(A-B)V \subseteq pV$. Then $(A^p - B^p)V \subseteq p^2 V$.

Let $e_j := E_p(p^j) = p^{j-1} + p^{j-3} + \cdots$, the sum over the exponents $j-i$ with $i \le j$ odd. Thus $e_0 = 0$ and $e_1 = 1$. For $j \ge 2$ one has $e_j = p^{j-1} + e_{j-2}$, and for $j \ge 1$ one has $e_j \le p\, e_{j-1} + 1$.

Problem 15.4.6. For every $j \ge 0$, as operators on $\mathcal{O}[[T]]$,

$$D^{p^j} \equiv 0 \pmod{p^{e_j}}, \qquad H^{p^j} \equiv D^{p^j} \pmod{p^{e_j+1}}.$$

Problem 15.4.7. $D^n\, \mathcal{O}[[X]] \subseteq p^{E_p(n)}\, \mathcal{O}[[X]]$ for every $n \ge 0$.

Problems 15.4.1–15.4.7 prove the following.

Theorem 15.4.1. *Let $p \equiv 3 \pmod 4$ and $f \in \mathcal{O}[[X]]$. Then $v_p\big((D^n f)(0)\big) \ge E_p(n)$ for every $n \ge 0$. The same holds for $f \in \mathcal{O}[[X_1, X_2]]$ and $D = D_1$, the invariant derivation in the first variable.*

The method gains nothing at the even levels. In Problem 15.4.4, D^q has the factor p^p, not the p^{p+1} one would get from $\lfloor q/p \rfloor + \lfloor q/q \rfloor$. The next odd level is p^3.

15.5. One theta function

The function F of Section 15.1 is not a function on E. Does it nevertheless gain? At $p = 3$ the valuations $v_3(F^{(k)}(0))$ for $k = 4, 8, \ldots, 60$ are

$$0,\ 0,\ 1,\ 1,\ 2,\ 2,\ 4,\ 4,\ 4,\ 4,\ 4,\ 5,\ 5,\ 7,\ 7,$$

far below $\lfloor k/3 \rfloor$.

Problem 15.5.1. $(\log F)'' = 2\,\mathrm{sl}^2$.

Let $b_n := (D^n X^2)(0) = n!\,[u^n]\ \mathrm{sl}^2\, u$, an element of $\mathbb{Z}[\frac{1}{2}]$. By Problem 15.5.1,

$$\log F(u) = 2 \sum_{n \ge 0} b_n \frac{u^{n+2}}{(n+2)!}.$$

Problem 15.5.2. Let $p \equiv 3 \pmod 4$ and $m := (p-3)/4$. Then $b_{p-1} \equiv -4^{-m}\binom{2m}{m} \pmod p$. In particular b_{p-1} is a p-adic unit. (For $p = 3$: $b_2 = 2$.)

Problem 15.5.3. Let $p \equiv 3 \pmod 4$. Then $F^{(p+1)}(0) \equiv 2b_{p-1} \pmod p$. Hence F, written as a series in $X = \mathrm{sl}\, u$, does not have p-integral coefficients. (For $p = 3$: $F^{(4)}(0) = 4$.)

For $p \equiv 3 \pmod 4$, the coefficient of u^{p+1} in $\log F$ is c_p/p with $c_p = 2b_{p-1}/\big((p+1)(p-1)!\big)$ a unit. For $p = 3, 7, 11$ this coefficient is $\frac{1}{6}, -\frac{1}{140}, \frac{1}{2475}$, so $c_p = \frac{1}{2}, -\frac{1}{20}, \frac{1}{225}$. By the Exercise below, for $g(u) := \exp(c_p u^{p+1}/p)$ one has $v_p(g^{(k)}(0)) = k/(p^2-1) + O(\log k)$ as k tends to infinity through multiples of $p+1$. At $p = 3$ the comparison gives $60/8 = 7.5$, while $v_3(F^{(60)}(0)) = 7$. We do not know whether $v_p(F^{(k)}(0)) = k/(p^2-1) + O(\log k)$ holds for each fixed prime $p \equiv 3 \pmod 4$ as k tends to infinity through multiples of 4; the other derivatives vanish at 0 by Problem 15.1.2.

For $p \equiv 3 \pmod 4$, the first term of the u-series of $\log F$ with a non-p-integral coefficient is $c_p u^{p+1}/p$. We next consider the product Θ in two variables. Chapter 16, *The isotropic plane*, shows that for $p \equiv 3 \pmod 8$ its restrictions to the axes in the directions $e_\pm$ are integral in the lemniscate parameter (Theorem 16.2.1). After division by the two axis restrictions, the remaining factor equals 1 on both axes (Problem 16.3.2). At $p = 7$ the axis restriction is not integral (Problem 16.2.6).

Exercise. Let c be a p-adic unit and let $g(u) := \exp(cu^{p+1}/p)$. For an integer $m \geq 0$, write $k := (p+1)m$. Then

$$v_p\big(k!\,[u^k]\,g\big) = \frac{k}{p^2-1} + \frac{s_p(m) - s_p(k)}{p-1},$$

where s_p is the sum of base-p digits.

Hints

§15.1.

15.1.1: Both sides are even, have leading term u^{-2}, and satisfy $f'^2 = 4f^3 - 4f$.

15.1.2: $\sigma(\mathrm{i}u) = \mathrm{i}\sigma(u)$ and $\wp(\mathrm{i}u) = -\wp(u)$. For the coefficients, $(\log\sigma)'' = -\wp$ and Problem 15.1.1.

15.1.3: Factor the Gaussian sum into two one-dimensional theta functions. Use Problem 11.2.7 after checking the transformation law.

15.1.4: Apply Problem 15.1.3 to each coordinate, with $z_1 = s + t$ and $z_2 = \zeta(s - t)$.

15.1.5: $F(\zeta v) = \sum_k f_{4k}(-1)^k v^{4k}$ if $F = \sum_k f_{4k} v^{4k}$. For the congruence, compare $\Theta(\zeta s e_+ - \zeta t e_-)$ with $\Theta(s e_+ + t e_-)$.

§15.2.

15.2.1: Differentiate $\mathrm{sl}'^2 = 1 - \mathrm{sl}^4$ to get $\mathrm{sl}'' = -2\,\mathrm{sl}^3$.

15.2.2: $\mathrm{sl}'\,u = \sqrt{1 - X^4}$ lies in $\mathbb{Z}[\frac{1}{2}][[X]]$.

15.2.4: Use the form of $[p]$ modulo p from [Si1, §IV.7], continuity in the (p, X)-adic topology, and [i].

§15.3.

15.3.1: Leibniz's rule.

15.3.2: Write $\delta = g(X)\,d/dX$. Apply $\delta\tau_Y = \tau_Y\delta$ to X, with δ acting on the X-variable, and set $X = 0$.

15.3.3: Use Problem 15.2.1. Alternatively, compare D^p with its pullback by [i].

15.3.4: Problem 15.3.3 in the variable X_1.

§15.4.

15.4.1: If $p \mid 4m + 1$ and $4m + 1 < q$, then $m \equiv (3p - 1)/4 \pmod p$. Count carries in $m + m$.

15.4.2: Write $p = 4r + 3$ and $m = (q - 1)/4 = rp + 3r + 2$. Take the unit parts of the factorials in $\binom{2m}{m}$ and use Wilson's theorem.

15.4.3: In the coordinate $z = \ell(T)$, translation by $g(z')$ is $z \mapsto z + z'$. For the consequences, compare coefficients of z^p and z^q in $\sum_j (\Delta_j f)(T)\,g(z)^j$.

15.4.4: Legendre's formula.

15.4.5: Factor $A^p - B^p$.

15.4.6: Induction on j, using Problems 15.4.4 and 15.4.5; apply the latter to $H^{p^{j-1}}$ and $D^{p^{j-1}}$ divided by $p^{e_{j-1}}$.

15.4.7: Write n in base p.

§15.5.

15.5.1: $(\log\sigma)'' = -\wp$, $\wp'' = 6\wp^2 - 2$, $\wp'^2 = 4\wp^3 - 4\wp$, and Problem 15.1.1.

15.5.2: By Lagrange inversion, $[u^n]\ \mathrm{sl}^k\, u = \frac{k}{n}\,[X^{n-k}]\,(X/\ell(X))^n$. Modulo p and modulo X^p, $(X/\ell(X))^p \equiv 1$.

15.5.3: In $\exp(\log F)$, only the term $2b_{p-1}u^{p+1}/(p+1)!$ of $\log F$ has p in its denominator up to degree $p+1$. For the second statement, compare with Problem 15.3.4.

References

[Ka] N. M. Katz, *Divisibilities, congruences, and Cartier duality*, J. Fac. Sci. Univ. Tokyo Sect. IA Math. **28** (1981), 667–678.

[LT] J. Lubin and J. Tate, *Formal complex multiplication in local fields*, Ann. of Math. **81** (1965), 380–387.

[Si1] J. H. Silverman, *The Arithmetic of Elliptic Curves*, 2nd ed., Grad. Texts in Math. 106, Springer, 2009.

[Si2] J. H. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*, Grad. Texts in Math. 151, Springer, 1994.

THE ISOTROPIC PLANE

Prerequisites. Chapter 15, *The invariant derivation at a supersingular prime*: the moments $t(a,w)$, the functions F and Θ and the directions $e_\pm$ of Section 15.1, the formal group $\hat{E}$ and the ring $\mathcal{O}=\mathbb{Z}_p[\mathrm{i}]$ of Section 15.2, the function E_p, Problem 15.3.4 and Theorem 15.4.1, and Section 15.5. Quasi-periods of σ and Legendre's relation [Si2, §I.5]. Decomposition groups in cyclotomic fields. Rational functions and divisors on an abelian scheme over a discrete valuation ring, at the level of the statement that a rational function whose divisor avoids a point is regular there [BK, Lemma 2.13].

16.1. The isotropic plane

The function F does not gain by itself (Problem 15.5.3). Why should Θ along the directions $e_\pm=(1,\pm\zeta)$ do better? They are the eigenlines of an action of $\mathbb{Z}[\zeta]$ on $\mathbb{Z}[\mathrm{i}]^2$. Let

$$\rho(\zeta):=\begin{pmatrix}0&1\\ \mathrm{i}&0\end{pmatrix},$$

let σ_+ be the identity of $\mathbb{Q}(\zeta)$ and σ_- the automorphism $\zeta\mapsto-\zeta$, and let $H(Z,W):=Z_1\bar{W}_1+Z_2\bar{W}_2$.

Problem 16.1.1. ρ extends to a ring homomorphism $\mathbb{Z}[\zeta]\to M_2(\mathbb{Z}[\mathrm{i}])$, and $\rho(\bar{a})=\rho(a)^*$, the conjugate transpose.

Problem 16.1.2. $\rho(a)e_\pm=\sigma_\pm(a)e_\pm$, and $H(e_+,e_-)=0$.

For each prime $p\equiv3\pmod4$, fix an embedding $\mathbb{Q}(\zeta)\hookrightarrow\mathbb{Q}_p(\mathrm{i})$ extending the embedding of $\mathbb{Q}(\mathrm{i})$ given by $\mathcal{O}=\mathbb{Z}_p[\mathrm{i}]$, and use it for v_p and for reduction modulo p. Let σ_p be the nonidentity automorphism of $\mathbb{Q}_p(\mathrm{i})/\mathbb{Q}_p$.

Now let $p\equiv3\pmod8$. The Frobenius $\zeta\mapsto\zeta^3$ generates the decomposition group of p in $\mathbb{Q}(\zeta)$, with fixed field $\mathbb{Q}(\sqrt{-2})$, $\sqrt{-2}:=\zeta+\zeta^3$. Since $\mathbb{Z}[\sqrt{-2}]$ is a principal ideal domain, $p=x^2+2y^2$ for integers x, y.

Problem 16.1.3. After replacing y by $-y$ if necessary, $a:=x+y\sqrt{-2}$ lies in $p\mathcal{O}$, while $\bar{a}=x-y\sqrt{-2}$ is a unit of $\mathcal{O}$. Moreover $\sigma_-(a)=\bar{a}$.

Problem 16.1.4. If $p\equiv7\pmod8$, then $v_p(a)=v_p(\bar{a})$ for every $a\in\mathbb{Z}[\zeta]$.

On Gaussian coefficients σ_p agrees with complex conjugation. The local form $H_p(z,w):=z_1\sigma_p(w_1)+z_2\sigma_p(w_2)$ on $\mathcal{O}^2$ reduces to the hermitian form $h(z,w):=z_1w_1^p+z_2w_2^p$ on $\mathbb{F}_{p^2}^2$. Let $\bar{e}_\pm$ be the reductions of $e_\pm\in\mathcal{O}^2$. Write $\widetilde{\zeta}$ for the reduction of ζ modulo p.

Problem 16.1.5. $h(\bar{e}_+,\bar{e}_+)=h(\bar{e}_-,\bar{e}_-)=1+\widetilde{\zeta}^{p+1}$ and $h(\bar{e}_+,\bar{e}_-)=1-\widetilde{\zeta}^{p+1}$. So for $p\equiv3\pmod8$ both lines are isotropic and h pairs them, while for $p\equiv7\pmod8$ they are anisotropic and orthogonal.

Date: November 24, 2026.

We call e_- the *partner* of e_+. In terms of embeddings, $\sigma_- = c \circ \mathrm{Frob} \circ \sigma_+$, where c is complex conjugation and $\mathrm{Frob}(\zeta) = \zeta^p$; for $p \equiv 7 \pmod 8$, by contrast, $c \circ \mathrm{Frob} \circ \sigma_+ = \sigma_+$. The derivatives along e_+ will gain, and those along the partner e_- will pay for it.

16.2. Integrality on an eigenline

Let $P(s) := \Theta(se_+) = F(s)\,F(\zeta s)$. Since F is even, $\Theta(te_-) = P(t)$, and $t(n,0) = P^{(n)}(0)$. Write $P(s) = \hat{P}(\mathrm{sl}\, s)$ with $\hat{P} \in \mathbb{Q}[[X]]$. We show that $\hat{P}$ is p-integral for every prime $p \equiv 3 \pmod 8$, unlike F.

Let L be the period lattice of sl and η the quasi-period map of Λ. Since $\eta(\mathrm{i}\omega) = -\mathrm{i}\eta(\omega)$, Legendre's relation gives $\eta(\omega) = (\pi/\operatorname{vol}\Lambda)\,\bar{\omega}$, and with the law $\sigma(u+\omega) = \pm e^{\eta(\omega)(u+\omega/2)}\sigma(u)$ [Si2, §I.5],

$$F(u+\omega) = \exp\bigl(c\,\bar{\omega}u + \tfrac{c}{2}|\omega|^2\bigr)F(u), \qquad \omega \in \Lambda, \quad c := \frac{2\pi}{\operatorname{vol}\Lambda}.$$

Problem 16.2.1. For $\gamma \in L^2$, $\Theta(Z+\gamma) = \exp\bigl(cH(Z,\gamma) + \frac{c}{2}H(\gamma,\gamma)\bigr)\Theta(Z)$. For $a \in \mathbb{Z}[\zeta]$, $a \neq 0$, the function

$$F_a(Z) := \frac{\Theta(\rho(a)Z)}{\Theta(\rho(\bar{a})Z)}$$

is L^2-periodic with $F_a(0) = 1$. It descends to a rational function on $E \times E$ defined over $\mathbb{Q}(\mathrm{i})$.

Problem 16.2.2. On $\mathbb{C}/L = E(\mathbb{C})$, the zeros of F are the two points at infinity of $y^2 = 1 - X^4$, each with multiplicity two.

Let $\mathcal{A}$ be $E \times E$ over $\mathcal{O}$, an abelian scheme on which $\mathbb{Z}[\zeta]$ acts through ρ, and write $\hat{F}_a(X_1, X_2)$ for the expansion of F_a in $X_1 = \mathrm{sl}\, Z_1$, $X_2 = \mathrm{sl}\, Z_2$.

Problem 16.2.3. $\hat{F}_a \in \mathcal{O}[[X_1, X_2]]$.

Now let $p \equiv 3 \pmod 8$, and let a be as in Problem 16.1.3.

Problem 16.2.4. $\hat{P}([a]X) = \hat{F}_a(X, [\zeta]X)\,\hat{P}([\bar{a}]X)$.

Problem 16.2.5. The coefficients of $\hat{P}$ lie in $\mathbb{Z}_{(p)}$.

Problems 16.2.1–16.2.5 and Theorem 15.4.1 prove the following.

Theorem 16.2.1. *Let $p \equiv 3 \pmod 8$. Then $\hat{P} \in \mathbb{Z}_{(p)}[[X]]$, and $v_p(t(n,0)) = v_p(P^{(n)}(0)) \geq E_p(n)$ for every $n \geq 0$.*

The induction in Problem 16.2.5 is the argument Bannai and Kobayashi use for the Kronecker theta function at ordinary primes [BK, Prop. 2.14], where one element of the CM order serves for all coordinates at once. Here $\mathcal{A}$ is supersingular, but on the line $\mathbb{C}e_+$ the element a acts by a non-unit and $\bar{a}$ by a unit. At $p \equiv 7 \pmod 8$ there is no such element (Problem 16.1.4), and at $p = 7$ the conclusion fails.

Problem 16.2.6. $\hat{P}(X) = 1 - \frac{1}{70}X^8 + O(X^{12})$. So $\hat{P}$ is not 7-integral, and $t(8,0) = -576$.

16.3. The cross term

Theorem 16.2.1 accounts for the derivatives along each axis. What remains is a factor equal to 1 on both axes. Throughout, $p \equiv 3 \pmod 8$, $X_1 = \operatorname{sl} s$, $X_2 = \operatorname{sl} t$, and $P_n := P^{(n)}(0)$.

Problem 16.3.1. $J(s,t) := \partial_s \partial_t \log \Theta(se_+ + te_-) = 2\operatorname{sl}^2(s+t) - 2\mathrm{i}\,\operatorname{sl}^2\big(\zeta(s-t)\big)$, and $J \in \mathcal{O}[[X_1, X_2]]$.

Let $M(s,t) := \int_0^s \int_0^t J$, and $M_{\alpha\beta} := \partial_s^\alpha \partial_t^\beta M(0,0)$.

Problem 16.3.2. $\Theta(se_+ + te_-) = P(s)\,P(t)\,e^{M(s,t)}$. The numbers $M_{\alpha\beta}$ vanish unless $\alpha, \beta \geq 1$, and then $M_{\alpha\beta} \in p^{E_p(\alpha-1)}\mathcal{O}$.

Problem 16.3.3. Let S and T be disjoint sets with a and w elements, respectively. Then

$$t(a,w) = \sum P_{|S_0|}\,P_{|T_0|} \prod_{B \in \pi} M_{|B\cap S|,|B\cap T|},$$

the sum over subsets $S_0 \subseteq S$, $T_0 \subseteq T$, and partitions π of $(S \smallsetminus S_0) \sqcup (T \smallsetminus T_0)$ into blocks each meeting both S and T.

Problem 16.3.4. Each term in Problem 16.3.3 has at most w blocks and valuation at least $\lfloor a/p \rfloor - w$.

Thus $v_p(t(a,w)) \geq \lfloor a/p \rfloor - w$. The *type* of a term in Problem 16.3.3 consists of $a_0 = |S_0|$, $w_0 = |T_0|$, and the numbers $m_{\alpha\beta}$ of blocks with $|B \cap S| = \alpha$ and $|B \cap T| = \beta$.

Problem 16.3.5. For every type $(a_0, w_0, (m_{\alpha\beta}))$ occurring in Problem 16.3.3, the number of terms of that type is $N \cdot a!/\big(a_0! \prod_{\alpha,\beta} (\alpha!)^{m_{\alpha\beta}}\big)$ for some positive integer N.

Problem 16.3.6. Let $\alpha_1, \ldots, \alpha_k$ be positive integers and a_0 a nonnegative integer such that $a_0 + \sum_{b=1}^k \alpha_b = a$. Let $n_i := \#\{b : p^i \mid \alpha_b\}$. Then

$$v_p\Big(\frac{a!}{a_0!\,\alpha_1! \cdots \alpha_k!}\Big) + E_p(a_0) + \sum_{b=1}^k E_p(\alpha_b - 1) \;\geq\; \sum_{\substack{i \geq 1 \\ i \text{ odd}}} \Big(\Big\lfloor \frac{a}{p^i} \Big\rfloor - n_i\Big)_+,$$

where $x_+ := \max(x, 0)$.

Problems 16.3.2–16.3.6, Theorem 16.2.1 and the symmetry $t(a,w) = t(w,a)$ of Problem 15.1.5 give the following theorem.

Theorem 16.3.1. *Let $p \equiv 3 \pmod 8$. For all integers $a, w \geq 0$,*

$$v_p\big(t(a,w)\big) \;\geq\; \max\left(\sum_{\substack{i \geq 1 \\ i \text{ odd}}} \Big(\Big\lfloor \frac{a}{p^i} \Big\rfloor - w\Big)_+,\; \sum_{\substack{i \geq 1 \\ i \text{ odd}}} \Big(\Big\lfloor \frac{w}{p^i} \Big\rfloor - a\Big)_+ \right).$$

In the table of Section 15.1 the bound is an equality whenever it is positive. It is not always sharp: $t(11,1) = -2^9 \cdot 3^6$, while the bound at $p = 3$ is 2.

Exercise. Let $M = s^p t/p$ and let $w \geq 0$ be an integer. Show that $\partial_s^{pw} \partial_t^w e^M(0,0) = (pw)!/p^w$, with valuation $v_p(w!)$. Deduce that this valuation is 0 for $0 \leq w < p$. Show also that for every $G \in \mathcal{O}[[X_1, X_2]]$, with $X_1 = \operatorname{sl} s$ and $X_2 = \operatorname{sl} t$, the valuation of $\partial_s^{pw} \partial_t^w G(0,0)$ is at least w.

16.4. Questions

Theorem 16.3.1 does not extend to $p \equiv 7 \pmod 8$: it fails at $p = 7$ (Problem 16.2.6). What fails is the choice of directions: $e_\pm$ are global eigenlines of $\mathbb{Z}[\zeta]$, and they are isotropic modulo p only for $p \equiv 3 \pmod 8$ (Problem 16.1.5). For every prime $p \equiv 3 \pmod 4$, the local form H_p on $\mathcal{O}^2$ admits a basis f, f' with $H_p(f, f) = H_p(f', f') = 0$ and $H_p(f, f') = 1$. If $p \equiv 7 \pmod 8$, neither line $\mathbb{Q}_p(\mathrm{i})e_\pm$ contains a nonzero isotropic vector. Theorem 16.3.1 concerns the two global eigenlines.

Let A be an abelian variety with complex multiplication by the ring of integers of a CM field K, with CM type Φ, and let Θ be a normalized theta function on its universal cover. Fix a prime p and an embedding $\jmath : \overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_p$, so that $\jmath \circ \phi$ determines a prime of K above p. The eigenlines $\mathbb{C}e_\phi$ ($\phi \in \Phi$) replace $e_\pm$; the case above is $K = \mathbb{Q}(\zeta)$, $\Phi = \{\sigma_+, \sigma_-\}$. The argument of Section 16.2 on $\mathbb{C}e_\phi$ needs an element a of the CM order with $\phi(a)$ a non-unit and $\phi(\bar{a})$ a unit, and such an element exists exactly when complex conjugation does not fix the prime of K determined by ϕ. In the first sum of Theorem 16.3.1, the subtracted order is w, the order along e_-. For $p \equiv 3 \pmod 8$, this is the partner direction at every odd level i, since $c \circ \mathrm{Frob}^i \circ \sigma_+ = \sigma_-$. For a general CM type, suppose p is unramified in the normal closure of K, and let Frob be the arithmetic Frobenius at the chosen prime of that closure. At a level i with $\mathrm{Frob}^i \circ \phi \notin \Phi$, is the order subtracted from the order along e_ϕ the order along $e_{c \circ \mathrm{Frob}^i \circ \phi}$?

Among the odd supersingular primes for E, the choice of a global CM element in Problem 16.1.3 fails exactly for $p \equiv 7 \pmod 8$. What derivative estimates hold in local hyperbolic coordinates at these primes? Let A_5 be the Jacobian of $y^2 = x^5 - 1$, with CM by $\mathbb{Q}(\zeta_5)$. Among odd primes $p \neq 5$, the supersingular primes for A_5 are exactly those with $p \not\equiv 1 \pmod 5$, by the Shimura–Taniyama formula for the slopes of a Jacobian with complex multiplication [LMPT]. At these primes complex conjugation is in the decomposition group of every prime above p, so there is no element of the CM order separating a prime from its conjugate. For this Jacobian at such a prime, what choices of normalized theta function, eigenline direction and formal parameter from an integral model give a restriction with p-integral coefficients? What valuation bound then holds for the derivatives in that direction at the origin?

Which step this chapter serves. This chapter gives a two-variable model for the partner terms in the divisibility estimate of the proof. Theorem 17.5.1 of Chapter 17, *Pairings on a formal group of height two*, bounds the valuation of jets along products of minors for series in the prescribed normal form and at the prescribed scale. Write $r_e(\tau)$ for the partner of the infinite place τ at level e, as defined there. Among the columns of height less than the number of rows, let a_τ count the columns of height one at τ, and let a'_τ count the other columns there. In the positive-level sum for the predicted divisibility, the summand at τ and e contains the positive part $\left(a_\tau/p^e - a_{r_e(\tau)} - a'_{r_e(\tau)}\right)_+$. The sum runs over all infinite places and over odd positive e if p is inert in $\mathbb{Q}(\sqrt{-d})$, or all positive e if $p = d$. Its weight is 1 if p is inert and $1/2$ if $p = d$. The order w along e_- in the first sum of Theorem 16.3.1 plays the analogous role. Theorem 17.5.1 assumes that the prime p does not split in $\mathbb{Q}(\sqrt{-d})$, with no separate congruence condition on p modulo 8. Theorems 16.2.1 and 16.3.1 give the estimates for the workbook moments.

In the Lean formalization. Theorem 17.5.1 is the valuation form of `Parameters.norm_jet_minorProd_le_of_has` in `grh/src/New/Derivatives/Divisibility/Count.lean` of the Lean proof [GL]. Its predicted divisibility is `predictedDivisibility` in the same file. The positive partner levels are `positivePartnerExponents` in `grh/src/Lib/CM/FormalGroup/PrimeNotation.lean`, and the partner map is `Parameters.partner` in `grh/src/New/Derivatives/FormalGroup/ThetaProducts.lean`

Hints

§16.1.

16.1.1: $\rho(\zeta)^2 = \mathrm{i}$, and $\rho(\zeta)$ is unitary.

16.1.3: $a\bar{a} = p$, and $\mathcal{O}$ is a discrete valuation ring with uniformizer p. For $p = 3$, take $x = 1$ and test the two signs of $y = \pm 1$ in the chosen embedding.

16.1.4: The Frobenius automorphism of $\mathcal{O}$ preserves v_p and maps ζ to ζ^p.

16.1.5: Compare the actions of σ_p and of complex conjugation on ζ.

§16.2.

16.2.1: $\rho(a)$ preserves L^2 because $\mathrm{i}L = L$, and $\rho(a)^*\rho(a) = \rho(a\bar{a}) = \rho(\bar{a})^*\rho(\bar{a})$. For the field of definition, compare the Taylor expansion at the origin with its transforms under automorphisms of $\mathbb{C}$ over $\mathbb{Q}(\mathrm{i})$.

16.2.2: $F = \sigma^2/\mathrm{sl}^2$ by Problem 15.1.1.

16.2.3: Use Problem 16.2.2 to locate the horizontal components of the divisor near the origin of the special fiber. How can the value $F_a(0)$ determine the remaining vertical multiplicity?

16.2.4: Evaluate $\Theta(\rho(a)Z) = F_a(Z)\Theta(\rho(\bar{a})Z)$ at $Z = se_+$, using Problems 16.1.2 and 15.2.4.

16.2.5: Induction on the degree, comparing coefficients of X^n in Problem 16.2.4.

§16.3.

16.3.1: Problem 15.5.1. Then $\mathrm{sl}(s+t) = X_1 \oplus X_2$ and $\mathrm{sl}(\zeta(s-t)) = [\zeta](X_1 \ominus X_2)$.

16.3.2: Restrict $\log\Theta$ to the two axes. For the bound, express $M_{\alpha\beta}$ through derivatives of J, and use Theorem 15.4.1.

16.3.3: Expand $e^M = \sum_k M^k/k!$ and distribute the $a+w$ labelled derivatives.

16.3.4: Each block meets T. Keep only the first level of each E_p.

16.3.5: Choose the T-parts first; after that the blocks are distinguishable.

16.3.6: Apply Legendre's formula level by level, and use $\lfloor \alpha/p^i \rfloor - \lfloor (\alpha - 1)/p^i \rfloor \in \{0, 1\}$. Each level contributes a nonnegative amount.

References

[BK] K. Bannai and S. Kobayashi, *Algebraic theta functions and the p-adic interpolation of Eisenstein–Kronecker numbers*, Duke Math. J. **153** (2010), 229–295; arXiv:math/0610163. Numbering as in the arXiv version.

[GL] L. Sernau, *GRH for Dirichlet L-functions, in Lean 4*, a shorter rewriting of the Lean proof, text by Claude, `https://github.com/lsernau/grh-lean`, commit `72fead1`, readable edition `grh/`.

[LMPT] W. Li, E. Mantovan, R. Pries and Y. Tang, *Newton polygons of cyclic covers of the projective line branched at three points*, arXiv:1805.04598.

[Si2] J. H. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*, Grad. Texts in Math. 151, Springer, 1994.

PAIRINGS ON A FORMAL GROUP OF HEIGHT TWO

Prerequisites. Chapter 13, *Complex multiplication and reduction at an inert prime*: formal groups, their logarithms and the invariant derivation D (Section 13.2), and the statement of Lubin–Tate theory with the model logarithm (Section 13.3, Problem 13.3.7). Chapter 15, *The invariant derivation at a supersingular prime*: the function E_p and Theorem 15.4.1. Chapter 16, *The isotropic plane*, Theorem 16.3.1. Chapter 2, Problem 2.1.1. The ring $\mathbb{Z}_{p^2}$ of integers of the unramified quadratic extension of $\mathbb{Q}_p$, its Teichmüller roots of unity, and its Frobenius σ, which satisfies $\sigma(a) \equiv a^p \pmod p$. Legendre's formula $v_p(n!) = (n - s_p(n))/(p-1)$, where $s_p(n)$ is the sum of the base-p digits of n. Section 17.5 uses, besides, the field $\mathbb{C}_p$, the completion of an algebraic closure of $\mathbb{Q}_p$, with its valuation $v(p) = 1$ and ring of integers $\mathcal{O}_{\mathbb{C}_p}$, and the infinite places of a cyclotomic extension of an imaginary quadratic field.

Chapter 16 found the gain at the odd levels only for $p \equiv 3 \pmod 8$, because it needed a global element of the CM order acting by a non-unit on one eigenline. What structure, visible at p alone, forces a series to be divisible by about $p^{\alpha p/(p^2-1)}$, that is by $p^{\sum_{i \text{ odd}} \alpha/p^i}$, after α derivatives? This chapter studies series $\exp(-\beta(x,y))\,U(x,y)$ with U integral, where x and y are parameters of a formal group of height two and β is a pairing, biadditive and semilinear for Frobenius up to series with integral exponential. Sections 17.1–17.4 construct the family $Q_{c,\sigma c}$ ($c \in \mathcal{O}$) and derive two divisibility bounds for series with $\beta \simeq Q_{c,\sigma c}$, in the simplest setting: one variable x and one partner variable y. Section 17.5 puts $\exp(-Q_{c,\sigma c})U$, for a unit c, into the normal form of the proof by changing the partner coordinate (Problem 17.5.2), and states the count proved there for series in that form at the infinite places of a number field.

17.1. The formal module of height two

Throughout, p is an odd prime, $\mathcal{O} := \mathbb{Z}_{p^2}$, $L := \mathbb{Q}_{p^2}$, σ is the Frobenius of L, and v is the valuation with $v(p) = 1$. A power series over L, or over a finite extension of L, is *integral* if all its coefficients have valuation ≥ 0. Let

$$\lg(X) := \sum_{j \geq 0} \frac{X^{p^{2j}}}{p^j}, \qquad \lg^*(X) := \frac{1}{p}\lg(X^p) = \sum_{j \geq 0} \frac{X^{p^{2j+1}}}{p^{j+1}}.$$

In the notation of Chapter 13, $\lg = \ell_p$ is the model logarithm for the uniformizer p of $\mathcal{O}$, whose residue field has p^2 elements.

We use Hazewinkel's functional-equation lemma [Ha, §2.2], [Ha79, (2.5)–(2.8)] in the following case. Let $f(X) \in L[[X]]$ satisfy $f(X) - p^{-1}f(X^{p^2}) \in \mathcal{O}[[X]]$ and $f(X) \equiv X$ modulo degree 2. Then: $f^{-1}(f(X) + f(Y))$ has coefficients in $\mathcal{O}$; if $g(X) \in XL[[X]]$ also satisfies $g(X) - p^{-1}g(X^{p^2}) \in \mathcal{O}[[X]]$, then $f^{-1}(g(X)) \in \mathcal{O}[[X]]$; and for $\alpha, \beta \in X\mathcal{O}[[X]]$ and $r \geq 1$, $\alpha \equiv \beta \pmod{p^r}$ if and only if $f(\alpha) \equiv f(\beta) \pmod{p^r}$.

Date: November 25, 2026.

Let $F(X,Y) := \lg^{-1}(\lg X + \lg Y)$ and $[\alpha](X) := \lg^{-1}(\alpha \lg X)$ for $\alpha \in \mathcal{O}$.

Problem 17.1.1. $F \in \mathbb{Z}_p[[X,Y]]$ and $[\alpha] \in \mathcal{O}[[X]]$, so F is a formal $\mathcal{O}$-module. Modulo degree p^2+1,

$$F(X,Y) \equiv X + Y - \frac{1}{p} \sum_{0<k<p^2} \binom{p^2}{k} X^k Y^{p^2-k}.$$

For $\zeta \in \mathcal{O}$ with $\zeta^{p^2-1} = 1$, $[\zeta](X) = \zeta X$ and $F(\zeta X, \zeta Y) = \zeta F(X,Y)$.

Problem 17.1.2. $[p](X) \equiv X^{p^2} \pmod p$. So F has height two.

Problem 17.1.3. Let ω be a root of unity of order $2(p^2-1)$, so that $\omega^{p^2-1} = -1$ and $\omega \in \mathbb{Z}_{p^4}$. Then $\ell_{-p}(\omega X) = \omega \lg(X)$. Hence for $p \equiv 3 \pmod 4$ the formal group of $y^2 = x^3 - x$ is isomorphic to F over $\mathbb{Z}_{p^4}$.

For a series f over L let f^σ be the series obtained by applying σ to the coefficients, and $f^\phi(X) := f^\sigma(X^p)$, where X^p raises every variable to the power p.

Problem 17.1.4. For f integral over $\mathcal{O}$ in any number of variables, $f^\phi \equiv f^p \pmod p$. In particular $F(X^p, Y^p) \equiv F(X,Y)^p \pmod p$.

17.2. Pairings and their normal form

In this chapter L is $\mathbb{Q}_{p^2}$, U an integral series, and in Section 17.5 κ is a shape, ι a filling, N a number of rows, r a partner rule, $\Delta(\kappa)$ the predicted divisibility, B a number of boxes, t a height and S a set of exponents; elsewhere in the workbook these letters denote the weight, an isomorphism $\mathbb{C} \simeq \bar{\mathbb{Q}}_\ell$, the level, a rank, the gap, the budget, the number $5r$ and the source forms, and K is $\mathbb{Q}(\sqrt{-d})$.

For series f, g over L write $f \simeq g$ if $f - g$ has no constant term and $\exp(f-g)$ is integral. The basic tool is Dwork's lemma [Ko, §IV.2], in the following form, which has the same proof since $\sigma(a) \equiv a^p \pmod p$: for a series Ψ over L in finitely many variables without constant term,

$$\exp \Psi \text{ is integral } \iff \Psi^\phi - p\Psi \in p\,\mathcal{O}[[X]].$$

For a series H in two variables let $H^{\mathrm{sw}}(X,Y) := H(Y,X)$ and

$$(d_F H)(X_0, X_1, X_2) := H\big(F(X_0,X_1), X_2\big) - H(X_0,X_2) - H(X_1,X_2),$$

and for a series f in one variable let $\partial_F f := f(F(X_0,X_1)) - f(X_0) - f(X_1)$. A *pairing* is a series $\beta(X,Y)$ over L such that: (i) every monomial of β contains both variables; (ii) $d_F\beta \simeq 0$ and $d_F\beta^{\mathrm{sw}} \simeq 0$; (iii) $\beta(\zeta X, Y) \simeq \beta(X, \zeta^p Y)$ for every $\zeta \in \mathcal{O}$ with $\zeta^{p^2-1} = 1$. Condition (ii) says that β is additive in each variable up to $\simeq$. Condition (iii) is semilinearity for Frobenius, since $\zeta^p = \sigma(\zeta)$.

Problem 17.2.1. The relation $\simeq$ is an equivalence relation, stable under sums and under substitution of series over $\mathcal{O}$ without constant term for the variables. If $f \simeq g$, then $d_F f \simeq d_F g$.

Problem 17.2.2. (i) $\beta(\zeta X, Y) = \beta(X, \zeta^p Y)$ for all ζ as in (iii) if and only if every monomial $X^m Y^n$ of β has $m \equiv pn \pmod{p^2-1}$. (ii) Let β be a pairing, ζ a primitive (p^2-1)th root of unity, and $G := (p^2-1)^{-1} \sum_{k=0}^{p^2-2} \beta(\zeta^k X, \zeta^{-pk} Y)$. Then G is a pairing, $G \simeq \beta$, and G satisfies the condition of (i).

For $c, c' \in L$ let

$$A(X,Y) := \sum_{0\le i\le j} \frac{X^{p^{2i}}\, Y^{p^{2j+1}}}{p^{\,i+j+1}}, \qquad Q_{c,c'}(X,Y) := c\,A(X,Y) - c'\,A(Y,X).$$

In every monomial of A the exponent of Y is the exponent of X times an odd power of p.

Problem 17.2.3. For all c, c', $Q_{c,c'}(\zeta X, Y) = Q_{c,c'}(X, \zeta^p Y)$ for every ζ as in (iii). No monomial of $\lg(X)\lg(Y)$ satisfies the congruence of Problem 17.2.2(i), and $\lg(X)\lg(Y)$ fails condition (iii): $\lg(\zeta X)\lg(Y) \not\simeq \lg(X)\lg(\zeta^p Y)$ for ζ a primitive (p^2-1)th root of unity.

Problem 17.2.4. $A(X^p, Y^p) = p\big(\lg^*(X)\lg(Y) - A(Y,X)\big)$. Hence

$$Q_{c',c}(X^p, Y^p) - p\,Q_{c,c'}(X,Y) = p\big(c'\lg^*(X)\lg(Y) - c\lg(X)\lg^*(Y)\big).$$

Problem 17.2.5. If $c \in L$ and $Q_{c,\sigma c} \simeq 0$, then $c = 0$.

Problem 17.2.6. If $c \in \mathcal{O}$, β is a pairing and $\beta \simeq Q_{c,\sigma c}$, then $p\cdot[XY^p]\,\beta \in \mathcal{O}$ and $p\cdot[XY^p]\,\beta \equiv c \pmod p$.

For $c \in \mathcal{O}$, is $Q_{c,\sigma c}$ itself a pairing? For $c \neq 0$ it is not integral, and it is not biadditive on the nose. Problems 17.2.7–17.2.10 show that it is biadditive up to $\simeq$.

Problem 17.2.7. Let Ψ be a series over L whose partial derivative $\partial\Psi/\partial X_m$ is integral, let the entries of $\mathbf{g}$ and the series V have coefficients in $\mathcal{O}$ and zero constant term. Then $\Psi(\mathbf{g} + pV\mathbf{e}_m) - \Psi(\mathbf{g}) \in p\,\mathcal{O}[[X]]$, where $\mathbf{e}_m$ is the unit vector of the variable X_m.

Problem 17.2.8. $\partial_F \lg = 0$, and $\partial_F \lg^*$ is integral.

Problem 17.2.9. For $c, c' \in \mathcal{O}$, the series $\partial_X\big(Q_{c,c'}(X,Y) - c\lg(X)\lg^*(Y)\big)$ is integral.

Problem 17.2.10. For $c \in \mathcal{O}$, $Q_{c,\sigma c}$ is a pairing.

Since $c \mapsto Q_{c,\sigma c}$ is additive, Problems 17.2.5, 17.2.6 and 17.2.10 prove the following.

Theorem 17.2.1. *For every $c \in \mathcal{O}$ the series $Q_{c,\sigma c}$ is a pairing. If $c, c' \in \mathcal{O}$ and $Q_{c,\sigma c} \simeq Q_{c',\sigma c'}$, then $c = c'$. If a pairing β satisfies $\beta \simeq Q_{c,\sigma c}$ with $c \in \mathcal{O}$, then $c \equiv p\cdot[XY^p]\,\beta \pmod p$.*

Below we use only pairings $\beta \simeq Q_{c,\sigma c}$ with $c \in \mathcal{O}$. The exactly biadditive series $\lg(X)\lg(Y)$ is not a pairing: it fails condition (iii) (Problem 17.2.3). The denominators of $Q_{c,\sigma c}$ sit only on the monomials $X^{p^{2i}}Y^{p^{2j+1}}$ and $Y^{p^{2i}}X^{p^{2j+1}}$, at odd shifts.

17.3. Odd shifts and the credit

How much do these denominators cost after α derivatives? Let ϖ_p be a root of $\varpi_p^{p^2-1} = p$, and let $\mathcal{O}' := \mathcal{O}[\varpi_p]$, so that $v(\varpi_p) = \rho$ with

$$\rho := \frac{1}{p^2-1}, \qquad \gamma_p := \frac{p}{p^2-1}.$$

Problem 17.3.1. $\gamma_p = \sum_{e\ge 0} p^{-(2e+1)}$ and $\gamma_p + \rho = 1/(p-1)$. If $n = \sum_k \delta_k p^k$ in base p, then

$$\gamma_p n - E_p(n) = \gamma_p \sum_{k \text{ even}} \delta_k + \rho \sum_{k \text{ odd}} \delta_k, \qquad v(n!) - \rho n = \gamma_p n - \frac{s_p(n)}{p-1}.$$

Hence $v(n!) - \rho n \le E_p(n) \le \gamma_p n$.

If $g(\varpi_p x)$ is integral, then $v(g^{(n)}(0)) \ge v(n!) - \rho n$. For the formal group of Chapter 15 at $p \equiv 3 \pmod 4$, the nth invariant derivative at zero of an integral series has valuation at least $E_p(n)$ (Theorem 15.4.1). By Problem 17.3.1, both bounds are the credit $\gamma_p n = \sum_{i \text{ odd}} n/p^i$ up to digit terms.

Problem 17.3.2. In $Q_{c,c'}(\varpi_p X, \varpi_p Y)$ the coefficient of $X^{p^{2i}} Y^{p^{2j+1}}$ $(i \le j)$ has valuation $v(c) + (p^{2i} + p^{2j+1})\rho - (i + j + 1)$. For $i = j = 0$ this is $v(c) + \frac{1}{p-1} - 1$; otherwise it is at least $v(c) + \frac{1}{p-1} + p - 2$. The same holds for the coefficient of $Y^{p^{2i}} X^{p^{2j+1}}$, with c' in place of c.

Problem 17.3.3. Let Ψ be a series without constant term over a finite extension L' of $L(\varpi_p)$. If every coefficient of Ψ has valuation at least $1/(p-1)$, then every coefficient of $\exp \Psi$ has valuation at least 0; for $L' = L(\varpi_p)$ they lie in $\mathcal{O}'$. For every series h over $\mathcal{O}'$ without constant term, $\exp(\varpi_p^{p+1} h/p) = \sum_{k\ge 0} (h/p)^k\, g_k$ with $g_k \in \mathcal{O}'$.

For a series h without constant term, let $\mathcal{C}(h)$ be the set of series $\sum_{k\ge 0} p^{-k} h^k g_k$ with g_k integral over $\mathcal{O}'$, the sum being finite in each degree. It is stable under multiplication by integral series. Problems 17.2.1 and 17.3.2–17.3.3 prove the following.

Theorem 17.3.1. *Let $c \in \mathcal{O}$, let β be a pairing with $\beta \simeq Q_{c,\sigma c}$, let $U \in \mathcal{O}[[x,y]]$, and let $\Theta := \exp(-\beta(x,y))\, U(x,y)$. Then*

$$\Theta(\varpi_p x, \varpi_p y) \in \mathcal{C}(h), \qquad h := \sigma(c)\, x^p y - c\, x y^p.$$

17.4. Two local estimates

Fix Θ, β, c, h as in Theorem 17.3.1. We bound the mixed derivatives at 0 of Θ, of order a in x and w in y, in two ways: in the formal parameters, with $\partial_x^a \partial_y^w$, and in the logarithm coordinates, with $D_x^a D_y^w$, where $D_x := \lg'(x)^{-1} \partial_x$ is the invariant derivation of Chapter 13. Thus $(D_x^a D_y^w \Theta)(0) = a!\, w!\, [\xi^a \eta^w]\, \Theta(\lg^{-1} \xi, \lg^{-1} \eta)$. We call x the *top* and y its *partner*.

Problem 17.4.1. If $G(\varpi_p x, \varpi_p y) \in \mathcal{C}(h)$, then

$$v\big((\partial_x^a \partial_y^w G)(0)\big) \;\ge\; v(a!) + v(w!) - \rho(a+w) - \min\Big(w,\; \Big\lfloor \frac{a}{p} \Big\rfloor + \Big\lfloor \frac{w}{p} \Big\rfloor\Big).$$

In the formal parameters the multiplication by p on the partner, $y \mapsto [p](y)$, is not linear. In the logarithm coordinates it is $\eta \mapsto p\eta$, and its effect on D_y^w is the factor p^w.

Problem 17.4.2. $\beta(x, [p]y) \simeq p\, \beta(x,y)$, and $\exp\big(-p\, Q_{c,\sigma c}(\varpi_p x, \varpi_p y)\big)$ is integral over $\mathcal{O}'$.

Problem 17.4.3. If $G(\varpi_p x, \varpi_p y)$ is integral over $\mathcal{O}'$, then $v\big((D_x^a D_y^w G)(0)\big) \ge v(a!) + v(w!) - \rho(a+w)$.

Applying Problem 17.4.1 to Θ, and Problem 17.4.3 to $\Theta(x,[p]y)$, which is allowed by Problem 17.4.2, gives the following.

Theorem 17.4.1. *For all $a,w\ge 0$:*

(A) $v\big((\partial_x^a\partial_y^w\Theta)(0)\big) \;\ge\; v(a!)+v(w!)-\rho(a+w)-\min\big(w,\ \lfloor a/p\rfloor+\lfloor w/p\rfloor\big)$,

(B) $v\big(p^w(D_x^aD_y^w\Theta)(0)\big) \;\ge\; v(a!)+v(w!)-\rho(a+w)$.

By Problem 17.3.1, both right sides are at least $\gamma_p a-w-(s_p(a)+s_p(w))/(p-1)$: the top earns the credit $\gamma_p a=\sum_{i\ \mathrm{odd}} a/p^i$, and the partner pays at most one factor of p per derivative. In (B) the payment is the explicit factor p^w, the effect of $[p]$ on the partner. The bounds use the hypothesis $\beta\simeq Q_{c,\sigma c}$ with $c\in\mathcal{O}$, the integrality of U and the formal $\mathcal{O}$-module F, not any global element of a CM order.

How are the w factors of p spent? For $\Theta=\exp(-Q_{c,\sigma c})$ with c a unit, $1\le w<p$ and $a=p^{2e+1}w$ for an integer $e\ge 0$, the loss relative to $v(a!)$ is w at each of the levels $1,3,\dots,2e+1$.

Problem 17.4.4. Let $c\in\mathcal{O}$, let w,e be integers with $1\le w<p$ and $e\ge 0$, and let $a:=p^{2e+1}w$. Then

$$\big(\partial_x^a\partial_y^w\exp(-Q_{c,\sigma c}(x,y))\big)(0)=\frac{a!\,\sigma(c)^w}{p^{(e+1)w}},$$

of valuation $v(a!)-(e+1)w$ when c is a unit. (For $p=3$, $w=1$, $e=1$: $27!\,\sigma(c)/9$, of valuation 11.)

For these orders the loss is w at each of the odd levels through $2e+1$, as in the bound $\sum_{i\ \mathrm{odd}}(\lfloor a/p^i\rfloor-w)_+$ of Theorem 16.3.1. The odd powers p^i are exactly those at which $1-\chi_K(p^i)=2$ for p inert, where χ_K is the character of $K=\mathbb{Q}(\sqrt{-d})$ (written χ_d there) (Problem 2.1.1(ii)).

17.5. Couplings and the count

In the normal form of the proof each variable has a place index, and the exponent uses couplings between a place and its partners. The proof defines couplings and the normal form for every prime p; here p stays odd.

Let Φ and V be finite sets, and let $r=(r_e)_{e\ge 0}$ be a sequence of maps $r_e\colon\Phi\to\Phi$, the *partner rule*. The variables are $z_{\tau i}$, $(\tau,i)\in\Phi\times V$, and a series is *integral* if its coefficients lie in $\mathcal{O}_{\mathbb{C}_p}$. The *couplings* are

$$\Gamma_e:=\sum_{(\tau,i)\in\Phi\times V} z_{\tau i}^{\,p^e}\,z_{r_e(\tau)i}\qquad(e\ge 0).$$

Problem 17.5.1. (i) $\Gamma_e(\alpha z)=\alpha^{p^e+1}\Gamma_e(z)$ for $\alpha\in\mathcal{O}_{\mathbb{C}_p}$. (ii) Let $\Phi=(\mathbb{Z}/q\mathbb{Z})^\times$ with $p\nmid q$, let V be a point, and $r_e(\tau):=-p^e\tau$. If $p^2\equiv 1\pmod q$ and $p\not\equiv -1\pmod q$, then for odd e the map r_e is an involution without fixed points, and Γ_e is the sum over its orbits $\{\tau,-p\tau\}$ of $z_\tau^{p^e}z_{-p\tau}+z_{-p\tau}^{p^e}z_\tau$. For $q=8$ and $p=3$, $\Gamma_1=z_1^3z_5+z_5^3z_1+z_3^3z_7+z_7^3z_3$.

Let S be a set of integers $e\ge 0$, let $\varpi\in\mathbb{C}_p$, and let $\lambda=(\lambda_{ej})_{e,j\ge 0}$ be a family in $\mathcal{O}_{\mathbb{C}_p}$. A series $\Theta\in\mathbb{C}_p[[z_{\tau i}]]$ has the *normal form* for (S,r,ϖ,λ) if there is an integral series W with

$$\Theta(\varpi z)=W(z)\exp\Big(\frac{\varpi^{p+1}}{p}\sum_{e\in S}\sum_{j\ge 0}\lambda_{ej}\,\Gamma_e^{p^j}\Big).$$

The sum converges, as $\Gamma_e^{p^j}$ is homogeneous of degree $(p^e+1)p^j$. The λ_{ej} may be any elements of $\mathcal{O}_{\mathbb{C}_p}$, and ϖ any element of $\mathbb{C}_p$.

In the next problem $\Phi = \{1,2\}$, V is a point, r_e is the transposition for every e, S is the set of odd numbers, and $z_1 = x$, $z_2 = y$; so $\Gamma_1 = x^p y + x y^p$. The series $Q_{c,c'}$ and the root ϖ_p are those of Sections 17.2 and 17.3.

Problem 17.5.2. Let $c \in \mathcal{O}^\times$, $U \in \mathcal{O}[[x,y]]$ and $\Theta := \exp(-Q_{c,\sigma c}(x,y))\,U(x,y)$. (i) Let $\epsilon \in \mathbb{C}_p$ satisfy $\epsilon^{p-1} = -\sigma(c)/c$. Then $\Theta(x,\epsilon y)$ has the normal form for $(S, r, \varpi_p, \lambda)$ with $\lambda_{10} = \sigma(c)\epsilon$ and $\lambda_{ej} = 0$ otherwise. For $p=3$, $c=1$, $U=1$, the coefficients of x^3y and of xy^3 in $\Theta(x,\epsilon y)$ are both $\epsilon/3$. (ii) If $U(0)=1$ and $c+\sigma(c) \in \mathcal{O}^\times$, then $\Theta(x,y)$ has the normal form for $(S, r, \varpi_p, \lambda)$ for no λ.

The count measures jets of such a series along products of minors. Let $\mathcal{R}$ and $\mathcal{U}$ be finite sets, $N := |\mathcal{R}|$, and take $V = \mathcal{R} \times \mathcal{U}$, so that the variables are $z_{\tau b u}$. A *shape* is a function κ on $\Phi \times \mathbb{Z}_{\geq 0}$ with values in $\mathbb{Z}_{\geq 0}$; $\kappa(\tau,t)$ is the number of columns of height t at τ, and only the heights $t < N$ will count. A *filling* ι of κ assigns a row $\iota_\tau(t,j,b) \in \mathcal{R}$ to every $\tau \in \Phi$, $t < N$, $j < \kappa(\tau,t)$ and $b < t$. For a family $\mu = (\mu_{\tau u k})$ in $\mathcal{O}_{\mathbb{C}_p}$ ($\tau \in \Phi$, $u \in \mathcal{U}$, $k \geq 0$) the product of minors is the polynomial

$$P_\mu(z) := \prod_{\tau\in\Phi} \prod_{t<N} \prod_{j<\kappa(\tau,t)} \det\Big(\sum_{u\in\mathcal{U}} \mu_{\tau u k}\, z_{\tau,\iota_\tau(t,j,b),u}\Big)_{0\leq b,k<t},$$

and the jet of Θ along it is $(P_\mu(\partial)\Theta)(0) = \sum_m m!\,[z^m]P_\mu\,[z^m]\Theta$, where $m! = \prod m_x!$ over the variables x. At each place the proof fixes a set of *standard* fillings: in a matrix of independent variables X_{bk}, their products of minors form a basis, over every commutative ring, of the span of the products for all fillings of that shape, and the sum over these fillings of the monomials $\prod_{\text{boxes}} x_{\text{entry}}$ satisfies the Weyl character formula. Substituting $X_{bk} = \sum_u \mu_{\tau u k} z_{\tau b u}$ gives the factors of P_μ at τ.

The predicted divisibility also depends on a prime d, which may equal p. In this formula $\chi_K(p) := \left(\frac{p}{d}\right)$ denotes the quadratic character of $\mathbb{Z}/d\mathbb{Z}$, evaluated at p; for $d \equiv 3 \pmod 4$ it agrees with the character of $K = \mathbb{Q}(\sqrt{-d})$ used above. Put $c_p := 1/2$ if $p = d$ and $c_p := 1$ otherwise, and let I_p° be the set of $e \geq 0$ such that $p = d$, or $\chi_K(p) = -1$ and e is odd; let $I_p := I_p^\circ \setminus \{0\}$. For a shape κ let

$$a_\tau := \sum_{t<N,\ t=1} \kappa(\tau,t), \qquad a'_\tau := \sum_{t<N,\ t\neq 1} \kappa(\tau,t), \qquad l_\tau := \sum_{t<N,\ t\neq 1} t\,\kappa(\tau,t)$$

be the numbers of columns of height one, of the other columns, and of the boxes in these. With $\tau_e := r_e(\tau)$ and $x_+ := \max(x,0)$, the *predicted divisibility* is the real number

$$\begin{aligned}\Delta(\kappa) := c_p \sum_{e\in I_p} \sum_{\tau\in\Phi} \Big[\Big(\frac{a_\tau}{p^e} - a_{\tau_e} - a'_{\tau_e}\Big)_+ + \Big(\frac{l_\tau}{p^e} - l_{\tau_e}\Big)_+ - \frac{a'_\tau}{p^e}\Big] \\ - [p=d]\,\frac{1}{2}\sum_{\tau\in\Phi} \big[\min(a_\tau, a_{\tau_0} + a'_{\tau_0}) + a'_\tau + \min(l_\tau, l_{\tau_0})\big],\end{aligned}$$

where $[p=d]$ is 1 if $p=d$ and 0 otherwise.

Problem 17.5.3. Let $\chi_K(p) = -1$, $\Phi = \{1,2\}$ with r_e the transposition for odd e (and any r_e for even e), $N \geq 2$, $\kappa(1,1) = a$, $\kappa(2,1) = w$, and $\kappa = 0$ otherwise.

Then

$$\Delta(\kappa) = \sum_{e\ge 1,\ e \text{ odd}} \Big[\Big(\frac{a}{p^e} - w \Big)_+ + \Big(\frac{w}{p^e} - a \Big)_+ \Big].$$

For one column ($a = 1$, $w = 0$) this is γ_p; for $p = 13$, $a = 200$, $w = 1$ it is $187/13$.

For $w = 0$ this is the credit $\gamma_p a$ of Section 17.3, without the loss from the digits (Problem 17.3.1); the bound of Theorem 16.3.1 has the same shape, with $\lfloor a/p^i \rfloor$ in place of a/p^i.

The count uses all infinite places of a cyclotomic extension of $\mathbb{Q}(\sqrt{-d})$. Let q_0 be a positive integer divisible by 18480, and d a prime with $q_0 \mid 2(d+1)$ and $q_0 \nmid d+1$. For an integer $s \ge 0$ let $q_1 := q_0 \cdot 3^{\lfloor \log_3 s \rfloor + 5}\, 2^s$, with $\lfloor \log_3 0 \rfloor := 0$, and let Φ be the set of infinite places of $\mathbb{Q}(\sqrt{-d}, \zeta_{q_1})$. It is a group, identified with $\mathrm{Gal}(\mathbb{Q}(\sqrt{-d}, \zeta_{q_1})/\mathbb{Q}(\sqrt{-d})) \cong (\mathbb{Z}/q_1\mathbb{Z})^\times$ through the place of a fixed embedding. Every prime factor of q_1 splits in $\mathbb{Q}(\sqrt{-d})$, so a prime p with $\chi_K(p) \ne 1$ is prime to q_1; for such p the partner rule is $r_e(\tau) := (-p^e)\,\tau$. Let $\rho(d,p) := c_p/(N_p - 1)$, where $N_p := p^2$ if $\chi_K(p) = -1$ and $N_p := p$ if $p = d$; for p inert, $\rho(d,p) = \rho$.

Theorem 17.5.1. *Let q_0, d, s, Φ be as above, let p be a prime with $\chi_K(p) \ne 1$, and fix an embedding of $\mathbb{C}$ into $\mathbb{C}_p$. Let $\mathcal{R}$, $\mathcal{U}$ be finite sets, $N := |\mathcal{R}|$, κ a shape, $\varpi \in \mathbb{C}_p$ with $v(\varpi) = \rho(d,p)$, λ a family in $\mathcal{O}_{\mathbb{C}_p}$, and $\Theta \in \mathbb{C}_p[[z_{\tau b u} : (\tau, b, u) \in \Phi \times \mathcal{R} \times \mathcal{U}]]$ a series with the normal form for $(I_p^\circ, r, \varpi, \lambda)$. Then for every standard filling of κ and every family μ in $\mathcal{O}_{\mathbb{C}_p}$,*

$$v\big((P_\mu(\partial)\Theta)(0)\big) \;\ge\; \Delta(\kappa) - fN^3\big(1 + \log_p \max(B,1)\big), \qquad B := \sum_{\tau\in\Phi} \sum_{t<N} t\,\kappa(\tau,t),$$

where $f := |\Phi|$, $\log_p$ is the real logarithm to the base p, and $v(0) = \infty$.

For a single column of height one the right side of Theorem 17.5.1 is negative: there $B = 1$, $N \ge 2$ and $\Delta(\kappa) \le 1/(p-1)$, while the error term is at least $8f$. Which series have the normal form is a separate statement; see the remark below.

In the Lean formalization. In the Lean proof [GL], the couplings, their sum and the normal form are `New.coupling`, `New.couplingSum` and `New.HasNormalForm`, in `New/Derivatives/Divisibility/NormalForm.lean`. Theorem 17.5.1 is `New.Parameters.norm_jet_minorProd_le_of_hasNormalForm`, in `New/Derivatives/Divisibility/Count.lean`, stated as the upper bound $p^{-(\Delta(\kappa) - fN^3(1+\log_p \max(B,1)))}$ for the norm of the jet; there P_μ for a standard filling is `New.minorProd` and Δ is `New.predictedDivisibility`. The jet is `New.jet`, the standard filling at one place is an element of `New.BasisTableau`, and a standard filling over all the places is an element of `New.WeylIndex`, in `Lib/GLn/SchurModule/Basic.lean`; I_p°, I_p, c_p, $\rho(d,p)$ are `New.partnerExponents`, `New.positivePartnerExponents`, `New.piPrimeValuation`, `New.varpiValuation`, in `Lib/CM/FormalGroup/PrimeNotation.lean`; the data q_0, d are `New.Parameters` and the partner rule is `New.Parameters.partner`. `New.rescale_coupling` gives the homogeneity of Γ_e, and `New.hasSum_couplingSum` gives the convergence of the sum defining the normal form; `New.IsTableauBasis` states the basis and character conditions, and `New.isTableauBasis_epsilon` proves them for the chosen set of fillings; $a_\tau, a'_\tau, l_\tau, B$ are `New.heightOneColumns`, `New.lowColumnCount`, `New.lowBoxCount`, `New.boxes`; χ_K and N_p are `New.chiK` and `New.primeNorm`; q_1/q_0 is `New.towerDeg` evaluated at s, the field is `New.Parameters.E`, and `New.Parameters.placeMulEquiv` identifies Φ with $(\mathbb{Z}/q_1\mathbb{Z})^\times$; the splitting of

the prime factors of q_1 is `New.Parameters.chiK_eq_one_of_dvd`. The corresponding statement of the Lean proof on which series have the normal form is `New.Parameters.exists_hasNormalForm`, in `New/Derivatives/FormalGroup/ThetaProducts.lean`.

Hints

§17.1.

17.1.1: Apply the functional-equation lemma with $f = \lg$ and $g = \alpha \lg$. Modulo degree p^2+1, $\lg(X) \equiv X + X^{p^2}/p$. For ζ, use $\zeta^{p^{2j}} = \zeta$. The coefficients of F lie in $\mathbb{Q}_p \cap \mathcal{O} = \mathbb{Z}_p$.

17.1.2: Compare $\lg([p]X)$ with $\lg(X^{p^2})$, using the last part of the functional-equation lemma.

17.1.3: $\omega^{p^{2j}} = (-1)^j \omega$. Then use Problem 13.3.7.

17.1.4: $(f+g)^p \equiv f^p + g^p$ and $\sigma(a) \equiv a^p$.

§17.2.

17.2.1: An integral series with constant term 1 has an integral inverse. For the last statement, express $\exp(d_F(f-g))$ through $\exp(f-g)$.

17.2.2: (i) Compare ζ^m with ζ^{pn}. (ii) Apply (iii) with ζ^k in place of ζ, and use the binomial series $(1+T)^{1/(p^2-1)}$.

17.2.3: $\zeta^{p^2} = \zeta$. For the last assertion, look at the terms linear in X of the exponential of the difference.

17.2.4: Expand $\lg^*(X)\lg(Y)$ as a double sum and split it according to the relative size of the two indices.

17.2.5: Dwork's lemma and Problem 17.2.4. Look at the coefficients of $X^p Y^{p^{2j}}$.

17.2.6: Set $\Psi := \beta - Q_{c,\sigma c}$, and use condition (i) of a pairing: which powers of Ψ contribute terms linear in X to $\exp\Psi$?

17.2.7: Expand one monomial in the changed variable, and compare the nth binomial term with the derivative.

17.2.8: For $\lg^*$, use Problems 17.1.4 and 17.2.7, and that $\lg'$ is integral.

17.2.9: Compare each exponent with its denominator.

17.2.10: The second variable follows from the first, since $Q^{\mathrm{sw}}_{c,\sigma c} = Q_{c'',\sigma c''}$ with $c'' = -\sigma c$. For the first, apply Dwork's lemma to $d_F Q_{c,\sigma c}$. The series $(d_F Q)^\phi$ differs from $d_F(Q^\phi)$ by evaluating $Q^\sigma = Q_{\sigma c,c}$ at $F(X_0^p, X_1^p)$ instead of $F(X_0,X_1)^p$. Split $Q_{\sigma c,c}$ as in Problem 17.2.9, and use Problems 17.2.4, 17.2.7, 17.2.8 and $\lg^*(Y^p) = \lg(Y) - Y$.

§17.3.

17.3.1: $\gamma_p n - E_p(n) = \sum_{i \text{ odd}} \{n/p^i\}$, the fractional parts. Legendre's formula.

17.3.3: $v(k!) < k/(p-1)$ for $k \geq 1$.

§17.4.

17.4.1: $\partial_x^a \partial_y^w$ commutes with the rescaling up to ϖ_p^{a+w}. Count the factors $x^p y$ and xy^p in a monomial of h^k of degree at most a in x and at most w in y.

17.4.2: $[p]$ is the p-fold sum for F. Problems 17.3.2 and 17.3.3.

17.4.3: The series $\varpi_p^{-1}\lg(\varpi_p T)$ has coefficients in $\mathbb{Z}_p$.

17.4.4: Only the terms of $A(y,x)$ with $i=0$ have degree less than p in y.

§17.5.

17.5.2: (i) Split off the terms $i=j=0$ of $Q_{c,\sigma c}$; Problems 17.3.2 and 17.3.3.
(ii) Compare the coefficients of $x^p y$ and xy^p on both sides.

17.5.3: Here $a'_\tau = l_\tau = 0$.

References

[GL] L. Sernau, *GRH for Dirichlet L-functions, in Lean 4*, a shorter rewriting of the Lean proof, text by Claude, `https://github.com/lsernau/grh-lean`, commit `72fead1`, readable edition `grh/`.

[Ha] M. Hazewinkel, *Formal Groups and Applications*, Academic Press, 1978.

[Ha79] M. Hazewinkel, *On formal groups. The functional equation lemma and some of its applications*, Astérisque **63** (1979), 73–82.

[Ko] N. Koblitz, *p-adic Numbers, p-adic Analysis, and Zeta-Functions*, 2nd ed., Grad. Texts in Math. 58, Springer, 1984.

HECKE NONDEGENERACY ON THE TREE

Prerequisites. Modules over a discrete valuation ring and the elementary divisor theorem [La, Ch. III, §7]. Unramified extensions of $\mathbb{Q}_p$ and Teichmüller representatives. The tree of GL_2 over a local field [SeT, Ch. II, §1]. Legendre's formula $v_p(m!) = (m - s_p(m))/(p-1)$, where $s_p(m)$ is the sum of the base-p digits of m. From Chapter 5, *Size against divisibility*: Problem 5.4.4, and the colength of a submodule, defined before Theorem 5.4.1. Section 18.7 uses the notation of Chapter 33 and the collisions and exceptional primes of Chapter 48.

In Chapter 5 an index was bounded by colengths of submodules (Theorem 5.4.1). When a gain at a prime holds on a submodule spanned by images of a Hecke operator, how large is that colength? For GL_2 and weight k we compute, at one fixed lattice, the image of the normalized sum of the values at the neighbouring lattices. When $Q > k$ its elementary divisors are expressed by binomial coefficients, and Kummer's theorem bounds them.

Why Hecke operators? The proof passes through a chain of theta lifts. At an exceptional prime $p < x_1$, let S_η denote the module of integral source forms and $Y_{\mathfrak{M}}$ the product of the scaled Hecke operators at a full mark $\mathfrak{M}$, as in Chapter 48. Chapter 48 obtains the valuation bound for the composite lift on $Y_{\mathfrak{M}}^m S_\eta + p^{j_p} S_\eta$, where m is the number of lifts; Section 48.4 gives the hypotheses on the lift and the exponent j_p. Theorem 48.5.1 gives a colength bound for each factor modulo p^{j_p}. Adding these bounds over the m copies of the product and estimating their sum bounds the colength of $Y_{\mathfrak{M}}^m S_\eta + p^{j_p} S_\eta$ in S_η. The computation at one vertex is a model for this bound. Chapter 24, *Hecke operators and theta lifts*, relates a sum over the neighbours of a lattice on a class set to a Hecke operator on modular forms through the theta lift. This chapter uses nothing from Chapter 24.

In Sections 18.1–18.6, K is the unramified extension of $\mathbb{Q}_p$ of degree f, with ring of integers W, residue field $\mathbb{F}_Q$ where $Q = p^f$, and valuation v normalized by $v(p) = 1$. We fix an integer $k \geq 1$.

18.1. The tree and the integral forms

A *lattice* is a free W-submodule of rank 2 of K^2. For a lattice L, its *sources* are the lattices L'' with $pL \subset L'' \subset L$ and $L/L'' \cong \mathbb{F}_Q$. The vertices of the tree are the classes of lattices up to homothety, and the neighbours of the class of L are the classes of its sources [SeT, Ch. II, §1].

Problem 18.1.1. The sources of L correspond to the lines of $L/pL \cong \mathbb{F}_Q^2$. There are $Q+1$ of them, and their classes are pairwise distinct.

Let V be the space of homogeneous polynomial functions of degree k on K^2, on which $\mathrm{GL}_2(K)$ acts by $(gF)(u) = F(g^{-1}u)$. For a lattice L with dual $L^\vee = \mathrm{Hom}_W(L, W)$, put

$$H(L) := \mathrm{Sym}^k(L^\vee) \subset V.$$

If x, y is the basis of $L^\vee$ dual to a basis of L, then $H(L) = \bigoplus_{j=0}^{k} W x^{k-j} y^j$.

Date: November 25, 2026.

Problem 18.1.2. $H(gL) = gH(L)$ for $g \in \mathrm{GL}_2(K)$, and $H(cL) = c^{-k}H(L)$ for $c \in K^\times$. If $L'' \subset L$, then $H(L) \subset H(L'')$.

Problem 18.1.3. Let L'' be a source of L. There is a basis x, y of $L^\vee$ such that $L''^\vee = Wx + Wp^{-1}y$. Hence the elementary divisors of $H(L)$ in $H(L'')$ are $1, p, \dots, p^k$, we have $p^k H(L'') \subset H(L)$, and $\mathrm{length}_W H(L'')/H(L) = k(k+1)/2$.

A *form* is a function F from lattices to V. It is *integral* if $F(L) \in H(L)$ for every L. The Hecke operator and its normalization are

$$(TF)(L) := \sum_{L''} F(L''), \qquad Y := p^k T,$$

where the sum runs over the $Q+1$ sources of L. Let

$$S(L) := \sum_{L''} p^k H(L'') \subset H(L).$$

Problem 18.1.4. Y maps integral forms to integral forms, and $\{(YF)(L) : F \text{ integral}\} = S(L)$.

Problem 18.1.5. $S(L) = \sum_M \mathrm{Sym}^k(M)$, the sum over the $Q+1$ lattices M with $pL^\vee \subset M \subset L^\vee$ and $L^\vee/M \cong \mathbb{F}_Q$.

Problem 18.1.6. For $Q = 2$ and $k = 2$, $S(L) = Wx^2 + 2Wxy + Wy^2$. For $k = 1$ and every Q, $S(L) = H(L)$.

The *loss* at L is $\mathrm{length}_W H(L)/S(L)$. It does not depend on L, by Problem 18.1.2. By Problem 18.1.3 a single source costs $k(k+1)/2$. The question is how much the $Q+1$ sources save together.

18.2. Elementary divisors

Let H be a free W-module of rank t and $S \subset H$ a submodule of full rank. By the elementary divisor theorem [La, Ch. III, §7] there is a basis $h_1, \dots, h_t$ of H with $S = \bigoplus_i p^{e_i} W h_i$, and the exponents $e_1 \le \cdots \le e_t$ are unique. Then $\mathrm{length}_W H/S = e_1 + \cdots + e_t$. For an integer $D \ge 0$ and a real $\varrho \in [0,1]$, we say that S is *nondegenerate up to p^D on a share ϱ* when $\#\{i : e_i \le D\} \ge \varrho t$.

Problem 18.2.1. Let A be a matrix whose rows are the coordinates, in a basis of H, of a finite generating set of S. For every integer $1 \le l \le t$, the sum $e_1 + \cdots + e_l$ is the least valuation of an $l \times l$ minor of A. In particular the e_i do not change under a finite unramified extension of W.

Problem 18.2.2. $\#\{i : e_i \le D\}$ is the largest ν for which there are $s_1, \dots, s_\nu \in S$ and $\varphi_1, \dots, \varphi_\nu \in \mathrm{Hom}_W(H, W)$ with $\varphi_a(s_b) = p^D \delta_{ab}$.

The vectors s_b are *witnesses* and the functionals φ_a are *tests*. The next problem gives a criterion on linear combinations of the tests.

Problem 18.2.3. Let Λ be a W-module and $\varphi_1, \dots, \varphi_M \colon \Lambda \to W$ linear maps. Suppose that for every $c \in W^M$ with some c_i a unit there is $G \in \Lambda$ with $v\big(\sum_i c_i \varphi_i(G)\big) \le D$. Then the image of $G \mapsto (\varphi_i(G))_i$ contains $p^D W^M$.

Problem 18.2.4. Let A, A' be $t \times t$ matrices over W with $A \equiv A' \pmod{p^T}$ for an integer $T \ge 1$, and let e_i and e_i' be the exponents of their row spans in W^t (where $e_i = \infty$ for the zero elementary divisors). Then $\min(e_i, T) = \min(e_i', T)$ for every i.

Problem 18.2.4 lets one compute exponents below T modulo p^T; Section 18.6 measures a loss in this truncated way.

18.3. Kummer's theorem

Valuations of binomial coefficients enter the formula for the exponents.

Problem 18.3.1. For $0 \le j \le n$, $v_p\binom{n}{j} = \big(s_p(j) + s_p(n-j) - s_p(n)\big)/(p-1)$, and this is the number of carries in the addition of j and $n-j$ in base p.

This is due to Kummer [Ku]; see [Gra] for a survey.

Problem 18.3.2. For $1 \le j \le n$, $v_p\binom{n}{j} \le \lfloor \log_p n \rfloor - v_p(j)$. In particular $p^{v_p\binom{n}{j}} \le n$.

Problem 18.3.3. Every $\binom{Q-1}{j}$ with $0 \le j \le Q-1$ is prime to p. For $0 < j < p^m$, $v_p\binom{p^m}{j} = m - v_p(j)$, so Problem 18.3.2 is sharp.

18.4. The Fock form

For $F = \sum_m F_m x^m$ and $G = \sum_m G_m x^m$ in $K[x_1, \dots, x_{n'}]$, with multi-indices m and $m! = \prod_s m_s!$, let

$$\langle F, G \rangle := \sum_m F_m G_m \, m!, \qquad \text{that is,} \qquad \langle x^m, x^{m'} \rangle = m! \, \delta_{mm'}.$$

In one variable over $\mathbb{C}$, with complex conjugation on the coefficients of F, this is the Gaussian inner product of Problem 5.4.4; it is the inner product of the Fock model [Ba].

Problem 18.4.1. $\langle x_s F, G \rangle = \langle F, \partial_s G \rangle$ for every s. Hence $\langle F, G \rangle = \big(F(\partial)G\big)(0)$, where $F(\partial)$ is F with each x_s replaced by $\partial/\partial x_s$.

Problem 18.4.2. For $F \in K[x,y]$ homogeneous of degree k and $a, b \in K$, $\langle (ax + by)^k, F \rangle = k! \, F(a,b)$.

Let $H = \bigoplus_{j=0}^k W x^{k-j} y^j$, and let $H^\sharp := \{G \in K[x,y]$ homogeneous of degree k : $\langle G, F \rangle \in k! \, W$ for all $F \in H\}$.

Problem 18.4.3. $H^\sharp = \bigoplus_{j=0}^k \binom{k}{j} W x^{k-j} y^j$, and $p^{\lfloor \log_p k \rfloor} H \subset H^\sharp \subset H$.

So $\langle \cdot, \cdot \rangle / k!$ is a perfect pairing between $H^\sharp$ and H. The inclusion $H^\sharp \subseteq H$ is therefore nondegenerate up to $p^{\lfloor \log_p k \rfloor}$ on all of the rank.

18.5. The span at a vertex

Fix L and a basis x, y of $L^\vee$, so that $H(L) = H$ and $H(L)^\sharp = H^\sharp$ in the notation of Section 18.4. The lattices M of Problem 18.1.5 are $M_\alpha := W(x + \alpha y) + pL^\vee$ for $\alpha \in W$, which depends only on α modulo p, and $M_\infty := Wy + pL^\vee$.

Problem 18.5.1. (i) If $Q > k$, the W-span of $\{\lambda^k : \lambda \in L^\vee\}$ is $H(L)^\sharp$. (ii) If $Q = 2$ and $k = 3$, this span has colength 1 in $H(L)^\sharp = H(L)$.

Problem 18.5.2. $\mathrm{Sym}^k(M_\alpha)$ is spanned by the $(x + \alpha y)^{k-i}(py)^i$ with $0 \le i \le k$. If $Q > k$, then for each i the W-span of $\{(x + \alpha y)^{k-i} y^i : \alpha \in W\}$ is $\bigoplus_{j=i}^k \binom{k-i}{j-i} W x^{k-j} y^j$. For the remaining line, $\mathrm{Sym}^k(M_\infty) = \bigoplus_{j=0}^k p^{k-j} W x^{k-j} y^j$.

Problems 18.1.5 and 18.5.2 give the following theorem. Problem 18.3.2 gives its last two sentences.

Theorem 18.5.1. *Suppose $Q > k$. Then $S(L) = \bigoplus_{j=0}^{k} p^{\varepsilon_j} W x^{k-j} y^j$, where the exponent ε_j of the monomial $x^{k-j}y^j$ is*

$$\varepsilon_j = \min\Big(k-j,\ \min_{0\le i\le j}\Big(i + v_p\binom{k-i}{j-i}\Big)\Big).$$

In particular $\varepsilon_j \le \min\big(j,\, k-j,\, v_p\binom{k}{j}\big) \le \lfloor \log_p k \rfloor$. So $p^{\lfloor \log_p k\rfloor} H(L) \subset S(L)$, and the loss is at most $\sum_j v_p\binom{k}{j}$.

When $Q > k$, the inclusion $S(L) \subseteq H(L)$ is therefore nondegenerate up to $p^{\lfloor \log_p k\rfloor}$ on all of the rank. The exponents can be strictly smaller than the valuations $v_p\binom{k}{j}$.

Problem 18.5.3. Assume $Q > k$. Then $\varepsilon_j = \varepsilon_{k-j}$. For $k = Q-1$ the loss is 0. For $k = p < Q$ the loss is $p-1$. For $p = 3$, $k = 6$ and $Q \ge 9$ the ε_j, in the order $j = 0, \dots, k$, are $0, 1, 1, 0, 1, 1, 0$. For $p = 2$, $k = 8$ and $Q \ge 16$ they are $0, 1, 1, 1, 1, 1, 1, 1, 0$, so the loss is 7, although $\sum_j v_2\binom{8}{j} = 17$.

What if there are few edges?

Problem 18.5.4. If $Q \le k$, then at most $Q+1$ of the exponents of $S(L)$ in $H(L)$ vanish, and the loss is at least $k - Q$. More generally, for each integer $u \ge 1$ at most $(Q+1)u$ of the exponents are less than u.

So the largest exponent is at least $(k+1)/(Q+1) - 1$, and for fixed Q the loss grows quadratically in k, since at least $k + 1 - (Q+1)u$ exponents are $\ge u$ for each u. For $Q = 2$ and $k = 15$, a Smith form computation gives the exponents $0, 0, 0, 1, 1, 1, 2, 2, 2, 3, 3, 3, 4, 4, 4, 5$, a loss of 35. For $Q = 3$ and $k = 15$ it gives $0, 0, 0, 0, 1, 1, 1, 1, 2, 2, 2, 2, 4, 4, 4, 4$. The formula of Theorem 18.5.1 assumes $Q > k$.

When $Q > k$, every exponent is at most $\lfloor \log_p k \rfloor$. Conversely, if every exponent is at most D, then $Q + 1 \ge (k+1)/(D+1)$.

18.6. Onto up to colength

At an exceptional prime $p < x_1$, Chapter 48 bounds the colength of $Y_{\mathfrak{M}}^{m} S_\eta + p^{j_p} S_\eta$ in the module S_η of integral source forms. Problem 18.2.4 illustrates this truncation over W. In this chapter U denotes an endomorphism. The colength of Chapter 5 makes sense over any commutative ring. Let O be a commutative ring, $\mathcal{V}$ an O-module, $\mathcal{V}_1, \mathcal{V}_2 \subseteq \mathcal{V}$ submodules and $\zeta \in O$. We say that *the colength of $\mathcal{V}_2$ in $\mathcal{V}_1$ divides ζ* if for every $t \ge 0$ and every family $v_1, \dots, v_t$ of elements of $\mathcal{V}_1$ there is a $t \times t$ matrix C over O with $\det C \mid \zeta$ and $\sum_j C_{ij} v_j \in \mathcal{V}_2$ for every i. No inclusion between $\mathcal{V}_1$ and $\mathcal{V}_2$ is assumed. For $p \in O$, an integer $u \ge 0$, an endomorphism U of $\mathcal{V}$ and a real number c, we say that *U is onto $\mathcal{V}_1$ modulo p^u up to colength c* if $U\mathcal{V}_1 \subseteq \mathcal{V}_1$ and there is an integer $l \ge 0$ with $l \le c$ such that the colength of $U\mathcal{V}_1 + p^u \mathcal{V}_1$ in $\mathcal{V}_1$ divides p^l.

Problem 18.6.1. Let $\mathcal{V}_1$ be a free W-module of finite rank, $\mathcal{V}_2 \subseteq \mathcal{V}_1$ a submodule, possibly with $\mathcal{V}_1/\mathcal{V}_2$ of infinite length, and $l \ge 0$ an integer. The colength of $\mathcal{V}_2$ in $\mathcal{V}_1$ divides p^l if and only if $\operatorname{length}_W \mathcal{V}_1/\mathcal{V}_2 \le l$.

Problem 18.6.2. Suppose $Q > k$, and let U be an endomorphism of $H(L)$ with $UH(L) = S(L)$, for example the diagonal one that multiplies $x^{k-j}y^j$ by p^{ε_j}. Then U is onto $H(L)$ modulo p^u up to colength c if and only if $c \ge \sum_{j=0}^{k} \min(\varepsilon_j, u)$. For $p = 3$, $k = 6$, $Q \ge 9$ and every $u \ge 1$ the least such c is 4.

Problem 18.6.3. Let $\mathcal{V}_1$ be a free W-module of finite rank. If U_1 and U_2 are onto $\mathcal{V}_1$ modulo p^u up to colengths c_1 and c_2, then U_1U_2 is onto $\mathcal{V}_1$ modulo p^u up to colength $c_1 + c_2$.

18.7. Exceptional primes and the theorem on elementary divisors

We use the notation of Chapter 33: the parameters q_0 and d, with $d \equiv q_0/2 - 1 \pmod{q_0}$, the character χ_K of $K = \mathbb{Q}(\sqrt{-d})$, the a-places Φ_a, the place $[\nu]$ of an integer ν, and the number m of lifts; and from Section 48.2 the collisions, o_p, r_p and the exceptional primes. Here a collision means a collision outside the empty set. Since $q_0/2$ is divisible by $8 \cdot 3 \cdot 5 \cdot 7 \cdot 11$, quadratic reciprocity gives $\chi_K = 1$ at every prime factor of q_0; so a prime p with $\chi_K(p) = -1$ is prime to q_0, and o_p is the order of $-p$ in $(\mathbb{Z}/q_0)^\times$.

Problem 18.7.1. Let p be a prime with $\chi_K(p) = -1$, and $e \geq 1$ odd. Then (τ, e) is a collision for one, equivalently every, $\tau \in \Phi_a$ if and only if $o_p \mid e$. So collisions exist if and only if o_p is odd, and if o_p is odd and $o_p > r_p$, every collision has $p^e \geq pm$.

The theorem on elementary divisors, Theorem 48.5.1, is stated in Chapter 48, Section 48.5, with Problem 48.5.1 on the size of its hypotheses; the proof needs it only at the exceptional primes (Section 48.4). Theorem 18.5.1 is its model, not a case of it.

In the Lean formalization. In the Lean proof [GL], Theorem 48.5.1 is `FrobeniusCycle.elementary_divisors`, with the hypotheses `IsLargeDegree`, in `New/UpperBound/ElementaryDivisors/ElementaryDivisorTheorem.le` the notion of Section 18.6 is `IsOntoUpToColength` in `New/Reduction/Lattices/Colength.lean`. The underlying divisibility predicate is `ColengthDvd` in the same file. For the use at exceptional primes, see `IsMarked.isOntoUpToColength_scaledHeckeOperator` in `MarkOperator.lean`, and the product bound `IsMarked.isOntoUpToColength_prod_scaledHeckeOperator_pow` and the exceptional case of `Data.exists_colengthDvd_gaugeLe_compositeLift` in `LocalDivisibility.lean`.

Chapters 16 and 17 study the local gain, and this chapter the colength at an exceptional prime; Chapter 48 combines the local estimates for the composite lift. The next part, from Chapter 20 on, turns to periods, masses and norms of theta lifts.

Hints

§18.1.

18.1.1: $L'' \mapsto L''/pL$. For the last statement, compare the indices in L of two homothetic sources.

18.1.2: $(gL)^\vee = (g^{-1})^\mathsf{T} L^\vee$ under the pairing. An inclusion of lattices reverses on duals.

18.1.3: Choose a basis u_1, u_2 of L with $L'' = Wu_1 + Wpu_2$, by the elementary divisor theorem.

18.1.4: For the image, take F supported on the sources of L.

18.1.5: Dualize the two inclusions defining a source.

18.1.6: List the three lattices M and expand.

§18.2.

18.2.1: Multiplying A on either side by an invertible matrix does not change the ideal generated by its $l \times l$ minors.

18.2.2: To construct a family, use the dual basis of (h_i). To bound the size of any such family, reduce the witness and test maps modulo p^{D+1}.

18.2.3: The image is a submodule of W^M; compare it with $p^D W^M$.

18.2.4: Compare the cokernels of A and A' after tensoring with $W/p^T W$.

§18.3.

18.3.1: Legendre's formula, and each carry lowers the digit sum by $p-1$.

18.3.2: Between which digit positions can a carry occur?

18.3.3: Problem 18.3.1.

§18.4.

18.4.1: Check it on monomials. Then induct on the degree of F.

18.4.2: Problem 18.4.1, or expand both sides.

18.4.3: The monomials are orthogonal. For the inclusions, Problem 18.3.2.

§18.5.

18.5.1: Use the Vandermonde matrix of Teichmüller representatives. For $Q = 2$, look for a cubic form that takes values in $2\mathbb{Z}_2$ on $\mathbb{Z}_2^2$.

18.5.2: The same Vandermonde argument, applied to the vectors $\left(\binom{k-i}{j-i}\alpha^{j-i}\right)_j$.

18.5.3: The symmetry $x \leftrightarrow y$ of $H(L)$ permutes the lattices M. Then Problem 18.3.3.

18.5.4: Reduce modulo p. For the general statement, use Problem 18.1.3 modulo p^u.

§18.6.

18.6.1: For one direction take $v_1, \dots, v_t$ a basis of $\mathcal{V}_1$. For the other, the vectors $c \in W^t$ with $\sum_j c_j v_j \in \mathcal{V}_2$ form a submodule whose quotient embeds in $\mathcal{V}_1/\mathcal{V}_2$.

18.6.2: Theorem 18.5.1 and Problem 18.6.1; then Problem 18.5.3.

18.6.3: U_1 maps $\mathcal{V}_1/(U_2\mathcal{V}_1 + p^u\mathcal{V}_1)$ onto $(U_1\mathcal{V}_1 + p^u\mathcal{V}_1)/(U_1U_2\mathcal{V}_1 + p^u\mathcal{V}_1)$.

§18.7.

18.7.1: For odd e, $-p^e = (-p)^e$, and $\tau \equiv 1 \pmod{q_0}$.

References

[Ba] V. Bargmann, *On a Hilbert space of analytic functions and an associated integral transform, Part I*, Comm. Pure Appl. Math. **14** (1961), 187–214.

[GL] L. Sernau, *GRH for Dirichlet L-functions, in Lean 4*, a shorter rewriting of the Lean proof, text by Claude, `https://github.com/lsernau/grh-lean`, commit `72fead1`, readable edition `grh/`.

[Gra] A. Granville, *Arithmetic properties of binomial coefficients I: Binomial coefficients modulo prime powers*, in: Organic Mathematics (Burnaby, 1995), CMS Conf. Proc. **20**, Amer. Math. Soc., 1997, 253–276.

[Ku] E. E. Kummer, *Über die Ergänzungssätze zu den allgemeinen Reciprocitätsgesetzen*, J. reine angew. Math. **44** (1852), 93–146.

[La] S. Lang, *Algebra*, rev. 3rd ed., Grad. Texts in Math. 211, Springer, 2002.

[SeT] J.-P. Serre, *Trees*, Springer, 1980.

THE BOUND IS ATTAINED

Prerequisites. Chapter 15, *The invariant derivation at a supersingular prime*: the lemniscate curve with parameter X, the lemniscate sine sl, the ring $\mathcal{O} = \mathbb{Z}_p[\mathrm{i}]$, the invariant derivation D, and Problems 15.2.2 and 15.2.3 (Section 15.2); the function E_p, the parameter T, the unit ε, the operator H, Problems 15.4.4 and 15.4.6, and Theorem 15.4.1 (Section 15.4). For the last section: the shape of the bound in Theorem 16.3.1, and the sparse sets of Chapter 4. Legendre's formula for $v_p(n!)$. The field $\mathbb{C}_p$, its valuation v with $v(p) = 1$, and its valuation ring.

19.1. The least valuation

Chapter 15 proves a lower bound for the divisibility of derivatives on the lemniscate. Is it the truth, or does every function gain more? Throughout this section and the next, $p \equiv 3 \pmod 4$ is a prime, $q := p^2$, $\mathcal{O} = \mathbb{Z}_p[\mathrm{i}]$, and $D = d/du$ is the invariant derivation, so that $(D^n g)(0) = n!\,[u^n]\,g(\mathrm{sl}\,u)$ for $g \in \mathcal{O}[[X]]$ (Problem 15.2.3). Recall Theorem 15.4.1: for $g \in \mathcal{O}[[X]]$ and every $n \geq 0$,

$$v_p\big((D^n g)(0)\big) \;\geq\; E_p(n) = \sum_{i \geq 1,\ i \text{ odd}} \Big\lfloor \frac{n}{p^i} \Big\rfloor .$$

Let $\mu(n)$ be the least value of $v_p((D^n g)(0))$ over $g \in \mathcal{O}[[X]]$. How far is $\mu(n)$ from $E_p(n)$?

Problem 19.1.1. $\mu(0) = 0$. For $n \geq 1$ the least value $\mu(n)$ exists and is attained by a power X^i with $1 \leq i \leq n$: $\mu(n) = \min_{1 \leq i \leq n} v_p\big(n!\,[u^n]\,\mathrm{sl}^i\,u\big)$.

Problem 19.1.2. For $p = 3$: $\mu(11) = 4$, while $E_3(11) = 3$.

So the bound of Theorem 15.4.1 is not attained in every degree. The rest of this section shows that μ is superadditive; Section 19.2 computes it at the powers of q.

Problem 19.1.3. Let $g \in \mathcal{O}[[X]]$, and write $g(X \oplus X') = \sum_{i,j} a_{ij} X^i X'^j$ with the group law $\oplus$ of Problem 15.2.2. Then $a_{ij} \in \mathcal{O}$, and for all $n, n' \geq 0$

$$(D^{n+n'} g)(0) = \sum_{i,j} a_{ij}\,(D^n X^i)(0)\,(D^{n'} X^j)(0).$$

Problem 19.1.4. $\mu(n + n') \geq \mu(n) + \mu(n')$ for all $n, n' \geq 0$.

Problem 19.1.5. Let $\phi\colon \mathbb{N} \to \mathbb{R}_{\geq 0}$ be superadditive, and let $\gamma' \geq 0$. If $\phi(N) \leq \gamma' N$ for infinitely many N, then $\phi(n) \leq \gamma' n$ for every $n \geq 0$.

19.2. The powers of q

Let

$$\gamma_p := \frac{p}{p^2 - 1} = \frac{1}{p} + \frac{1}{p^3} + \frac{1}{p^5} + \cdots .$$

Problem 19.2.1. $E_p(n) \leq \gamma_p n$ for every $n \geq 0$, and $E_p(q^j) = \gamma_p(q^j - 1)$ for every $j \geq 0$.

Date: November 26, 2026.

In the degrees q^j the function X itself attains the bound.

Problem 19.2.2. $v_p\big((D^{q^j}X)(0)\big) = E_p(q^j)$ for every $j \ge 0$. (For $p = 3$: $(D^9X)(0) = 3024$, of valuation 3; and $v_3((D^{81}X)(0)) = 30$.)

Problem 19.2.3. $v_p\big([u^{q^j}]\ \mathrm{sl}\, u\big) = -(q^j-1)/(q-1)$ for every $j \ge 0$. (For $p = 3$: $[u^9]\ \mathrm{sl}\, u = 1/120$; for $p = 7$: $v_7([u^{49}]\ \mathrm{sl}\, u) = -1$.)

Thus $\mu(q^j) = E_p(q^j) = \gamma_p(q^j - 1)$. Problems 19.1.4, 19.1.5 and 19.2.2, with Theorem 15.4.1, prove the following.

Theorem 19.2.1. *Let $p \equiv 3 \pmod 4$. For every $n \ge 0$,*

$$E_p(n) \ \le\ \mu(n) \ \le\ \gamma_p n,$$

and $\mu(q^j) = E_p(q^j)$, attained by $g = X$, for every $j \ge 0$.

Problem 19.2.4. $0 \le \gamma_p n - E_p(n) < h + 2$, where h is the number of positive odd integers i with $p^i \le n$. Hence $\mu(n) = \gamma_p n + O(\log n)$.

So γ_p is the exact rate, and Theorem 15.4.1 loses at most a logarithm in every degree. A computation of $\mu(n)$ by Problem 19.1.1 gives, for instance,

$p = 3$, n	9	10	11	20	27	40	80	81
$E_3(n)$	3	3	3	6	10	14	28	30
$\mu(n)$	3	3	4	7	10	14	29	30
$3n/8$	3.375	3.75	4.125	7.5	10.125	15	30	30.375

For $p = 7$ one finds $\mu(n) = E_7(n)$ for $n \le 54$, and $\mu(55) = 8 > E_7(55) = 7$. We have checked $E_p(n) \le \mu(n) \le \gamma_p n$ by machine for $p = 3, 7$ and $n \le 100$.

19.3. Curves with complex multiplication by $\mathbb{Q}(\sqrt{-d})$

The proof works with curves whose complex multiplication is by $K = \mathbb{Q}(\sqrt{-d})$ for a prime $d \equiv 7 \pmod 8$, and with every prime p, split, inert or ramified in K. The lemniscate is not among these curves, since $\mathbb{Q}(\mathrm{i})$ is not of this form; it serves here as the simplest case. Let q_p be the norm of a prime of K above p: $q_p = p^2$ if p is inert and $q_p = p$ otherwise. Let $\pi_p := \sqrt{-d}$ if $p = d$ and $\pi_p := p$ otherwise. In valuations and congruences we use its image under a chosen ring homomorphism $\eta\colon \mathbb{C} \to \mathbb{C}_p$; then $c_p := v(\pi_p)$ is $\frac12$ if $p = d$ and 1 otherwise. Put

$$\rho_p := \frac{c_p}{q_p - 1}, \qquad \gamma_p := \frac{1}{p-1} - \rho_p.$$

For the lemniscate at $p \equiv 3 \pmod 4$ we used $\gamma_p = p/(p^2-1)$; by Problem 19.3.1 the two agree at inert primes.

Problem 19.3.1. $\gamma_p = 0,\ p/(p^2-1),\ 1/(2(p-1))$ according as p is split, inert or ramified in K. The inert value is the rate γ_p of Section 19.2.

Let $\Lambda \subset \mathbb{C}$ be a lattice with $\mathcal{O}_K\Lambda \subseteq \Lambda$, let $t \in \mathbb{C}$ with $t \notin \Lambda$, $2t \in \Lambda$, and $\omega t, \bar\omega t \notin \Lambda$ for $\omega = (1 + \sqrt{-d})/2$, and let $a_1 \in \mathbb{C}$ with $a_1^2 = 12\wp(t)$; assume the normalization $g_2(\Lambda) = 12\wp(t)^2 - 4$. Let $y(z)$ be the Taylor series at 0 of $\frac12\big(\wp'(z+t) - a_1(\wp(z+t) - \wp(t))\big)$, with η applied to its coefficients; it begins with z. Let $\mathfrak{o}$ be the valuation ring of $\mathbb{C}_p$, and $\mathfrak{o}[[y]]$ the ring of series $\Psi(y(z))$ with $\Psi \in \mathfrak{o}[[W]]$. The proof establishes the following.

Theorem 19.3.1. *Let $d \equiv 7 \pmod 8$ be prime, Λ, t, a_1 as above, p a prime and $\eta\colon \mathbb{C} \to \mathbb{C}_p$ a ring homomorphism. For every $n \geq 0$ there is $g \in \mathfrak{o}[[y]]$ with*

$$v\big(n!\,[z^n]g\big) \;\leq\; \gamma_p n.$$

In the Lean formalization. In the Lean proof [GL] this is `CMLattice.katz_divisibility_limit`, in `New/Derivatives/Sharpness/OneCurve.lean` of the readable edition, stated with norms: $|n!\,[z^n]g| \geq (p^{-\gamma_p})^n$. The Lean proof establishes it as in Sections 19.1 and 19.2: the greatest norm of $n!\,[z^n]g$ over $g \in \mathfrak{o}[[y]]$ is attained by a power of y, it is submultiplicative in n, and a lemma of Fekete's type (Problem 19.1.5, in multiplicative form) carries a bound at the degrees q_p^j to all degrees. At those degrees it uses, in place of Problem 19.2.2, the part y_1 of y in degrees $\equiv 1 \pmod{q_p - 1}$: the coefficient $[z^{q_p^j}]\,y_1$ has valuation $-(q_p^j - 1)\rho_p$, as in Problem 19.2.3. It proves this by rescaling: for some ϖ of valuation ρ_p the series $y_1(\varpi z)/\varpi$ is integral and congruent to $\sum_{j\geq 0} z^{q_p^j}$ modulo π_p.

The proof uses Theorem 19.3.1 in many variables, along a linear form whose coefficients are units.

Problem 19.3.2. Return to the lemniscate of Section 19.1, with $p \equiv 3 \pmod 4$ and $\mathcal{O} = \mathbb{Z}_p[\mathrm{i}]$. Let $g \in \mathcal{O}[[X]]$, let $\beta_j \in \mathcal{O}^\times$ for j in a finite set J, and let $F\big((u_j)_{j\in J}\big) := g\big(\mathrm{sl}(\sum_{j\in J} \beta_j u_j)\big)$. For every multi-index ν,

$$\nu!\,[u^\nu]\,F = \beta^\nu\,(D^{|\nu|}g)(0),$$

so that $v_p(\nu!\,[u^\nu]\,F) = v_p\big((D^{|\nu|}g)(0)\big)$; for every ν there is such a g for which this value is at most $\gamma_p|\nu| = p|\nu|/(p^2-1)$.

19.4. Many places

In the proof the one-copy variables are indexed by the infinite places $\tau \in \Phi$ of the CM field E, each with its weight $\kappa(\tau)$, as in Chapter 33. For a prime p let $\mathcal{I}_p$ be the set of odd $e \geq 1$ if p is inert, of all $e \geq 1$ if $p = d$, and empty if p splits. For $e \in \mathcal{I}_p$ the *partner* of τ is $[-p^e]\tau$. The divisibility predicted at p for a derivative of order κ_0 in the variable of τ is

$$s_{\mathrm{fin},p}(\kappa_0, \tau) = v(\pi_p) \sum_{e\in\mathcal{I}_p} \Big(\frac{\kappa_0}{p^e} - \kappa([-p^e]\tau)\Big)_+,$$

the part at p of the prime sum of Chapter 33, divided by $2\log p$, without the cutoff at a. Each term has the shape of the bound in Theorem 16.3.1, with the weight of the partner in the place of w.

Problem 19.4.1. For real $\kappa_0 \geq 0$, $s_{\mathrm{fin},p}(\kappa_0, \tau) \leq \gamma_p\kappa_0$, with equality if κ vanishes at all partners of τ. Hence $\sum_\tau s_{\mathrm{fin},p}(\kappa(\tau), \tau) \leq \gamma_p \sum_\tau \kappa(\tau)$.

Setting all partner weights to zero in $s_{\mathrm{fin},p}(\kappa_0, \tau)$ gives $\gamma_p\kappa_0$. By Theorem 19.3.1, a larger linear rate cannot hold as a divisibility bound for every series on one curve. In independent variables the least valuations add.

Problem 19.4.2. Use the lemniscate, the prime $p \equiv 3 \pmod 4$, the ring $\mathcal{O}$ and the function μ of Section 19.1. For $n, n' \geq 0$, the least value of $v_p\big((D_1^n D_2^{n'} g)(0)\big)$ over $g \in \mathcal{O}[[X_1, X_2]]$, with D_1, D_2 the invariant derivations in the two variables, is $\mu(n) + \mu(n')$.

If $e \in \mathcal{I}_p$ and both $\kappa(\tau)$ and $\kappa([-p^e]\tau)$ are positive, then $s_{\mathrm{fin},p}(\kappa(\tau),\tau) < \gamma_p\kappa(\tau)$: a partner lowers the prediction. By Problem 4.1.4, for a prime $p \le kt$ with $p \nmid q_1$ and for $0 < i < j < l_0(s)$, the places τ, $[-p]^i\tau$, $[-p]^j\tau$ are not all in Φ_b. Call (τ, e) a *near pair* if $e \in \mathcal{I}_p$, $2e < l_0(s)$, and both τ and its partner lie in Φ_b. For each nonsplit prime $p \le k$, the proof uses the sparsity of Φ_b (Chapter 4) to show that distinct near pairs have distinct starts and distinct ends, and that no end is a start.

Problem 19.4.3. Let Γ be an abelian group, $\xi \in \Gamma$, $\mathcal{B} \subseteq \Gamma$ and $L \ge 1$, such that for no $x \in \Gamma$ and $0 < i < j < L$ are x, $\xi^i x$, $\xi^j x$ all in $\mathcal{B}$. Call (x, e) near if $0 < 2e < L$ and $x, \xi^e x \in \mathcal{B}$. Then two near pairs with the same start, or with the same end, are equal, and the end of a near pair is never the start of one.

For every degree vector in the range of Theorem 63.5.1, the proof chooses one nonzero scalar c_{att} for all primes. For each modulus and p-adic place in that theorem, some Taylor coefficient on twelve copies, normalized as in the theorem, has valuation at most $\sum_{\tau\in\Phi} s_{\mathrm{fin},p}(\kappa(\tau),\tau)$. This sum also enters the divisibility bound for the composite lift in Chapter 48. The proof uses Theorem 19.3.1 in several variables and the sparsity of Φ_b (Problem 19.4.3). Chapter 63 takes this up: the version at many places, on twelve copies of the variables.

Hints

§19.1.

19.1.1: Write $g = \sum_i a_i X^i$ with $a_i \in \mathcal{O}$; $\mathrm{sl}^i u$ begins with u^i. Use the ultrametric inequality.

19.1.2: $\mathrm{sl}^i u$ has only exponents $\equiv i \pmod 4$, and $[u^{11}]\,\mathrm{sl}^3 u = 11/200$. As a numerical check, $(D^{11}X^3)(0) = 2195424$.

19.1.3: Expand $g(\mathrm{sl}(u + w))$ in two ways and compare the coefficients of $u^n w^{n'}$.

19.1.4: Problem 19.1.3.

19.1.5: Treat $n = 0$ separately. For $n > 0$, write $N = sn + s'$ with $0 \le s' < n$.

§19.2.

19.2.1: Geometric series.

19.2.2: Start with $(DX)(0) = 1$. For the induction step take $j \ge 1$. $X \in \mathcal{O}[[T]]$; $D^{q^j} = (p^p\varepsilon)^{q^{j-1}} H^{q^{j-1}}$ by Problem 15.4.4; compare $H^{q^{j-1}}$ with $D^{q^{j-1}}$ by Problem 15.4.6 at level $2j - 2$.

19.2.3: Legendre's formula for $v_p(q^j!)$.

19.2.4: Write $\gamma_p n - E_p(n)$ as a sum over odd i of $n/p^i - \lfloor n/p^i \rfloor$, and bound the terms with $p^i > n$ by a geometric series.

§19.3.

19.3.2: $(D^n g)(0) = n!\,[w^n]\,g(\mathrm{sl}\, w)$, and the multinomial theorem; Theorem 19.2.1.

§19.4.

19.4.1: Compare each summand with its value when the partner has weight zero.

19.4.2: As in Problem 19.1.1, the least value is attained by a monomial $X_1^i X_2^j$.

19.4.3: For a common end $\xi^e x = \xi^{e'} x'$ with $e < e'$, consider x', $\xi^{e'-e}x'$, $\xi^{e'}x'$.

References

[GL] L. Sernau, *GRH for Dirichlet L-functions, in Lean 4*, a shorter rewriting of the Lean proof, text by Claude, `https://github.com/lsernau/grh-lean`, commit `72fead1`, readable edition `grh/`.

THE KRONECKER LIMIT FORMULA AND CHOWLA–SELBERG

Prerequisites. Euler's Gamma function: the reflection and duplication formulas, the Beta integral, and $\psi := \Gamma'/\Gamma$ with $\psi(1) = -\gamma$. Poisson summation. Dirichlet L-functions: the functional equation [Dav, Ch. 9], the class number formula and binary quadratic forms [Dav, Ch. 6]. The Hurwitz zeta function [Ap, Ch. 12]. Compact Riemann surfaces and their holomorphic differentials, for Section 20.4 only. From Chapter 11, *Complex tori, theta functions and periods*: Problem 11.1.9 of Section 11.1 and Problem 11.3.4 of Section 11.3.

Chapter 11 took Kronecker's limit formula from the literature and computed $L'(1,\chi)/L(1,\chi)$ for the character χ modulo 4 through the discriminant of the lemniscatic lattice. Here we prove the limit formula and reach the same value through $s = 0$, where no elliptic functions appear. Comparing the two routes is the method of Chowla and Selberg [CS]. It shows that, for the character χ of every imaginary quadratic field, $e^{\gamma - L'(1,\chi)/L(1,\chi)}$ is, up to an algebraic factor, the square of a period of an elliptic curve with complex multiplication divided by π^2.

20.1. Eisenstein series and Kronecker's limit formula

What is the constant term at $s = 1$ of $\sum'_{\mu\in\mathbb{Z}[\mathrm{i}]} |\mu|^{-2s}$? The answer comes from letting the lattice vary. For $\tau = x + \mathrm{i}y$ with $y > 0$ and $\operatorname{Re} s > 1$, let

$$E(\tau, s) := \sum_{(m,n)\neq(0,0)} \frac{y^s}{|m + n\tau|^{2s}}.$$

Let $q := e^{2\pi\mathrm{i}\tau}$, let $\eta(\tau) := e^{\pi\mathrm{i}\tau/12}\prod_{n\geq 1}(1 - q^n)$ be Dedekind's function, and let $\sigma_t(n) := \sum_{e|n} e^t$. For $z > 0$, let $K_\nu(z) := \frac{1}{2}\int_0^\infty t^{\nu-1}e^{-z(t+t^{-1})/2}\,dt$.

Problem 20.1.1. $E(g\tau, s) = E(\tau, s)$ for every $g \in \mathrm{SL}_2(\mathbb{Z})$.

Problem 20.1.2. For real x, $y > 0$ and $\operatorname{Re} s > \frac{1}{2}$,

$$\sum_{m\in\mathbb{Z}} \frac{1}{((m + x)^2 + y^2)^s} = \frac{\sqrt{\pi}\,\Gamma(s - \frac{1}{2})}{\Gamma(s)\,y^{2s-1}} + \frac{4\pi^s}{\Gamma(s)}\sum_{k\geq 1}\Big(\frac{k}{y}\Big)^{s-\frac{1}{2}} K_{s-\frac{1}{2}}(2\pi ky)\cos(2\pi kx).$$

Problem 20.1.3. $E(\tau, s)$ equals

$$2\zeta(2s)y^s + \frac{2\sqrt{\pi}\,\Gamma(s - \frac{1}{2})}{\Gamma(s)}\zeta(2s - 1)y^{1-s} + \frac{8\pi^s\sqrt{y}}{\Gamma(s)}\sum_{n\geq 1} n^{s-\frac{1}{2}}\sigma_{1-2s}(n)K_{s-\frac{1}{2}}(2\pi ny)\cos(2\pi nx).$$

In particular $E(\tau, s)$ continues meromorphically to $\operatorname{Re} s > \frac{1}{2}$, with only a simple pole at $s = 1$.

Problem 20.1.4. $K_{1/2}(z) = \sqrt{\frac{\pi}{2z}}\,e^{-z}$.

Date: November 25, 2026.

Problem 20.1.5. At $s = 1$ the last term in Problem 20.1.3 is $-4\pi \log\bigl|\prod_{n\geq 1}(1-q^n)\bigr|$.

Problem 20.1.6. As $s \to 1$,

$$\frac{2\sqrt{\pi}\,\Gamma(s-\frac{1}{2})}{\Gamma(s)}\zeta(2s-1)y^{1-s} = \frac{\pi}{s-1} + 2\pi\bigl(\gamma - \log 2 - \tfrac{1}{2}\log y\bigr) + O(s-1).$$

Problems 20.1.3–20.1.6 give Kronecker's first limit formula [We], [La, Ch. 20, 21].

Theorem 20.1.1 (Kronecker's first limit formula)**.** $E(\tau, s) = \dfrac{\pi}{s-1} + 2\pi\bigl(\gamma - \log 2 - \log(\sqrt{y}\,|\eta(\tau)|^2)\bigr) + O(s-1)$.

Problem 20.1.7. $|\eta(-1/\tau)| = |\tau|^{1/2}|\eta(\tau)|$.

Problem 20.1.8. Let $Z(s) := \sum'_{\mu\in\mathbb{Z}[\mathrm{i}]}|\mu|^{-2s}$, and let χ be the non-trivial character modulo 4. Then $Z(s) = \pi/(s-1) + 2\pi(\gamma - \log 2 - 2\log\eta(\mathrm{i})) + O(s-1)$, and

$$\frac{L'(1,\chi)}{L(1,\chi)} = \gamma - 2\log 2 - 4\log\eta(\mathrm{i}).$$

The last equality is Problem 11.3.5, now deduced from the limit formula developed here. It expresses $L'/L(1,\chi)$ through a value of a modular form. To see Gamma values instead, we move to $s = 0$, where $L(s,\chi)$ is a finite combination of Hurwitz zeta functions.

20.2. Lerch's formula and the functional equation

For $x > 0$ and $\operatorname{Re} s > 1$, let $\zeta(s,x) := \sum_{n\geq 0}(n+x)^{-s}$. Euler–Maclaurin summation gives

$$\zeta(s,x) = \frac{x^{1-s}}{s-1} + \frac{x^{-s}}{2} - s\int_0^\infty \frac{\{t\}-\frac{1}{2}}{(t+x)^{s+1}}\,dt,$$

which continues $\zeta(s,x)$ to $\operatorname{Re} s > -1$ with a single pole at $s = 1$. Write $\zeta'(s,x)$ for $\partial_s\zeta(s,x)$.

Problem 20.2.1. $\zeta(0,x) = \frac{1}{2} - x$, and $\zeta(s,\frac{1}{2}) = (2^s-1)\zeta(s)$.

Problem 20.2.2. $\partial_x^2\,\zeta'(0,x) = \zeta(2,x) = (\log\Gamma)''(x)$, and $\zeta'(0,x+1) - \zeta'(0,x) = \log x$.

Problems 20.2.1 and 20.2.2 give Lerch's formula.

Theorem 20.2.1 (Lerch)**.** $\zeta'(0,x) = \log\Gamma(x) - \frac{1}{2}\log 2\pi$ *for* $x > 0$.

Problem 20.2.3. Let χ be an odd character modulo N. Then $L(0,\chi) = -\frac{1}{N}\sum_{a=1}^{N} a\,\chi(a)$, and

$$L'(0,\chi) = \sum_{a=1}^{N-1}\chi(a)\log\Gamma(a/N) - L(0,\chi)\log N.$$

Let χ be a primitive odd character modulo N, and let

$$\Lambda(s,\chi) := (N/\pi)^{(s+1)/2}\,\Gamma\bigl(\tfrac{s+1}{2}\bigr)L(s,\chi).$$

Then $\Lambda(s,\chi) = W(\chi)\Lambda(1-s,\bar\chi)$ with $|W(\chi)| = 1$ [Dav, Ch. 9]; moreover $W(\chi) = \tau(\chi)/(\mathrm{i}\sqrt{N})$, which is 1 if χ is real, because then the Gauss sum is $\tau(\chi) = \mathrm{i}\sqrt{N}$ [Dav, Ch. 6].

Problem 20.2.4. $\dfrac{L'(1,\chi)}{L(1,\chi)} + \dfrac{L'(0,\bar\chi)}{L(0,\bar\chi)} = \gamma + \log\dfrac{2\pi}{N}$.

Problem 20.2.5. For the nontrivial character χ modulo 4,

$$\frac{L'(1,\chi)}{L(1,\chi)} = \gamma + 2\log 2 + 3\log\pi - 4\log\Gamma(\tfrac14) = 0.24560\ldots$$

Problem 20.2.6. $\eta(\mathrm{i}) = \Gamma(\frac14)/(2\pi^{3/4})$.

We now pass from $\mathbb{Q}(\mathrm{i})$ to a general imaginary quadratic field.

20.3. The character of an imaginary quadratic field

Let K be an imaginary quadratic field of discriminant $-d$, with class number h and w roots of unity, and let χ be its character, a primitive real odd character modulo d. The class number formula is $L(1,\chi) = 2\pi h/(w\sqrt{d})$. For each $\mathrm{SL}_2(\mathbb{Z})$-equivalence class of positive definite integral binary quadratic forms of discriminant $-d$, choose the reduced representative $Q = [a,b,c]$, so that $Q(m,n) = am^2 + bmn + cn^2$, $b^2 - 4ac = -d$, $|b| \le a \le c$, and $b \ge 0$ if $|b| = a$ or $a = c$. Let $\tau_Q := (-b + \mathrm{i}\sqrt{d})/2a$ and $y_Q := \operatorname{Im}\tau_Q$. The forms Q together represent each $n \ge 1$ exactly $w\sum_{e|n}\chi(e)$ times [Dav, Ch. 6], so

$$\sum_Q \sum_{(m,n)\neq(0,0)} Q(m,n)^{-s} = w\,\zeta(s)L(s,\chi) \qquad (\operatorname{Re} s > 1).$$

The sum over Q has h terms. When $h > 1$, can one class be taken alone?

Problem 20.3.1. For $d = 20$ the reduced forms are $Q_1 = [1,0,5]$ and $Q_2 = [2,2,3]$. The form Q_1 represents 1 twice and 3 not at all, Q_2 represents 1 not at all and 3 four times, and $w\sum_{e|n}\chi(e)$ is 2 for $n = 1$ and 4 for $n = 3$. Prove also that neither $\sum'_{(m,n)} Q_i(m,n)^{-s}$ is a constant multiple of $\zeta(s)L(s,\chi)$.

The sum over classes in the displayed identity leads at $s = 1$ to a formula for $\prod_Q \sqrt{y_Q}\,|\eta(\tau_Q)|^2$.

Problem 20.3.2. $L(0,\chi) = 2h/w$. For $d = 3,4,7,23$ this is $\frac13, \frac12, 1, 3$.

Problem 20.3.3. $\dfrac{L'(1,\chi)}{L(1,\chi)} = \gamma + \log 2\pi - \dfrac{w}{2h}\displaystyle\sum_{a=1}^{d-1}\chi(a)\log\Gamma\Big(\frac{a}{d}\Big)$. For $d = 3,7,23$ it is $0.36828\ldots$, $0.01563\ldots$ and $-0.42212\ldots$.

Problem 20.3.4. $Q(m,n) = \dfrac{\sqrt{d}}{2y_Q}|m - n\tau_Q|^2$. For $\operatorname{Re} s > 1$,

$$\sum_Q E(\tau_Q, s) = w\Big(\frac{\sqrt{d}}{2}\Big)^s \zeta(s)L(s,\chi).$$

Problem 20.3.5. $\dfrac{L'(1,\chi)}{L(1,\chi)} = \gamma - \log 2 - \dfrac12\log d - \dfrac{2}{h}\displaystyle\sum_Q \log\big(\sqrt{y_Q}\,|\eta(\tau_Q)|^2\big)$.

Problems 20.3.3 and 20.3.5 prove the formula of Chowla and Selberg [CS].

Theorem 20.3.1 (Chowla–Selberg)**.**

$$\prod_Q \sqrt{y_Q}\,|\eta(\tau_Q)|^2 = (4\pi\sqrt{d})^{-h/2} \prod_{a=1}^{d-1} \Gamma\Big(\frac{a}{d}\Big)^{w\chi(a)/4}.$$

Problem 20.3.6. For $d = 20$, $y_{Q_1} = \sqrt{5}$ and $y_{Q_2} = \sqrt{5}/2$. The geometric mean of $\sqrt{y_Q}\,|\eta(\tau_Q)|^2$ over the two classes is

$$(8\pi\sqrt{5})^{-1/2}\Big(\frac{\Gamma(\frac{1}{20})\Gamma(\frac{3}{20})\Gamma(\frac{7}{20})\Gamma(\frac{9}{20})}{\Gamma(\frac{11}{20})\Gamma(\frac{13}{20})\Gamma(\frac{17}{20})\Gamma(\frac{19}{20})}\Big)^{1/4} = 0.52301\ldots,$$

while the two values themselves are $0.46373\ldots$ for Q_1 and $0.58987\ldots$ for Q_2.

Problem 20.3.7. Let $\rho := e^{2\pi\mathrm{i}/3}$. Then $|\eta(\rho)|^2 = \dfrac{3^{1/4}\,\Gamma(\frac{1}{3})^3}{4\pi^2}$.

20.4. Periods

How do the Gamma values in Theorem 20.3.1 enter the periods of CM elliptic curves? We first relate Beta values to integrals on Fermat curves.

Let $N \geq 3$ be an integer, and let F_N be the smooth projective curve with affine equation $u^N + v^N = 1$. For integers $a, b \geq 1$, let $\omega_{a,b} := u^{a-1}v^{b-N}\,du$. This algebraic differential is holomorphic on F_N when $a + b \leq N - 1$. Let κ be the path $u \mapsto (u, (1-u^N)^{1/N})$, $0 \leq u \leq 1$, from $(0,1)$ to $(1,0)$. Let $\zeta_N := e^{2\pi\mathrm{i}/N}$, and let $A(u,v) := (\zeta_N u, v)$ and $B(u,v) := (u, \zeta_N v)$.

Problem 20.4.1. For all integers $a, b \geq 1$, the path integral converges and $\int_\kappa \omega_{a,b} = \frac{1}{N}\mathrm{B}(\frac{a}{N}, \frac{b}{N})$.

Problem 20.4.2. Assume $a + b \leq N - 1$. The chain $(1 - A)(1 - B)\kappa$ is a closed cycle on F_N, and the integral of $\omega_{a,b}$ over it is $\frac{1}{N}(1-\zeta_N^a)(1-\zeta_N^b)\,\mathrm{B}(\frac{a}{N}, \frac{b}{N})$.

So each $\mathrm{B}(\frac{a}{N}, \frac{b}{N})$ with $a, b \geq 1$ and $a + b \leq N - 1$ is, up to an algebraic factor, a period of a holomorphic differential on F_N defined over $\mathbb{Q}$.

Problem 20.4.3. For integers $a \geq 1$, $\Gamma(\frac{a}{N})^N = \Gamma(a)\prod_{j=1}^{N-1}\mathrm{B}(\frac{a}{N}, \frac{ja}{N})$.

It follows that for every integer $a \geq 1$, $\Gamma(a/N)^N$ is, up to a rational factor, a product of integrals along κ of the differentials $\omega_{r,s}$ with $1 \leq r, s \leq N$.

Problem 20.4.4. The map $(u, v) \mapsto (t, y) = (u, v^2)$ on affine charts extends to a map from F_4 to the smooth projective model of $y^2 = 1 - t^4$. Its pullback of dt/y is $\omega_{1,2}$, and $\mathrm{B}(\frac{1}{4}, \frac{1}{2}) = 2\varpi$.

For K as in Section 20.3, let

$$\Omega_K := \sqrt{\pi}\prod_{a=1}^{d-1}\Gamma\Big(\frac{a}{d}\Big)^{w\chi(a)/4h}.$$

For $K = \mathbb{Q}(\mathrm{i})$, $\Omega_K = 2\varpi$ is, up to a factor in $\bar{\mathbb{Q}}^\times$, a period of dt/y on the smooth projective model of $y^2 = 1 - t^4$. The quantity computed in Problem 11.3.7 is $\Omega_K^2/(2\pi) = 2\varpi^2/\pi$.

Problem 20.4.5. For $K = \mathbb{Q}(\sqrt{-3})$,

$$\Omega_K = \sqrt{\pi}\,\big(\Gamma(\tfrac{1}{3})/\Gamma(\tfrac{2}{3})\big)^{3/2} = 3^{1/4}2^{-1/2}\,\mathrm{B}(\tfrac{1}{3}, \tfrac{1}{3}).$$

Here F_3 is itself a curve of genus one, $\omega_{1,1}$ is its holomorphic differential, and A multiplies $\omega_{1,1}$ by ζ_3: the curve has complex multiplication by $\mathbb{Z}[\rho]$. This is the general pattern. Chowla and Selberg deduced the following from Theorem 20.3.1 [CS]; we give it in the formulation of Gross [Gr]. Every nonzero period of a nonzero holomorphic differential defined over $\bar{\mathbb{Q}}$ on an elliptic curve over $\bar{\mathbb{Q}}$ with complex multiplication by $\mathcal{O}_K$ lies in $\bar{\mathbb{Q}}^\times\,\Omega_K$. Gross proved this period relation geometrically by comparing periods on a product of CM elliptic curves with periods of special differential forms on a factor of a Fermat Jacobian [Gr, §§ 2–3]. The calculation on Fermat curves uses Beta integrals of the kind in Problem 20.4.2.

Problem 20.4.6. $e^{\gamma - L'(1,\chi)/L(1,\chi)} = \dfrac{\Omega_K^2}{2\pi^2}$. For $K = \mathbb{Q}(\mathrm{i})$ this is $\dfrac{2\varpi^2}{\pi^2} = \dfrac{\Gamma(\frac14)^4}{4\pi^3} = 1.39320\ldots$

Thus $e^{\gamma - L'(1,\chi)/L(1,\chi)} = -2\,(\Omega_K/2\pi\mathrm{i})^2$: up to a factor in $\bar{\mathbb{Q}}^\times$, it is the square of the ratio of a period of an elliptic curve with complex multiplication by $\mathcal{O}_K$ to $2\pi\mathrm{i}$, the period of dz/z on the multiplicative group.

In the proof, with parameters as in Chapter 33 and $K = \mathbb{Q}(\sqrt{-d})$, the constant $e^{\gamma - \mathrm{Re}\,L'(1,\chi)/L(1,\chi)}$ of this chapter appears in the period constant Ω of Section 33.4. Chapter 14, Section 14.6, describes how it cancels against the corresponding term in the main term of the mean prime sum.

In the Lean formalization. The Lean proof [GL] uses the area formula `CMLattice.chowla_selberg`, whose proof uses `kronecker_limit`; one consequence is `Parameters.norm_jetScale_sq`, by which the squared modulus of the scale `P.jetScale` is $1/\Omega$. The cancellation of Chapter 14 occurs in the proof of `Data.jetSize_sub_mainPrimeSum_le`.

Hints

§20.1.

20.1.1: For $g = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$, write $m+n\,g\tau$ as $(m'+n'\tau)/(c\tau+d)$, and use $\mathrm{Im}(g\tau) = y/|c\tau+d|^2$.

20.1.2: Apply Poisson summation in m. To find the Fourier transform of $(t^2+y^2)^{-s}$, write it as an integral of Gaussians in t by means of $\Gamma(s)$.

20.1.3: Separate $n = 0$. For $n \neq 0$ apply Problem 20.1.2 with nx and $|n|y$, pair the two signs of n, and collect the terms with $k|n| = N$. For the continuation, $K_\nu(z)$ decays exponentially as $z \to \infty$, uniformly for ν in a compact set.

20.1.4: Substitute $t = e^{2v}$ and then $w = \sinh v$, and reduce to a Gaussian integral.

20.1.5: $\sum_{n\geq1} \sigma_{-1}(n)\,q^n = -\sum_{m\geq1}\log(1-q^m)$. Compare $2\zeta(2)y$ with $-4\pi\log|e^{\pi\mathrm{i}\tau/12}|$.

20.1.6: $\zeta(2s-1) = \frac{1}{2(s-1)} + \gamma + O(s-1)$, and $\psi(\frac12) = -\gamma - 2\log 2$ by the duplication formula.

20.1.7: Theorem 20.1.1 and Problem 20.1.1.

20.1.8: $Z(s) = E(\mathrm{i}, s)$ and $\eta(\mathrm{i}) > 0$. Then compare with the Laurent expansion of $4\zeta(s)L(s,\chi)$, using $L(1,\chi) = \pi/4$.

§20.2.

20.2.1: Set $s = 0$ in the continuation formula. For the second statement, split $\zeta(s)$ into even and odd n.

20.2.2: $\partial_x \zeta(s,x) = -s\,\zeta(s+1,x)$. Differentiate this identity once more in x, then in s at $s=0$. For the second statement, $\zeta(s,x+1) = \zeta(s,x) - x^{-s}$. To obtain the constant in Lerch's formula, use $x = 1/2$, $\zeta(0) = -1/2$, and $\Gamma(1/2) = \sqrt{\pi}$.

20.2.3: $L(s,\chi) = N^{-s}\sum_{a=1}^{N} \chi(a)\,\zeta(s,a/N)$, and $\sum_a \chi(a) = 0$.

20.2.4: Take the logarithmic derivative of the functional equation at $s=1$, and use $\psi(\frac{1}{2})$ as in Problem 20.1.6. By Dirichlet's nonvanishing theorem, $L(1,\chi) \neq 0$. The functional equation then gives $L(0,\overline{\chi}) \neq 0$.

20.2.5: Use Problems 20.2.3 and 20.2.4 and the identity $\Gamma(\frac{1}{4})\Gamma(\frac{3}{4}) = \pi\sqrt{2}$.

20.2.6: Compare Problems 20.1.8 and 20.2.5. For the derivation from the discriminant of the lemniscatic lattice, see Problem 11.3.6.

§20.3.

20.3.2: Compare $\Lambda(0,\chi)$ with $\Lambda(1,\chi)$, and use the class number formula.

20.3.3: Problems 20.2.3, 20.2.4 and 20.3.2.

20.3.4: Expand $a|m - n\tau_Q|^2$. Then replace n by $-n$.

20.3.5: Expand both sides of Problem 20.3.4 at $s=1$ by Theorem 20.1.1. The residues agree by the class number formula; compare the constant terms.

20.3.1: List the small values of each form. For the right side, $\chi(3) = (\frac{-20}{3})$. Compare the coefficients of the two Dirichlet series at 1 and 3.

20.3.6: Theorem 20.3.1 with $h = w = 2$; list the $a < 20$ with $\chi(a) = 1$. For the numerical values, sum the product for η to a few terms.

20.3.7: Theorem 20.3.1 with $d = 3$, and the reflection formula.

§20.4.

20.4.1: Substitute $t = u^N$ in $\mathrm{B}(\frac{a}{N},\frac{b}{N}) = \int_0^1 t^{a/N-1}(1-t)^{b/N-1}\,dt$.

20.4.2: $A^*\omega_{a,b} = \zeta_N^a\,\omega_{a,b}$ and $B^*\omega_{a,b} = \zeta_N^b\,\omega_{a,b}$. For the boundary, A fixes the points with $u = 0$ and B those with $v = 0$.

20.4.3: $\mathrm{B}(x,y) = \Gamma(x)\Gamma(y)/\Gamma(x+y)$; the product telescopes. To reduce the arguments, use symmetry and $\mathrm{B}(x,y+1) = y\mathrm{B}(x,y)/(x+y)$.

20.4.4: Problem 20.4.1 and the definition of ϖ in Chapter 11.

20.4.5: $h = 1$, $w = 6$, and the reflection formula as in Problem 20.3.7.

20.4.6: Problem 20.3.3.

References

[Ap] T. M. Apostol, *Introduction to Analytic Number Theory*, Undergrad. Texts Math., Springer, 1976.

[CS] A. Selberg and S. Chowla, *On Epstein's zeta-function*, J. reine angew. Math. **227** (1967), 86–110.

[Dav] H. Davenport, *Multiplicative Number Theory*, 3rd ed., Grad. Texts in Math. 74, Springer, 2000.

[GL] L. Sernau, *GRH for Dirichlet L-functions, in Lean 4*, a shorter rewriting of the Lean proof, text by Claude, `https://github.com/lsernau/grh-lean`, commit `72fead1`, readable edition `grh/`.

[Gr] B. H. Gross, *On the periods of abelian integrals and a formula of Chowla and Selberg*, with an appendix by D. E. Rohrlich, Invent. Math. **45** (1978), 193–211.

[La] S. Lang, *Elliptic Functions*, 2nd ed., Grad. Texts in Math. 112, Springer, 1987.

[We] A. Weil, *Elliptic Functions according to Eisenstein and Kronecker*, Ergeb. Math. Grenzgeb. 88, Springer, 1976.

MASSES AND THE COUNT OF FORMS

Prerequisites. Hermitian forms over the Gaussian integers, at the level of definitions. The classification of positive definite unimodular $\mathbb{Z}$-lattices of rank at most 8 [CoS, Ch. 16]. Schur functors and the Weyl dimension formula for $\mathrm{GL}_n(\mathbb{C})$ [FH, Theorem 6.3 and Eq. (15.17)]. The values of Dirichlet L-functions at negative integers [Wa, Theorem 4.2], and the functional equations of $\zeta(s)$ and $L(s,\chi)$ [Dav, Ch. 8, 9]. Stirling's formula. No earlier chapter is used.

Chapter 8 introduces a chain of linear maps. Chapter 23, *Definite theta lifts and their norms*, studies theta lifts between definite unitary groups; the corresponding construction of the proof is the composite lift of Chapter 33. For the definite spaces we take definite unitary groups over $\mathbb{Z}[\mathrm{i}]$ as a model. The genus of the standard lattice has finitely many classes. At the level given by the stabilizer of that lattice, a form of a fixed weight assigns an invariant vector in the weight representation to each class. How many forms are there? For fixed positive rank, when 4 divides the total degree of the weight and its gaps are large, the answer is asymptotically four times the product of a mass and a Weyl dimension, and both factors carry $\prod_{j<n} j!$, which cancels. Chapter 22 evaluates examples of genus averages and relates them to a rank-one lift norm.

21.1. Hermitian lattices over $\mathbb{Z}[\mathrm{i}]$

Let $\mathcal{O} := \mathbb{Z}[\mathrm{i}]$ and $K := \mathbb{Q}(\mathrm{i})$. A *Hermitian lattice* of rank n is a free $\mathcal{O}$-module L of rank n with a positive definite Hermitian form $h\colon L \times L \to \mathcal{O}$, linear in the first variable. Its dual is $L^\sharp := \{y \in L \otimes_{\mathcal{O}} K : h(x,y) \in \mathcal{O} \text{ for all } x \in L\}$, and L is *unimodular* if $L^\sharp = L$. The basic example is $I_n := \mathcal{O}^n$ with $h(x,y) = \sum_k x_k \bar{y}_k$. Let Γ_L be the group of $\mathcal{O}$-linear automorphisms of L preserving h; it is finite, since it permutes the finitely many vectors of bounded length that span L.

Two Hermitian lattices are in the same *genus* if they become isometric over $\mathcal{O} \otimes \mathbb{Z}_p$ for every prime p. Let Cl_n be the set of isometry classes in the genus of I_n. By Problem 21.1.1 below, a class gives a unimodular $\mathbb{Z}$-lattice of rank $2n$ together with an automorphism of it; there are finitely many such lattices up to isometry [Ca, Ch. 9], each with a finite automorphism group, so Cl_n is finite. We call Cl_n the *class set*. For the unitary group of I_n it is the finite adelic double-coset set at the stabilizer of the standard lattice. Its *mass* is

$$M_n := \sum_{L \in \mathrm{Cl}_n} \frac{1}{|\Gamma_L|}, \qquad M_0 := 1.$$

What do the class sets look like in small rank?

Problem 21.1.1. Let L be a Hermitian lattice and $B(x,y) := \operatorname{Re} h(x,y)$. Then B is a positive definite symmetric $\mathbb{Z}$-bilinear form with $B(x,x) = h(x,x)$, multiplication by i preserves B, and $h(x,y) = B(x,y) + \mathrm{i}B(x,\mathrm{i}y)$. The dual of L for B is $L^\sharp$; in particular L is unimodular exactly when (L,B) is.

Date: November 25, 2026.

Problem 21.1.2. Γ_{I_n} is the group of monomial matrices whose nonzero entries lie in $\mu_4 = \{\pm 1, \pm \mathrm{i}\}$. Its order is $4^n n!$.

Problem 21.1.3. For $n \geq 1$, every lattice in the genus of I_n contains a vector x with $h(x,x)$ odd.

Problem 21.1.4. If $n \leq 4$, then $\mathrm{Cl}_n = \{I_n\}$.

Combining Problems 21.1.2 and 21.1.4 gives $M_n = 1/(4^n n!)$ for $n \leq 4$. Let Λ be the Gaussian Hermitian lattice with underlying real lattice E_8. Its norms are even, and $|\Gamma_\Lambda| = 46080$, the order of the reflection group G_{31} of Shephard and Todd [ShT].

21.2. The mass of a genus

How does M_n grow? Let χ be the non-trivial character modulo 4, and let χ^j be χ for odd j and the trivial character for even j, so that $L(s, \chi^j) = \zeta(s)$ for even j. For the genus of I_n, the mass formula reads

$$M_n = \delta_n \prod_{j=1}^{n} \frac{|L(1-j, \chi^j)|}{2}, \tag{1}$$

where δ_n is a positive rational number, a local factor at the prime 2, which is ramified in K. This is the Hermitian analogue of Siegel's mass formula for quadratic forms [Si], with the local factors computed by Gan and Yu [GY] and, at the ramified prime 2, by Cho [Cho]. We set $\delta_0 := 1$, so that (1) also holds for $n = 0$, where $M_0 = 1$.

Problem 21.2.1. For $j = 1, 2, 3, 4, 5$, the numbers $|L(1-j, \chi^j)|/2$ are 1/4, 1/24, 1/4, 1/240, 5/4.

Problem 21.2.2. Determine the local factors from the class masses, taking the local factors as unknowns. Prove that $\delta_1 = \delta_3 = 1$, $\delta_2 = 3$ and $\delta_4 = 15$.

For all positive ranks, [JZ, Corollary 4.3] gives $\delta_n = 1$ for odd n and $\delta_n = 2^n - 1$ for even n.

In rank 5, with $\delta_5 = 1$, the formula gives $M_5 = 1/73728$. Two unimodular lattices of the same rank over $\mathcal{O}$, each containing a vector x with $h(x,x)$ odd, lie in the same genus [JZ, Corollary 2.2]; thus $\Lambda \perp I_1 \in \mathrm{Cl}_5$.

Problem 21.2.3. The only vectors $x \in \Lambda \perp I_1$ with $h(x,x) = 1$ are the four multiples ue, $u \in \mu_4$, of a generator e of I_1; hence $\Gamma_{\Lambda \perp I_1} = \Gamma_\Lambda \times \mu_4$. Moreover $\mathrm{Cl}_5 = \{I_5, \Lambda \perp I_1\}$.

What is the factorial contribution of the jth mass factor?

Problem 21.2.4. For $j \geq 1$,

$$\frac{|L(1-j, \chi^j)|}{2} = (j-1)!\, \pi^{-j} \beta_j, \qquad \beta_j := \begin{cases} 2^{j-1} L(j, \chi) & j \text{ odd}, \\ 2^{-j} \zeta(j) & j \text{ even}. \end{cases}$$

For $r \geq 1$ define $\kappa_r > 0$ by

$$\frac{M_r}{M_{r-1}} = (r-1)!\, \pi^{-r} \kappa_r. \tag{2}$$

By (1) and Problem 21.2.4, $\kappa_r = (\delta_r/\delta_{r-1})\beta_r$. Multiplying (2) over $r \le n$,

$$M_n = \pi^{-n(n+1)/2} \prod_{j=0}^{n-1} j! \prod_{j=1}^{n} \kappa_j. \tag{3}$$

After removing $(r-1)!$ from the mass ratio, the logarithm of the remaining factor is $-r\log\pi + \log\kappa_r$.

Problem 21.2.5. For $r \le 4$, $\kappa_r = \pi^r/(4\cdot r!)$; thus $\kappa_1, \dots, \kappa_4$ are $\pi/4$, $\pi^2/8$, $\pi^3/24$, $\pi^4/96$. With $\delta_5 = 1$, $\kappa_5 = \pi^5/288$.

Problem 21.2.6. For every $r \ge 1$, $3/4 \le \kappa_r \le 2$; in particular $\log\kappa_r = O(1)$.

By (3), $\log M_n$ grows like $\frac{1}{2}n^2\log n$; for $n \ge 1$ every Γ_L contains μ_4, so the class set has at least $4M_n$ elements, more than $8\cdot 10^5$ for $n = 15$.

21.3. Forms and the Weyl dimension formula

On a definite group a form is a function on the class set, with values in a representation. How many are there?

For $L \in \mathrm{Cl}_n$ let $L_{\mathbb{C}} := L \otimes_{\mathcal{O}} \mathbb{C}$, using the inclusion $\mathcal{O} \subset \mathbb{C}$. The form h extends to a Hermitian inner product on $L_{\mathbb{C}}$, and Γ_L is a finite subgroup of its unitary group. A *weight* is a sequence of integers $\lambda = (\lambda_1 \ge \cdots \ge \lambda_n \ge 0)$; write $|\lambda| := \sum_k \lambda_k$. For a finite-dimensional Hermitian space A, let $\mathbb{S}_\lambda(A) \subset A^{\otimes|\lambda|}$ be the image of the Young symmetrizer [FH, §6.1], with the inner product induced from $A^{\otimes|\lambda|}$. A linear map $x\colon A \to B$ induces $\mathbb{S}_\lambda(x)\colon \mathbb{S}_\lambda(A) \to \mathbb{S}_\lambda(B)$, the restriction of $x^{\otimes|\lambda|}$. Then $\mathbb{S}_\lambda(xy) = \mathbb{S}_\lambda(x)\mathbb{S}_\lambda(y)$ and $\mathbb{S}_\lambda(x)^* = \mathbb{S}_\lambda(x^*)$, the latter because $(x^*)^{\otimes|\lambda|}$ intertwines the permutation actions on the two tensor powers. If λ has at most $\dim A$ nonzero entries, $\mathbb{S}_\lambda(A)$ is the irreducible representation of $\mathrm{GL}(A)$ of highest weight λ; otherwise it is zero [FH, Theorem 6.3]. For $\lambda = (a)$ it is $\mathrm{Sym}^a(A)$. There, for $u \in A$ we write $u^a := u \otimes \cdots \otimes u$; for a basis $e_1, \dots, e_n$ of A and $|\nu| = a$, the vectors e^ν are defined by $(\sum_k t_k e_k)^a = \sum_\nu (a!/\nu!)\, t^\nu e^\nu$, and $e^\nu e^\mu := e^{\nu+\mu}$ is the product of the symmetric algebra.

Let $V_\lambda(L) := \mathbb{S}_\lambda(L_{\mathbb{C}})$. Weyl's dimension formula reads, with $z_k := \lambda_k + n - k$,

$$\dim V_\lambda(L) = D_n(z) := \frac{V_n(z)}{\prod_{j=0}^{n-1} j!}, \qquad V_n(z) := \prod_{1\le k<l\le n} (z_k - z_l) \tag{4}$$

[FH, Eq. (15.17)]. Fix one lattice in each class of Cl_n. A *form of weight* λ assigns to each $L \in \mathrm{Cl}_n$ a vector $\varphi(L) \in V_\lambda(L)$ fixed by Γ_L. The forms make up a space $\mathcal{A}_\lambda(n)$, with the squared norm

$$\|\varphi\|^2 := \sum_{L\in\mathrm{Cl}_n} \frac{1}{|\Gamma_L|}\, \|\varphi(L)\|^2.$$

These are the algebraic modular forms of Gross [Gr] on the unitary group of I_n, of level one.

Problem 21.3.1. For $n \ge 1$ and $a \ge 0$, $\dim \mathrm{Sym}^a(\mathbb{C}^n) = \binom{a+n-1}{n-1}$, and $\dim \mathbb{S}_{(3,2,0)}(\mathbb{C}^3) = 15$. The denominator in (4) is $\prod_{j=0}^{n-1} j! = V_n(n-1, \dots, 1, 0)$.

Problem 21.3.2. In $\mathrm{Sym}^a(A)$, $\langle u^a, v^a\rangle = \langle u, v\rangle^a$. If $e_1, \dots, e_n$ is orthonormal, the e^ν are orthogonal and $\|e^\nu\|^2 = \nu!/a!$.

Problem 21.3.3. $\mathcal{A}_\lambda(n) = 0$ unless $4 \mid |\lambda|$. The space $\mathcal{A}_{(a)}(1)$ is one-dimensional when $4 \mid a$.

Problem 21.3.4. $\dim \mathcal{A}_\lambda(n) = \sum_L |\Gamma_L|^{-1} \sum_{\gamma \in \Gamma_L} \operatorname{tr}(\gamma \mid V_\lambda(L))$. For $n \geq 1$ and $4 \mid |\lambda|$, the scalars $\gamma \in \mu_4$ contribute $4M_n \dim V_\lambda$ to this sum.

Problem 21.3.5. The Γ_{I_2}-invariants in the symmetric algebra of $\mathbb{C}^2$ form the polynomial algebra on $e_1^4 + e_2^4$ and $e_1^4 e_2^4$. Hence, for $4 \mid a$, $\dim \mathcal{A}_{(a)}(2) = \lfloor a/8 \rfloor + 1$, which is $(1 + o(1)) \cdot 4M_2 \dim V_{(a)}$ as $a \to \infty$.

Does $|\lambda| \to \infty$ suffice? Compare two weights of the same size.

Problem 21.3.6. Let $j \geq 1$, $\lambda := (8j, 0)$ and $\lambda' := (4j, 4j)$. Then $\dim \mathcal{A}_\lambda(2) = j+1$ and $\dim \mathcal{A}_{\lambda'}(2) = 1$, while the scalar contributions $4M_2 \dim V$ of Problem 21.3.4 are $j + \frac{1}{8}$ and $\frac{1}{8}$. In both cases the non-scalar elements of Γ_{I_2} contribute exactly $\frac{7}{8}$.

These weights have the same total degree and different gaps.

Fix a positive rank n. When $4 \mid |\lambda|$ and all the gaps $\lambda_k - \lambda_{k+1}$ tend to infinity, the Weyl character formula shows that each non-scalar γ contributes $o(\dim V_\lambda)$, so $\dim \mathcal{A}_\lambda(n) \sim 4M_n \dim V_\lambda$. The count of forms is thus asymptotically four times the product of the mass and the Weyl dimension. By (3) and (4) each factor contains $\prod_{j<n} j!$, once in the numerator and once in the denominator; §21.4 returns to this.

21.4. The count of forms

When $4 \mid |\lambda|$ and the gaps of λ are large, the space of forms of weight λ has dimension about $4M_n \dim V_\lambda$ (§21.3). The mass contains the product $\prod_{j<n} j!$, whose logarithm is about $\frac{1}{2}n^2 \log n$, and the Weyl dimension contains its inverse. How does $M_r D_r$ change when the rank increases?

Problem 21.4.1. $\sum_{j=0}^{n-1} \log j! = \frac{1}{2}n^2 \log n - \frac{3}{4}n^2 + O(n \log n)$.

Problem 21.4.2. Let $r_0 < r_1$, and let $u \in \mathbb{Z}^{r_0}$ and $w \in \mathbb{Z}^{r_1}$ be strictly decreasing. Then

$$\frac{M_{r_1} D_{r_1}(w)}{M_{r_0} D_{r_0}(u)} = \frac{V_{r_1}(w)}{V_{r_0}(u)} \, \pi^{-\sum_{r=r_0+1}^{r_1} r} \prod_{r=r_0+1}^{r_1} \kappa_r.$$

With $r_0 = 0$, where $M_0 = D_0 = V_0 = 1$ (empty products), Problem 21.4.2 reads as follows.

Theorem 21.4.1 (The count identity)**.** *For every $r \geq 1$ and every strictly decreasing $z \in \mathbb{Z}^r$,*

$$M_r D_r(z) = V_r(z) \, \pi^{-r(r+1)/2} \prod_{j=1}^{r} \kappa_j.$$

No factorial survives: what remains is a product of differences of weights, a power of π and the factors κ_j.

The simplest instance adds one rank, with one large new weight.

Problem 21.4.3. Fix $r_0 \geq 1$ and a strictly decreasing $u \in \mathbb{Z}^{r_0}$. For an integer $w_1 > u_1$, let $w = (w_1, u_1, \ldots, u_{r_0})$. Then

$$\log \frac{M_{r_0+1} D_{r_0+1}(w)}{M_{r_0} D_{r_0}(u)} = \sum_{i=1}^{r_0} \big(\log(w_1 - u_i) - \log \pi \big) - \log \pi + \log \kappa_{r_0+1}.$$

For fixed r_0 and u, the sum in this formula grows like $r_0 \log w_1$ as $w_1 \to \infty$, and the remaining term $\log \kappa_{r_0+1} - \log \pi$ is constant.

In the Lean formalization. This chapter serves the bound for the dimension d_T of the target forms T of Chapter 33, which the Lean proof [GL] combines with a second-moment estimate in `targetDim_mul_sum_hilbertSchmidtNorm_sq_le`. For parameters and data as in Chapter 33, with $\bar{G}$ and the definite space W_m as there, `finrank_principalForms_spaceW` states that the complex dimension of the principal forms $H(W_m)$ equals $\#\bar{G}\cdot$`mass D.E D.r`$\cdot\prod_v$ `(toHCParam 1 (D.paramW v)).formalDegree`, the product over the infinite places v; and `targetDim_le_card_mul_besselDegree_mul_mass` states $d_T \le \#\bar{G} \cdot$ `D.filling.besselDegree` $\cdot$ `mass D.E D.r`. Both are in `New/Spanning/SecondMoment/SpanningTheorem.lean` of the readable edition.

Hints

§21.1.

21.1.1: Compute $B(\mathrm{i}x, \mathrm{i}y)$ and $B(x, \mathrm{i}y)$. For the dual, replace x by $\mathrm{i}x$ in the condition $B(x, y) \in \mathbb{Z}$.

21.1.2: An automorphism permutes the vectors with $h(x, x) = 1$. Which vectors of I_n are these?

21.1.3: Over $\mathbb{Z}_2$ the lattice is isometric to $I_n \otimes \mathbb{Z}_2$. Approximate a vector of odd length 2-adically by a vector of L.

21.1.4: Use Problems 21.1.1 and 21.1.3 and the classification of odd unimodular lattices of rank at most 8; then look at the vectors of length one.

§21.2.

21.2.1: For odd j use $B_{j,\chi} = 4^{j-1}\sum_{a=1}^{4}\chi(a)B_j(a/4)$. For even j use $\zeta(1-j) = -B_j/j$.

21.2.2: Compare (1) with $M_n = 1/(4^n n!)$.

21.2.4: For ζ use $\zeta(1-s) = 2(2\pi)^{-s}\cos(\pi s/2)\Gamma(s)\zeta(s)$. For the odd character χ of conductor 4, whose Gauss sum is 2i, complete $L(s,\chi)$ by $(4/\pi)^{(s+1)/2}\Gamma(\frac{s+1}{2})$, and use the reflection and duplication formulas for Γ. Check the case $j = 1$: $L(1,\chi) = \pi/4$.

21.2.3: Λ is even. For the second part, compare with the mass M_5.

21.2.5: Use $M_r/M_{r-1} = 1/(4r)$ for $r \le 4$, and $M_5 = 1/73728$.

21.2.6: Use $\kappa_r = (\delta_r/\delta_{r-1})\beta_r$ and the values of δ_n, treating odd and even r separately; $1 - 3^{-r} \le L(r,\chi) \le 1$. For $r = 1$ use Problem 21.2.5.

§21.3.

21.3.1: For $\lambda = (a)$, $z = (a+n-1, n-2, \dots, 0)$.

21.3.2: Expand $\langle(\sum t_k e_k)^a, (\sum s_k e_k)^a\rangle$ in two ways.

21.3.3: The scalar $\mathrm{i} \in \Gamma_L$ acts on $V_\lambda(L)$ by $\mathrm{i}^{|\lambda|}$.

21.3.4: The dimension of the invariants of a finite group is the average of the trace.

21.3.5: An invariant must be invariant under $e_k \mapsto \mathrm{i}e_k$ and under the swap. Count the pairs (i,j) with $4i + 8j = a$.

21.3.6: For λ use Problem 21.3.5. For λ', $\mathbb{S}_{(k,k)}(\mathbb{C}^2)$ is the k-th power of the determinant, and every element of Γ_{I_2} has determinant in μ_4. Use $M_2 = 1/32$; the non-scalar part is the dimension less the scalar contribution.

§21.4.

21.4.1: For $j \ge 1$, $\log j! = j\log j - j + O(\log(j+1))$; compare the sum with an integral. The $j = 0$ term vanishes.

21.4.2: Write the left side as a telescoping product, and use (2) and (4).
21.4.3: $V_{r_0+1}(w) = V_{r_0}(u)\prod_i(w_1 - u_i)$.

References

[Ca] J. W. S. Cassels, *Rational Quadratic Forms*, Academic Press, 1978.

[Cho] S. Cho, *Group schemes and local densities of ramified hermitian lattices in residue characteristic 2*, arXiv:1210.7894v1, 2012.

[CoS] J. H. Conway and N. J. A. Sloane, *Sphere Packings, Lattices and Groups*, 3rd ed., Grundlehren Math. Wiss. 290, Springer, 1999.

[Dav] H. Davenport, *Multiplicative Number Theory*, 3rd ed., Grad. Texts in Math. 74, Springer, 2000.

[FH] W. Fulton and J. Harris, *Representation Theory: A First Course*, Grad. Texts in Math. 129, Springer, 1991.

[GY] W. T. Gan and J.-K. Yu, *Group schemes and local densities*, Duke Math. J. **105** (2000), 497–524.

[GL] L. Sernau, *GRH for Dirichlet L-functions, in Lean 4*, a shorter rewriting of the Lean proof, text by Claude, `https://github.com/lsernau/grh-lean`, commit `72fead1`, readable edition `grh/`.

[Gr] B. H. Gross, *Algebraic modular forms*, Israel J. Math. **113** (1999), 61–93.

[ShT] G. C. Shephard and J. A. Todd, *Finite unitary reflection groups*, Canad. J. Math. **6** (1954), 274–304.

[JZ] M. Jürgens and M. C. Zimmermann, *Steinitz classes and partial genera of unimodular lattices over imaginary-quadratic fields*, arXiv:1512.03297, 2015.

[Si] C. L. Siegel, *Über die analytische Theorie der quadratischen Formen*, Ann. of Math. **36** (1935), 527–606.

[Wa] L. C. Washington, *Introduction to Cyclotomic Fields*, 2nd ed., Grad. Texts in Math. 83, Springer, 1997.

THE SIEGEL–WEIL FORMULA IN THE SMALLEST CASE

Prerequisites. Modular forms for $\mathrm{SL}_2(\mathbb{Z})$, theta series of even unimodular lattices, and the mass formula, as in [SeA, Ch. V, §2.3 and Ch. VII, §§2–6]. Quadratic forms over finite fields [SeA, Ch. IV, §1.7] and Hensel's lemma [SeA, Ch. II, §2.2]. For §22.3: the space of modular forms of weight n on $\Gamma_0(4)$ with character χ^n, its dimension and its basis in terms of θ [Ko, Ch. IV, §1], and its Eisenstein series [DS, §4.5]. From Chapter 21, *Masses and the count of forms*: the class sets Cl_n, the groups Γ_L, the masses M_n, Problems 21.1.2, 21.1.4 and 21.2.3, and the forms of §21.3 with Problem 21.3.2.

For a positive definite lattice, the isometry classes in its genus form a finite set. In the convergent range, Siegel's theorem identifies the average of their theta series, with weights proportional to the reciprocals of the automorphism orders, as an Eisenstein series. We check this average for even unimodular lattices and for the rank-five Hermitian class set of Chapter 21. We then express a rank-one lift norm in terms of averaged representation numbers.

22.1. Even unimodular lattices

Let L be an even unimodular positive definite lattice of rank $m > 0$, with inner product $x \cdot y$, and let $r_L(j)$ be the number of $x \in L$ with $x \cdot x = 2j$. Then $8 \mid m$, and $\theta_L(\tau) := \sum_{j \geq 0} r_L(j) q^j$, $q = e^{2\pi i \tau}$, is a modular form of weight $k := m/2$ for $\mathrm{SL}_2(\mathbb{Z})$ [SeA, Ch. VII, Theorem 8]. Let $\mathcal{M}_k$ be the space of such forms and

$$E_k := 1 - \frac{2k}{B_k} \sum_{j \geq 1} \sigma_{k-1}(j) q^j, \qquad \Delta := q \prod_{j \geq 1} (1 - q^j)^{24} = \sum_{j \geq 1} \tau(j) q^j,$$

so that $E_4 = 1 + 240 \sum \sigma_3(j) q^j$, $E_8 = 1 + 480 \sum \sigma_7(j) q^j$, $E_{12} = 1 + \frac{65520}{691} \sum \sigma_{11}(j) q^j$. (Serre writes E_2, E_4, E_6 for these, indexing by half the weight.) The spaces $\mathcal{M}_4$ and $\mathcal{M}_8$ are spanned by E_4 and E_8, and $\mathcal{M}_{12}$ by E_{12} and Δ [SeA, Ch. VII, §3.2]. We write E_8 also for the root lattice; the context decides. Let $D_{16}^+ := D_{16} \cup (D_{16} + (\frac{1}{2}, \ldots, \frac{1}{2}))$, where $D_{16} = \{x \in \mathbb{Z}^{16} : \sum x_i \text{ even}\}$ [CoS, Ch. 4, §7].

Problem 22.1.1. $r_{E_8}(j) = 240\, \sigma_3(j)$ for $j \geq 1$. In particular E_8 has 240 roots and 2160 vectors with $x \cdot x = 4$.

Problem 22.1.2. $\theta_{E_8 \oplus E_8} = \theta_{D_{16}^+} = E_8$. Both lattices have 480 roots and 61920 vectors with $x \cdot x = 4$, and $\sigma_7(j) = \sigma_3(j) + 120 \sum_{i=1}^{j-1} \sigma_3(i) \sigma_3(j-i)$ for $j \geq 1$.

Problem 22.1.3. $E_8 \oplus E_8$ and D_{16}^+ are not isometric.

So the theta series does not determine the lattice. Milnor observed that the tori $\mathbb{R}^{16}/(E_8 \oplus E_8)$ and $\mathbb{R}^{16}/D_{16}^+$ therefore have the same Laplace spectrum without being isometric [Mi].

Problem 22.1.4. If Λ_{24} is an even unimodular lattice of rank 24 without roots (the Leech lattice [CoS, Ch. 4, §11]), then $\theta_{\Lambda_{24}} = E_{12} - \frac{65520}{691} \Delta$, and Λ_{24} has 196560 vectors with $x \cdot x = 4$.

Date: November 25, 2026.

In rank 24 write $\theta_L = E_{12} + c_L\Delta$ [SeA, Ch. VII, §6.6]. Let C_m be the set of isometry classes of positive definite even unimodular lattices of rank m, let $g_L := |O(L)|$, and let $\mu_m := \sum_{L\in C_m} g_L^{-1}$ be the mass. Siegel proved [Si] that

$$\sum_{L\in C_m} \frac{\theta_L}{g_L} = \mu_m\, E_{m/2}, \tag{1}$$

see [SeA, Ch. VII, §6.5, Remark], and the Minkowski–Siegel mass formula [SeA, Ch. V, §2.3]

$$\mu_m = \frac{|B_k|}{2k} \prod_{j=1}^{k-1} \frac{|B_{2j}|}{4j}, \qquad m = 2k.$$

One has $C_8 = \{E_8\}$ with $g_{E_8} = |W(E_8)| = 696729600$, and $C_{16} = \{E_8 \oplus E_8, D_{16}^+\}$ with $g = 2\,|W(E_8)|^2$ and $g = 2^{15}\,16!$ respectively [SeA, Ch. V, §2.3].

Problem 22.1.5. The mass formula holds for $m = 8$ and $m = 16$. In the average obtained by dividing (1) by μ_{16} for $m = 16$, $E_8 \oplus E_8$ has weight 286/691 and D_{16}^+ has weight 405/691.

Problems 22.1.1 and 22.1.2 give (1) for ranks 8 and 16. In rank 24 the individual theta series can differ.

Problem 22.1.6. For $m = 24$, (1) is equivalent to $\sum_{L\in C_{24}} c_L/g_L = 0$. Hence the mass-weighted mean number of roots of an even unimodular lattice of rank 24 is 65520/691; in particular $\mu_{24}^{-1}\sum_L \theta_L/g_L$ is not the theta series of a lattice.

22.2. Local densities

Why should an average of theta series be an Eisenstein series? Its coefficients are averages of representation numbers, and Siegel's theorem says that these are products of local quantities. Let $Q(x) := x\cdot x/2$ on L. For a prime p and $j \geq 1$ the *local density* is

$$\alpha_p(j) := \lim_{r\to\infty} p^{r(1-m)}\, \#\{x \in L/p^rL : Q(x) \equiv j \pmod{p^r}\},$$

and the *archimedean density* is $\alpha_\infty(j) := \frac{d}{dt}\,\mathrm{vol}\{x \in L\otimes\mathbb{R} : Q(x) \leq t\}\big|_{t=j}$, the volume being normalized so that L has covolume 1. In this language Siegel's theorem reads

$$\frac{1}{\mu_m} \sum_{L\in C_m} \frac{r_L(j)}{g_L} = \alpha_\infty(j) \prod_p \alpha_p(j) \qquad (j \geq 1), \tag{2}$$

and the densities depend only on $L\otimes\mathbb{Z}_p$ and $L\otimes\mathbb{R}$, which are the same for every $L \in C_m$. For every prime p, the reduction L/pL with the form Q mod p is isometric to the orthogonal sum H^k of $k = m/2$ hyperbolic planes, $Q = x_1y_1 + \cdots + x_ky_k$ [Ca, Ch. 8].

Problem 22.2.1. $\alpha_\infty(j) = (2\pi)^k j^{k-1}/\Gamma(k)$.

Problem 22.2.2. For $j \in \mathbb{F}_p$, the number of $(x,y) \in \mathbb{F}_p^k \times \mathbb{F}_p^k$ with $x_1y_1 + \cdots + x_ky_k = j$ is $p^{2k-1} - p^{k-1}$ for $j \neq 0$, and $p^{2k-1} + p^k - p^{k-1}$ for $j = 0$.

Problem 22.2.3. If $p \nmid j$, then $\alpha_p(j) = 1 - p^{-k}$.

Problem 22.2.4. If $p\|j$, then $\alpha_p(j) = (1-p^{-k})(1+p^{1-k})$. More generally, for $v = v_p(j)$, one has $\alpha_p(j) = (1-p^{-k})\sum_{i=0}^{v} p^{i(1-k)}$.

Problem 22.2.5. $\alpha_\infty(j)\prod_p \alpha_p(j) = -\frac{2k}{B_k}\,\sigma_{k-1}(j)$.

Thus the right side of (2) is the jth coefficient of E_k, and (2) is (1) coefficient by coefficient. With Problems 22.1.1 and 22.1.2 this proves the following.

Theorem 22.2.1. *For $m = 8$ and $m = 16$, and every $j \geq 1$, the mass-weighted mean of $r_L(j)$ over C_m is $\alpha_\infty(j)\prod_p \alpha_p(j)$.*

Weil reformulated (1) as an identity on adelic groups: the integral of the theta function over $O(V)(\mathbb{Q})\backslash O(V)(\mathbb{A})$ taken with the invariant measure of total mass one, is an Eisenstein series, under hypotheses that include the absolute convergence of the Eisenstein series [We65, Theorem 5]. For a positive definite space the quotient is compact. With the theta kernel attached to a lattice, the integral with measure of total mass one is the normalized genus average. This is the *Siegel–Weil formula in the convergent range*.

22.3. The Hermitian class set over $\mathbb{Z}[\mathrm{i}]$

Return to the class sets Cl_n of Hermitian lattices over $\mathcal{O} = \mathbb{Z}[\mathrm{i}]$ from Chapter 21. For $L \in \mathrm{Cl}_n$ let $\theta_L(\tau) := \sum_{x\in L} q^{h(x,x)}$, and let $\theta := \sum_{j\in\mathbb{Z}} q^{j^2}$. Let χ be the nontrivial character modulo 4, and $\mathcal{M}_n(4,\chi^n)$ the space of modular forms of weight n on $\Gamma_0(4)$ with character χ^n. It has dimension $1 + \lfloor n/2\rfloor$ and basis $\theta^{2n-4i}F^i$, $0 \leq i \leq n/2$, where $F := \sum_{\substack{j\geq 1\\ j \text{ odd}}} \sigma_1(j)q^j$ [Ko, Ch. IV, §1]; so an element is determined by its coefficients of $q^0, \ldots, q^{\lfloor n/2\rfloor}$. Each θ_L lies in $\mathcal{M}_n(4,\chi^n)$.

For Hermitian lattices Siegel's theorem is due to Braun [Br], and it is a case of Weil's theorem [We65, Theorem 5]; for the unitary formulation see [Li, Theorem 2.3.1]. It reads, for $n \geq 3$,

$$\sum_{L\in\mathrm{Cl}_n} \frac{\theta_L}{|\Gamma_L|} = M_n\, E^{(n)}, \qquad E^{(n)} = 1 + \sum_{j\geq 1} \alpha_\infty(j)\prod_p \alpha_p(j)\, q^j, \tag{3}$$

with the densities of I_n defined as in §22.2 on the underlying $\mathbb{Z}$-lattice of rank $2n$, with $Q(x) := h(x,x)$, and $E^{(n)}$ an Eisenstein series in $\mathcal{M}_n(4,\chi^n)$. The condition $n \geq 3$ is where Eisenstein series of weight n converge absolutely.

Problem 22.3.1. For τ in the upper half-plane and $s \in \mathbb{R}$, the sum $\sum_{(c,d)\in\mathbb{Z}^2\setminus\{(0,0)\}} |c\tau + d|^{-s}$ converges if and only if $s > 2$.

Problem 22.3.2. $\theta_{I_n} = \theta^{2n}$, and $\theta_{\Lambda\perp I_1}(\tau) = E_4(2\tau)\,\theta(\tau)^2$, with Λ as in Problem 21.2.3.

For $n = 3$ and 4, $\mathrm{Cl}_n = \{I_n\}$ (Problem 21.1.4), so (3) says that θ^{2n} is itself an Eisenstein series. This is Jacobi's formula for sums of $2n$ squares; for $n = 4$ and positive odd j it reads $r_8(j) = 16\,\sigma_3(j)$. Here are its local factors.

Problem 22.3.3. For I_4 and positive odd j, $\alpha_\infty(j) = \pi^4 j^3/6$ and $\alpha_\infty(j)\prod_{p \text{ odd}} \alpha_p(j) = 16\,\sigma_3(j)$.

Problem 22.3.4. For positive odd j, the number of $x \in (\mathbb{Z}/8\mathbb{Z})^8$ with $x_1^2 + \cdots + x_8^2 \equiv j \pmod 8$ is 8^7. For every $r \geq 3$ the number of solutions modulo 2^r is 2^{7r}. Deduce that $\alpha_2(j) = 1$ and that the full density product is $16\,\sigma_3(j)$.

In rank 5 the class set has two elements, I_5 and $\Lambda \perp I_1$ (Problem 21.2.3), and $\dim \mathcal{M}_5(4,\chi) = 3$, and its Eisenstein subspace has dimension 2. Let $e_4(j) := \sum_{d\mid j,\, d \text{ odd}} \chi(d)\, d^4$ and $e_4'(j) := \sum_{d\mid j,\, j/d \text{ odd}} \chi(j/d)\, d^4$. The series $G_5 := 1 + \frac{4}{5}\sum_{j\ge 1}(e_4(j) + 16e_4'(j))q^j$ is a combination of the two Eisenstein series of $\mathcal{M}_5(4,\chi)$ [DS, §4.5].

Problem 22.3.5. In Cl_5, the weights $|\Gamma_L|^{-1}/M_5$ are $3/5$ for I_5 and $2/5$ for $\Lambda \perp I_1$.

Problem 22.3.6. $\frac{3}{5}\,\theta^{10} + \frac{2}{5}\,E_4(2\tau)\theta^2 = G_5$. The coefficients of q in θ^{10}, $E_4(2\tau)\theta^2$ and G_5 are 20, 4 and 68/5.

In rank 5 the mass-weighted average is therefore Eisenstein. To identify the cusp parts of the individual theta series, consider the following form. Let $f := \frac{1}{4}\sum_{\alpha\in\mathcal{O}} \alpha^4 q^{|\alpha|^2} = q - 4q^2 + 16q^4 - 14q^5 + \cdots$, the theta series of $\mathcal{O}$ with the harmonic polynomial α^4; it is a cusp form in $\mathcal{M}_5(4,\chi)$ [Iw, Ch. 10].

Problem 22.3.7. $\theta^{10} - E_4(2\tau)\theta^2 = 16f$. Hence $\theta^{10} = G_5 + \frac{32}{5}f$ and $E_4(2\tau)\theta^2 = G_5 - \frac{48}{5}f$.

The identity for θ^{10} in Problem 22.3.7 is the theta-series form of Liouville's ten-square formula [Liouville], $r_{10}(j) = \frac{4}{5}(e_4(j) + 16e_4'(j)) + \frac{8}{5}\sum_{|\alpha|^2=j}\alpha^4$. The cusp parts $\frac{32}{5}f$ and $-\frac{48}{5}f$ cancel in the average with weights $3/5$ and $2/5$, and only there. Since $f \neq 0$, neither individual theta series is Eisenstein.

22.4. Gram rows and nonvanishing

In the definite model of Chapter 21 the theta lifts go from forms on Cl_n to forms on $\mathrm{Cl}_{n'}$. Their Gram matrices are sums over the target class set, which can be large even when its mass is explicit (Chapter 21, §21.2). We take $n = 1$.

Let $n' \ge 1$. For an integer $a \ge 0$ and $L' \in \mathrm{Cl}_{n'}$ let

$$v_a(L') := \sum_{x\in L'} x^a\, e^{-\pi h(x,x)} \in \mathrm{Sym}^a(L'_{\mathbb{C}}),$$

with x^a as in §21.3. For $4 \mid a$, let $\varphi(I_1)$ be the standard basis vector of $\mathrm{Sym}^a(\mathbb{C})$. The lift of the next chapter, *Definite theta lifts and their norms*, satisfies $v_a = 4\Theta_{(a)}\varphi$, since $|\Gamma_{I_1}| = 4$ (Problem 21.3.3). For $x, y \in L'$ let $\mathrm{Gram}(x,y)$ be the matrix with entries $h(x,x)$, $h(x,y)$, $h(y,x)$, $h(y,y)$, and for a 2×2 Hermitian matrix T over $\mathcal{O}$ put

$$R_{n'}(T) := \sum_{L'\in \mathrm{Cl}_{n'}} \frac{1}{|\Gamma_{L'}|}\, \#\{(x,y) \in L'^2 : \mathrm{Gram}(x,y) = T\}.$$

Problem 22.4.1. v_a is a form of weight (a) on $\mathrm{Cl}_{n'}$, and $v_a = 0$ unless $4 \mid a$.

Problem 22.4.2. $\|v_a\|^2 = \sum_T R_{n'}(T)\, T_{12}^a\, e^{-\pi\,\mathrm{tr}\,T}$, the sum running over positive semi-definite T.

For this rank-one source the norm depends on the target genus through the averaged counts $R_{n'}(T)$. For $n' > 4$ the degree-two Siegel–Weil formula gives, for each positive definite integral Hermitian T,

$$R_{n'}(T) = M_{n'}\, \alpha_\infty(T) \prod_p \alpha_p(T).$$

Here $\alpha_p(T)$ is the limit, as $r \to \infty$, of $p^{r(4-4n')}$ times the number of pairs in $(I_{n'}/p^r I_{n'})^2$ with Gram matrix congruent to T modulo p^r. At infinity take the density of the image of Lebesgue measure under the Gram map, with covolume one for $I_{n'}^2$ and for the lattice of integral Hermitian matrices in the target [We65, Theorem 5]. The condition $n' > 4$ is the range of absolute convergence of the Eisenstein series for pairs. If a positive definite T is represented over every $\mathbb{Z}_p$, then $R_{n'}(T) > 0$. Some lattice in the genus therefore represents T, although a prescribed lattice can fail to do so.

Problem 22.4.3. Let 1_2 be the identity matrix. Then I_5 contains 320 pairs (x, y) with $\mathrm{Gram}(x, y) = 1_2$, and $\Lambda \perp I_1$ contains none. Hence $R_5(1_2) = 1/384$.

For $a = 0$ one can take the lift one step further and pair it with the constant form.

Problem 22.4.4. For $n' \geq 3$, $\langle v_0, 1\rangle = M_{n'}\, E^{(n')}(\mathrm{i}/2)$. For $n' = 5$ this is $G_5(\mathrm{i}/2)/73728$, and $G_5(\mathrm{i}/2) = 2.06195\ldots$.

The classical Rallis inner product formula gives a nonvanishing criterion. Let φ be a nonzero form on Cl_n that is a decomposable vector in an irreducible automorphic representation, and form its theta lift $\Theta\varphi$ to $\mathrm{Cl}_{n'}$, $n' > 4n$, with decomposable test data. In the doubling calculation of $\|\Theta\varphi\|^2$, one integrates the doubled theta kernel over the target unitary quotient. For the lattice data at the standard stabilizer level this inner integral is a genus average, as in Problem 22.4.2. The Siegel–Weil formula evaluates the theta integral [Ra, JSL]. With the standard doubling normalization, the ratio $\|\Theta\varphi\|^2/\|\varphi\|^2$ is, up to a nonzero measure constant, a partial twisted standard L-value divided by the unramified normalizing product of Tate L-values, times the local integrals at the remaining places [Li, §2.4]. In this range the Euler products converge absolutely and are nonzero, so nonvanishing of those local integrals implies nonvanishing of the lift. For sums of decomposable data or vectors, expand the pairing by sesquilinearity.

The genus averages in this chapter illustrate two steps of the proof: the estimate for the main term of the second moment (Chapter 36) and the norms of the single lifts of the chain (Chapter 55).

In the Lean formalization. The corresponding statements of the Lean proof [GL] are `IsFillingData.mul_sum_norm_sum_cosetAmplitude_sq_le` in `grh/src/New/Spanning/MainTerm/EnergyEsti` for the main term, `exists_adjoint_singleLift_comp_eq` in `grh/src/New/Determinant/Norms/AdjointThetal` for the single lifts, and `inner_product_formula` in `grh/src/Lib/SiegelWeil/RallisInner/Doubling.lean` for the unfolding by doubling.

Hints

§22.1.

22.1.1: $\dim \mathcal{M}_4 = 1$.

22.1.2: $\dim \mathcal{M}_8 = 1$, and $\theta_{E_8 \oplus E_8} = \theta_{E_8}^2$. For the roots of D_{16}^+, compute $x \cdot x$ on the non-trivial coset.

22.1.3: Is each lattice spanned by its roots?

22.1.4: Write $\theta_{\Lambda_{24}} = E_{12} + c\Delta$ and compare coefficients of q; then use $\tau(2) = -24$.

22.1.5: $B_2, B_4, \ldots, B_{16}$; for $m = 16$ one needs $B_8 = -1/30$ and $B_{14} = 7/6$.

22.1.6: Subtract $\mu_{24} E_{12}$ from both sides of (1), and compare coefficients of q.

§22.2.

22.2.1: Since L is unimodular, the volume is that of a Euclidean ball of radius $\sqrt{2t}$ in dimension $2k$.

22.2.2: Induction on k: count first the solutions with $x_k = 0$, then those with $x_k \neq 0$.

22.2.3: Every solution modulo p of $Q(x) \equiv j$ has $x \not\equiv 0$, and the gradient of Q is nonzero there, for every p, because L is unimodular; apply Hensel's lemma.

22.2.4: Separate the solutions with $x \not\equiv 0 \pmod p$, which lift as in Problem 22.2.3, from those with $x \equiv 0$, for which $Q(x) \equiv 0 \pmod{p^2}$. When $p^2 \mid j$, what density comes from vectors divisible by p?

22.2.5: The Euler product of $\zeta(k)$, Euler's formula for $\zeta(k)$ in terms of B_k, and $\sigma_{k-1}(j) = j^{k-1}\sigma_{1-k}(j)$.

§22.3.

22.3.1: Count the pairs with $N \le |c\tau + d| < N + 1$.

22.3.2: $h(x, x)$ is additive on orthogonal sums, and $h(x, x) = x \cdot x$ is even on Λ.

22.3.3: As in Problem 22.2.1, but $\{Q \le t\}$ is now the ball of radius $\sqrt{t}$. The counting argument of Problems 22.2.3–22.2.4 uses only that $Q \bmod p$ is isometric to H^4, which holds for $x_1^2 + \cdots + x_8^2$ and odd p. Then $\zeta(4) = \pi^4/90$.

22.3.4: Write the count as $\frac{1}{8}\sum_{t \bmod 8} e(-tj/8)\, g(t)^8$ with the Gauss sums $g(t) := \sum_{x \bmod 8} e(tx^2/8)$, where $e(u) := \exp(2\pi i u)$. For $r \ge 3$, how does adding 2^{r-1} to the first odd coordinate change the norm modulo 2^{r+1}?

22.3.5: Problem 21.1.2 and $|\Gamma_\Lambda| = 46080$.

22.3.6: Both sides lie in $\mathcal{M}_5(4, \chi)$; compare the coefficients of q^0, q^1, q^2.

22.3.7: As in Problem 22.3.6; then combine with it.

§22.4.

22.4.1: Substitute $x \mapsto \gamma x$ for $\gamma \in \Gamma_{L'}$, and $x \mapsto \mathrm{i}x$.

22.4.2: Problem 21.3.2: $\langle x^a, y^a \rangle = h(x, y)^a$. Then group the pairs by their Gram matrix.

22.4.3: Problem 21.2.3: the vectors of $\Lambda \perp I_1$ with $h(x, x) = 1$ are ue, $u \in \mu_4$.

22.4.4: What is $v_0(L')$ as a value of $\theta_{L'}$?

References

[Br] H. Braun, *Zur Theorie der hermitischen Formen*, Abh. Math. Sem. Hansischen Univ. **14** (1941), 61–150.

[Ca] J. W. S. Cassels, *Rational Quadratic Forms*, Academic Press, 1978.

[CoS] J. H. Conway and N. J. A. Sloane, *Sphere Packings, Lattices and Groups*, 3rd ed., Grundlehren Math. Wiss. 290, Springer, 1999.

[DS] F. Diamond and J. Shurman, *A First Course in Modular Forms*, Grad. Texts in Math. 228, Springer, 2005.

[GL] L. Sernau, *GRH for Dirichlet L-functions, in Lean 4*, a shorter rewriting of the Lean proof, text by Claude, `https://github.com/lsernau/grh-lean`, commit `72fead1`, readable edition `grh/`.

[Iw] H. Iwaniec, *Topics in Classical Automorphic Forms*, Grad. Stud. Math. 17, Amer. Math. Soc., 1997.

[Ko] N. Koblitz, *Introduction to Elliptic Curves and Modular Forms*, 2nd ed., Grad. Texts in Math. 97, Springer, 1993.

[JSL] J.-S. Li, *Non-vanishing theorems for the cohomology of certain arithmetic quotients*, J. Reine Angew. Math. **428** (1992), 177–217.

[Li] C. Li, *Geometric and arithmetic theta correspondences*, arXiv:2402.12159, 2024.

[Liouville] J. Liouville, *Nombre des représentations d'un entier quelconque sous la forme d'une somme de dix carrés*, J. Math. Pures Appl. (2) **11** (1866), `https://www.numdam.org/item/JMPA_1866_2_11__1_0/`.

[Mi] J. Milnor, *Eigenvalues of the Laplace operator on certain manifolds*, Proc. Nat. Acad. Sci. USA **51** (1964), 542.

[Ra] S. Rallis, *Injectivity properties of liftings associated to Weil representations*, Compositio Math. **52** (1984), 139–169.

[SeA] J.-P. Serre, *A Course in Arithmetic*, Grad. Texts in Math. 7, Springer, 1973.

[Si] C. L. Siegel, *Über die analytische Theorie der quadratischen Formen*, Ann. of Math. **36** (1935), 527–606.

[We65] A. Weil, *Sur la formule de Siegel dans la théorie des groupes classiques*, Acta Math. **113** (1965), 1–87.

DEFINITE THETA LIFTS AND THEIR NORMS

Prerequisites. Chapter 21, *Masses and the count of forms*: the class sets Cl_n, the groups Γ_L, the representations $V_\lambda(L) = \mathbb{S}_\lambda(L_{\mathbb{C}})$, the notation e^ν in Sym^a, and the spaces of forms $\mathcal{A}_\lambda(n)$ with their norm (Sections 21.1 and 21.3). From Chapter 11: Theorem 11.3.1 and Problems 11.3.7, 11.3.1 and 11.3.4. From Chapter 15: Section 15.1 and Problem 15.1.3. Stirling's formula.

Since a definite unitary group has a finite class set, a theta lift between two such groups is a finite matrix. What are its entries, and how large is it? We compute both in the smallest cases.

23.1. The theta kernel

How does one map forms on one class set to forms on another? The idea is to sum over all homomorphisms between the two lattices, with a Gaussian weight.

Let L and L' be positive definite unimodular Hermitian lattices over $\mathcal{O} = \mathbb{Z}[\mathrm{i}]$ of ranks n and n'. For $x \in \mathrm{Hom}_{\mathcal{O}}(L, L')$ let $x^* \in \mathrm{Hom}(L'_{\mathbb{C}}, L_{\mathbb{C}})$ be its adjoint, and let $h(x, y) := \mathrm{tr}(y^* x)$. Let

$$\Theta_{L,L'}(Z) := \sum_{x \in \mathrm{Hom}_{\mathcal{O}}(L,L')} e^{-\pi h(x,x) + \mathrm{tr}(Zx)}, \qquad Z \in \mathrm{Hom}(L'_{\mathbb{C}}, L_{\mathbb{C}}).$$

For a polynomial P in the entries of x, let $P(\partial)$ be the differential operator obtained by replacing $x_{\beta\alpha}$ with $\partial/\partial Z_{\alpha\beta}$. For a weight λ define

$$\vartheta_\lambda(L, L') := \sum_{x \in \mathrm{Hom}_{\mathcal{O}}(L,L')} \mathbb{S}_\lambda(x)\, e^{-\pi h(x,x)} \colon V_\lambda(L) \to V_\lambda(L'),$$

and, for the class sets Cl_n and $\mathrm{Cl}_{n'}$, the *lift* $\Theta_\lambda \colon \mathcal{A}_\lambda(n) \to \mathcal{A}_\lambda(n')$,

$$(\Theta_\lambda \varphi)(L') := \sum_{L \in \mathrm{Cl}_n} \frac{1}{|\Gamma_L|}\, \vartheta_\lambda(L, L')\, \varphi(L). \tag{1}$$

In bases, Θ_λ is a finite matrix whose block in row L' and column L is $|\Gamma_L|^{-1}\vartheta_\lambda(L, L')$, restricted from $V_\lambda(L)^{\Gamma_L}$ to $V_\lambda(L')^{\Gamma_{L'}}$. For a matrix coefficient P of $\mathbb{S}_\lambda$, the series $\sum_x P(x)\, q^{h(x,x)}$ is a classical theta series with polynomial coefficients, and the corresponding entry of ϑ_λ is its value at $q = e^{-\pi}$.

Thus $\Theta_{L,L'}$ is a theta function of the Hermitian lattice $\mathrm{Hom}_{\mathcal{O}}(L, L')$, which is unimodular of rank nn' by Problem 23.1.1 below. Chapter 12, *The Fock model and theta intertwiners*, treats one-variable theta functions of self-dual lattices with semicharacters; for commensurable lattices whose semicharacters agree on their intersection it defines an intertwiner, and for the neighbours of $\mathbb{Z}[\mathrm{i}]$ studied there the composition scalar is a root of unity given by a Gauss sum. The problems of this chapter use only the series itself.

Problem 23.1.1. If L and L' are unimodular, then with $h(x, y) = \mathrm{tr}(y^* x)$, $\mathrm{Hom}_{\mathcal{O}}(L, L')$ is a unimodular Hermitian lattice of rank nn', and $\mathrm{Hom}_{\mathcal{O}}(I_n, I_{n'}) \cong I_{nn'}$.

Date: November 25, 2026.

Problem 23.1.2. $\Theta_{L,L'}$ is entire, and $P(\partial)\Theta_{L,L'}(0) = \sum_x P(x)\, e^{-\pi h(x,x)}$. If $\Theta_{L,L'}(Z) = \sum_\nu b_\nu Z^\nu$ and $P(x) = \sum_\nu P_\nu x^\nu$, with the matching indexing of the entries of Z and of x, this equals $\sum_\nu P_\nu\, \nu!\, b_\nu$.

Problem 23.1.3. In Schur bases of $V_\lambda(L)$ and $V_\lambda(L')$ obtained over $\mathbb{Q}$ from $\mathcal{O}$-bases of L and L', each entry of $\vartheta_\lambda(L,L')$ is $P(\partial)\Theta_{L,L'}(0)$ for a polynomial P, homogeneous of degree $|\lambda|$, with rational coefficients. Moreover $\vartheta_\lambda(L,L') = 0$ unless $4 \mid |\lambda|$.

Problem 23.1.4. For $\gamma \in \Gamma_L$ and $\gamma' \in \Gamma_{L'}$, $\mathbb{S}_\lambda(\gamma')\,\vartheta_\lambda(L,L') = \vartheta_\lambda(L,L') = \vartheta_\lambda(L,L')\,\mathbb{S}_\lambda(\gamma)$. Hence (1) is a form on $\mathrm{Cl}_{n'}$, and it does not depend on the lattices chosen in the classes, up to transport of forms along isometries.

Problem 23.1.5. $\vartheta_\lambda(L,L')^* = \vartheta_\lambda(L',L)$. Hence the lift $\Theta'_\lambda\colon \mathcal{A}_\lambda(n') \to \mathcal{A}_\lambda(n)$ in the other direction is the adjoint of Θ_λ: $\langle \Theta_\lambda\varphi, \psi\rangle = \langle \varphi, \Theta'_\lambda\psi\rangle$.

23.2. The smallest examples

What are these matrices for $\mathrm{U}(1)\times\mathrm{U}(1)$ and $\mathrm{U}(1)\times\mathrm{U}(2)$? By Problem 21.1.4 each class set has one element, and the lift is a single block. Everything is expressed through the Gaussian moments

$$c_a := \sum_{\alpha\in\mathcal{O}} \alpha^a e^{-\pi|\alpha|^2} \qquad (a \ge 0).$$

Let ϖ, ϑ_0 and $F = \sigma^2\wp$ be as in §15.1.

Problem 23.2.1. c_a is real, $c_a = 0$ unless $4 \mid a$, and $c_a = \vartheta_0\,(\varpi/2\pi)^a F^{(a)}(0)$ with $F^{(a)}(0) \in \mathbb{Q}$.

Problem 23.2.2. For $a = 0, 4, 8, 12, 16$ the rational numbers $F^{(a)}(0)$ are 1, 4, 272, -7104, 3203328.

We identify $\mathrm{Sym}^a(\mathbb{C}) = \mathbb{C}e^a$ with $\mathbb{C}$ by $e^a \mapsto 1$, so that the values $\varphi(I_1)$ of forms on $\mathrm{U}(1)$ are numbers.

Problem 23.2.3. For $n = n' = 1$ and $4 \mid a$, $\Theta_{(a)}$ is multiplication by $c_a/4$ on the line $\mathcal{A}_{(a)}(1)$.

For $n = 1$ and $n' = 2$, $\mathrm{Hom}_\mathcal{O}(I_1, I_2) = \mathcal{O}^2$ is the space of columns $x = (x_1, x_2)$.

Problem 23.2.4. For $\varphi \in \mathcal{A}_{(a)}(1)$,

$$(\Theta_{(a)}\varphi)(I_2) = \frac{\varphi(I_1)}{4} \sum_j \binom{a}{j} c_j c_{a-j}\, e_1^j e_2^{a-j}.$$

For $a = 8$ this is $4\varphi(I_1)\,\vartheta_0^2(\varpi/2\pi)^8\big(17e_1^8 + 70e_1^4e_2^4 + 17e_2^8\big)$.

Problem 23.2.5. The lift $\Theta'_{(a)}\colon \mathcal{A}_{(a)}(2) \to \mathcal{A}_{(a)}(1)$ is

$$(\Theta'_{(a)}\psi)(I_1) = \frac{1}{32} \sum_j c_j c_{a-j}\, \psi_j, \qquad \text{where } \psi(I_2) = \sum_j \psi_j\, e_1^j e_2^{a-j}.$$

How large are these entries?

Problem 23.2.6. $\log c_a^2 \le a\log a - a(1 + \log 2\pi) + O(\log a)$, where $\log 0 := -\infty$.

Numerically the bound is attained up to $O(\log a)$: for $a = 40, 80, \dots, 240$ the left side exceeds the right side without the $O(\log a)$ by between 1.7 and 4.8. The scale 2π belongs to the Gaussian; the rational part $F^{(a)}(0)$ of c_a sees instead the period. By Problem 11.3.7, $\varpi^2/2\pi = \Omega/4$ with $\Omega = 2\varpi^2/\pi$, and by Theorem 11.3.1, $\log\Omega = \gamma + \log\pi - L'(1,\chi)/L(1,\chi)$. Combining these with Problems 23.2.1 and 23.2.6 gives

$$\log F^{(a)}(0)^2 \le a\log a - a\Big(1 + \gamma + \log\frac{\pi}{4} - \frac{L'(1,\chi)}{L(1,\chi)}\Big) + O(\log a). \tag{2}$$

This is how Euler's constant and $L'(1,\chi)/L(1,\chi)$ enter the linear term of a size bound.

23.3. The Gaussian norm and the norm of the lift

The size of an entry is one thing; the size of the lift is measured by its operator norm. What is $\|\Theta_{(a)}\|$ in the smallest case?

Let $\mathcal{F}_m$ be the space of entire functions on $\mathbb{C}^m$ with

$$\|f\|^2 := \pi^{-m}\int_{\mathbb{C}^m} |f(z)|^2 e^{-|z|^2}\, dA(z) < \infty.$$

For $m = 1$ this is the norm of Chapter 5, in which the monomials are orthogonal and $\|z^a\|^2 = a!$ (Problem 5.4.4); since the measure and the inner product of two monomials factor over the variables, the monomials z^ν are orthogonal in $\mathcal{F}_m$ with $\|z^\nu\|^2 = \nu!$. By Problems 21.3.2 and 5.4.4, sending e^ν to z^ν identifies $\mathrm{Sym}^a(\mathbb{C}^m)$ with the homogeneous polynomials of degree a in $\mathcal{F}_m$, with $\|e^\nu\|^2 = \|z^\nu\|^2/a!$. In this normalization the size of a derivative is controlled as follows.

Problem 23.3.1. If $\Theta(Z) = \sum_\nu b_\nu Z^\nu$ and $P = \sum_\nu P_\nu x^\nu$, then

$$|P(\partial)\Theta(0)|^2 \le \|P\|_{\mathcal{F}}^2 \sum_{\nu\in\operatorname{supp} P} \nu!\,|b_\nu|^2.$$

What is the squared norm of the lift from U(1) to U(2)?

Problem 23.3.2. For $\Theta_{(a)}\colon \mathcal{A}_{(a)}(1) \to \mathcal{A}_{(a)}(2)$ and $\varphi \neq 0$,

$$\frac{\|\Theta_{(a)}\varphi\|^2}{\|\varphi\|^2} = \frac{1}{128}\sum_{x,y\in\mathcal{O}^2} h(x,y)^a e^{-\pi(|x|^2+|y|^2)} = \frac{1}{128}\sum_j \binom{a}{j} c_j^2 c_{a-j}^2.$$

For $a = 4$ and $a = 8$ it equals $\frac14\vartheta_0^4(\varpi/2\pi)^8$ and $1296\,\vartheta_0^4(\varpi/2\pi)^{16}$.

The middle expression is a theta sum over $\mathrm{Hom}_{\mathcal{O}}(I_1 \oplus I_1, I_2)$, the lattice of pairs (x,y). This is the structure of the Rallis inner product formula [Ra]. More generally, the diagonal kernel of $\Theta'_\lambda\Theta_\lambda$ is a stabilizer-weighted sum over $L' \in \mathrm{Cl}_{n'}$ of theta series on the doubled lattice $\mathrm{Hom}_{\mathcal{O}}(L\oplus L, L')$. In the convergent range the Siegel–Weil formula identifies the corresponding adelic theta integral with an Eisenstein series [We65], and the doubled theta sum is the construction behind the inner product formula of [Ra, §1]. For $4 \mid a$ the source $\mathcal{A}_{(a)}(1)$ is a line, and Problem 23.3.2 computes the scalar directly.

The two smallest lifts satisfy the following norm estimate.

Theorem 23.3.1. *For the lifts $\Theta_{(a)}\colon \mathcal{A}_{(a)}(1) \to \mathcal{A}_{(a)}(n')$ with $n' = 1, 2$, one has $\|\Theta_{(a)}\|^2 = c_a^2/16$ and $\|\Theta_{(a)}\|^2 = \frac{1}{128}\sum_j \binom{a}{j} c_j^2 c_{a-j}^2$ respectively, and in both cases*

$$\log\|\Theta_{(a)}\|^2 \le a\log a - a(1 + \log 2\pi) + O(\log a).$$

So the squared norm of the lift is at most a power of a times one factorial, $\|z^a\|^2 = a!$, times $(2\pi)^{-a}$. Numerically, for $n' = 2$ and $a = 40, 80, \dots, 240$, the left side exceeds the right side without the $O(\log a)$ by an amount growing from 1.5 to 5.1, roughly like $2\log a - 5.8$.

What kind of number is $c_a^2/16$? For $4 \mid n$ the function $\upsilon_n((\alpha)) := \alpha^n$ is well defined on the nonzero ideals of $\mathcal{O}$, since the units of $\mathcal{O}$ are fourth roots of unity; it is a Hecke character. For $\Re s > n/2 + 1$ let

$$L(\bar\upsilon_n, s) := \sum_{\mathfrak{a}\neq 0} \overline{\upsilon_n(\mathfrak{a})}\, \mathrm{N}\mathfrak{a}^{-s} = \frac{1}{4} \sum_{\alpha\in\mathcal{O}}{}' \bar\alpha^n |\alpha|^{-2s}.$$

For $n \geq 4$ the series converges at $s = n$, where it equals $\frac{1}{4}\sum'_\alpha \alpha^{-n} = (2\varpi)^n H_n/(4\cdot n!)$ by Problem 11.3.1.

Problem 23.3.3. For $4 \mid n$ and $n \geq 4$, $\left|\sum'_\alpha \alpha^{-n} - 4\right| < 3$. Hence $L(\bar\upsilon_n, n) > 0$ and $H_n > 0$.

Problem 23.3.4. For $4 \mid a$ and $a \geq 4$ there is $\kappa_a \in \mathbb{Q}$ (a local notation of this chapter) with

$$\frac{c_a^2}{16} = \kappa_a\, \vartheta_0^2\, (2\pi)^{-2a}\, L(\bar\upsilon_{2a}, 2a),$$

and $\kappa_a \neq 0$ if and only if $F^{(a)}(0) \neq 0$. Moreover $\kappa_4 = 2100$ and $\kappa_8 = 22992840000$.

So for $4 \mid a$, $a \geq 4$, the squared norm of the smallest lift is a value of a Hecke L-function times the factor $\vartheta_0^2(2\pi)^{-2a}$, up to a rational factor that the problem does not explain.

23.4. The seesaw

A seesaw computes one period in two ways: lift to a large group and restrict to a subgroup, or restrict first and lift between smaller groups [Ku]. In the definite lattice model, take an orthogonal decomposition $L' = L_1 \perp L_2$.

Problem 23.4.1. $\Theta_{L,L_1\perp L_2}(Z_1, Z_2) = \Theta_{L,L_1}(Z_1)\,\Theta_{L,L_2}(Z_2)$.

Here is the smallest case. Write $I_2 = Y \perp \mathcal{O}z$ with $Y = \mathcal{O}e_1$ and $z = e_2$, and let $0 \leq j \leq a$ be integers with $4 \mid j$ and $4 \mid a - j$. For $\psi \in \mathcal{A}_{(a)}(2)$ and $\xi \in \mathcal{A}_{(j)}(1)$, viewed as a form on the class set of Y, the *period* of ψ along Y is

$$P(\psi, \xi) := \frac{1}{|\Gamma_Y|} \big\langle \psi(Y \perp \mathcal{O}z),\ \xi(Y)\, e_2^{a-j} \big\rangle.$$

On the other side let $\theta_z := \vartheta_{(a-j)}(\mathcal{O}z, I_1)\, e_2^{a-j} \in \mathrm{Sym}^{a-j}(\mathbb{C})$, the vector obtained from $\mathcal{O}z$ alone. Since $4 \mid a$, we identify each vector of $\mathrm{Sym}^a((I_1)_\mathbb{C})$ with the unique form in $\mathcal{A}_{(a)}(1)$ taking that value at I_1.

Problem 23.4.2. For $\varphi \in \mathcal{A}_{(a)}(1)$ and $\xi \in \mathcal{A}_{(j)}(1)$,

$$P(\Theta_{(a)}\varphi, \xi) = \big\langle \varphi,\ (\Theta_{(j)}\xi)(I_1)\, \theta_z \big\rangle,$$

where the pairing on the right is the inner product of $\mathcal{A}_{(a)}(1)$, the product is that of $\mathrm{Sym}^j(\mathbb{C}) \otimes \mathrm{Sym}^{a-j}(\mathbb{C}) \to \mathrm{Sym}^a(\mathbb{C})$, and $e_1 \mapsto 1$ identifies Y with I_1 for the lift of ξ; both factors of the product take values in the symmetric algebra of $(I_1)_\mathbb{C} = \mathbb{C}$. Both sides equal $\varphi(I_1)\overline{\xi(I_1)}\, c_j c_{a-j}/16$.

The left side lifts φ to U(2) and integrates along U(1). The right side lifts ξ to U(1) and pairs with φ there; it depends on ξ only through $\Theta_{(j)}\xi$. Here both sides are computed explicitly.

Problem 23.4.3. For $(a,j) = (8,4)$ both sides of Problem 23.4.2 equal $\varphi(I_1)\overline{\xi(I_1)}\,\vartheta_0^2(\varpi/2\pi)^8$.

In the proof an identity of the same kind holds for chains of m lifts (Theorem 43.4.1): on the ramified source forms, the lower chain applied to the Poincaré image of a form equals one constant $c \neq 0$, independent of the twist, times a composite lift along the upper chain restricted to Y_m, whose data are chosen for each twist.

23.5. Chains

How do kernels and norms behave under composition?

Problem 23.5.1. The composite $\mathcal{A}_\lambda(n) \to \mathcal{A}_\lambda(n') \to \mathcal{A}_\lambda(n'')$ of two lifts is $\varphi \mapsto \big(L'' \mapsto \sum_{L\in \mathrm{Cl}_n} |\Gamma_L|^{-1} K(L,L'')\,\varphi(L)\big)$, with the kernel

$$K(L,L'') = \sum_{L'\in \mathrm{Cl}_{n'}} \frac{1}{|\Gamma_{L'}|}\,\vartheta_\lambda(L',L'')\,\vartheta_\lambda(L,L').$$

Problem 23.5.2. In the bases e^μ of $\mathrm{Sym}^a(\mathbb{C}^n)$ and $\mathrm{Sym}^a(\mathbb{C}^{n'})$, every entry of $\vartheta_{(a)}(I_n, I_{n'})$ lies in $\vartheta_0^{nn'}(\varpi/2\pi)^a\,\mathbb{Q}$.

So for fixed n, n' and a, the entries of the standard kernel have the common factor $\vartheta_0^{nn'}(\varpi/2\pi)^a$. For a term of the composite kernel passing through standard lattices of ranks $n_0,\dots,n_m$, the product of its kernel entries lies in $\vartheta_0^{\sum_{j=1}^m n_{j-1}n_j}(\varpi/2\pi)^{ma}\,\mathbb{Q}$; the class sums add the weights $1/|\Gamma_L|$.

Problem 23.5.3. Let $S \subset R$ be commutative rings and $D_1,\dots,D_m \in R$. Suppose that in a composite of m maps $(T_j f)(i') = \sum_i h_j(i)\,K_j(i,i')\,f(i)$, with finite sums and $h_j(i) \in R$, all $K_j(i,i')$ and all starting values lie in S, and that $D_j h_j(i) \in S$ for all i. Then $D_1\cdots D_m$ times every final value lies in S.

How large is a chain? It is measured by the volume $\det(u^*u)$ of the map u it defines.

Problem 23.5.4. Let $u_j\colon H_{j-1} \to H_j$, $1 \le j \le m$, be linear maps between complex inner product spaces of the same finite dimension, and $u := u_m \circ \cdots \circ u_1$. Then $\det(u^*u) = \prod_j \det(u_j^* u_j)$. For $4 \mid a$ the space $\mathcal{A}_{(a)}(1)$ is a line, and for the chain of m lifts $\Theta_{(a)}\colon \mathcal{A}_{(a)}(1) \to \mathcal{A}_{(a)}(1)$ this is $(c_a^2/16)^m$.

Problem 23.5.5. Let $u(\omega)\colon H \to H'$ be linear maps of finite-dimensional complex inner product spaces, depending on a parameter ω, with $\langle u(\omega)x, u(\omega)y\rangle = a(\omega)\langle S(\omega)x, y\rangle$ for all $x, y \in H$, where $a(\omega) \in \mathbb{C}$ and $S(\omega) \in \mathrm{End}(H)$. Then $\det(u(\omega)^*u(\omega)) = a(\omega)^{\dim H}\det S(\omega)$. Hence, if $\det(u(1)^*u(1)) \neq 0$ and $a(\omega) = c\,b(\omega)$ with c independent of ω and $b(1) \neq 0$, the ratio $\det(u(\omega)^*u(\omega))/\det(u(1)^*u(1))$ equals $(b(\omega)/b(1))^{\dim H}\det S(\omega)/\det S(1)$ and does not involve c.

For the chains of the proof see Chapter 34. Theorem 55.4.1 compares the determinant of the chain from Y_0 to Y_m with the determinants of the single lifts from W_j

to V_j. Problem 23.5.4 gives a model for composition, and Problem 23.5.5 explains how division by the value at the trivial twist cancels the common constant.

Beyond the smallest cases a chain needs more. The class sets grow with the rank (Section 21.2), and in the proof the norm of a lift comes from Rallis's inner product formula (Theorem 56.2.1) in place of Problem 23.3.2. For the moments c_a the rational factors are the derivatives $F^{(a)}(0)$; Problem 15.5.3 gives a one-variable obstruction at inert primes, and Theorem 16.3.1 gives a divisibility bound for the normalized two-variable moments $t(a, w)$ of Section 15.1 when $p \equiv 3 \pmod 8$. Constants need not be exact: one seesaw constant works for all twists (Theorem 43.4.1), and constants independent of the twist cancel in the ratio of Theorem 55.4.1.

In the upper-bound argument of the proof, the seesaw transfers a size bound for the composite lift to the lower chain on Poincaré images (Theorem 43.4.1). In the lower-bound argument, the norms of single lifts enter the factorization of the ratio of chain determinants (Theorem 55.4.1).

In the Lean formalization. The corresponding statement of the Lean proof [GL] for the squared norm of a lift, as in Problem 23.3.4, is `New.LValueData.inner_trivialLift_self_eq_L` in `New/OneLift/HeckeValues/CharacterLiftNorm.lean`; it concerns the lift of a character from U(1) to a definite U($2k$) with $k \geq 2$.

23.6. Questions

For a tending to infinity through multiples of 4, does $\log c_a^2 = a \log a - a(1 + \log 2\pi) + O(\log a)$ hold? Section 23.2 gives numerical examples.

Hints

§23.1.

23.1.1: In bases, $h(x, y) = \sum_{\alpha,\beta} x_{\beta\alpha}\bar{y}_{\beta\alpha}$ when L and L' are standard. In general, if G and G' are the Gram matrices of L and L', so that $h(u, v) = \bar{v}^t G u$, then $y^* = G^{-1}\bar{y}^t G'$; compute the Gram matrix of $\mathrm{Hom}(L, L')$ and its determinant.

23.1.2: Differentiate under the sum; $\partial/\partial Z_{\alpha\beta}$ brings down $x_{\beta\alpha}$.

23.1.3: The entries of $x^{\otimes k}$ are monomials in the entries of x. For the vanishing, replace x by $\mathrm{i}x$.

23.1.4: Substitute $x \mapsto \gamma' x$ and $x \mapsto x\gamma$; both preserve $\mathrm{Hom}_{\mathcal{O}}(L, L')$ and $h(x, x)$.

23.1.5: $\mathbb{S}_\lambda(x)^* = \mathbb{S}_\lambda(x^*)$. What does $x \mapsto x^*$ do to $\mathrm{Hom}(L, L')$ when L and L' are unimodular?

§23.2.

23.2.1: Use the symmetries of the square lattice and Problem 15.1.3. For rationality: the Laurent coefficients of $\wp$ lie in $\mathbb{Q}[g_2, g_3]$, and $(\log\sigma)'' = -\wp$.

23.2.2: Expand σ and $\wp$ with $g_2 = 4$, $g_3 = 0$ further than in Problem 15.1.2.

23.2.3: $\Gamma_{I_1} = \mu_4$, and $\mathrm{Sym}^a(x)$ is multiplication by x^a.

23.2.4: $\mathrm{Sym}^a(x)$ sends $1 \in \mathrm{Sym}^a(\mathbb{C})$ to $(x_1 e_1 + x_2 e_2)^a$. Expand by the binomial theorem; the sum over $\mathcal{O}^2$ factors.

23.2.5: $\mathrm{Hom}(I_2, I_1)$ consists of rows y, and $\mathrm{Sym}^a(y)\, e_1^j e_2^{a-j} = y_1^j y_2^{a-j}$. Alternatively use Problems 23.1.5 and 21.3.2.

23.2.6: $|c_a| \le \sum_\alpha f(\alpha)$ with $f(z) := |z|^a e^{-\pi|z|^2}$. Bound the $O(a)$ terms with $|\alpha|^2 \le a$ by $\max f$, attained at $|z|^2 = a/2\pi$, and the others by a geometric series.

§23.3.

23.3.1: Problem 23.1.2, and the Cauchy–Schwarz inequality.

23.3.2: $\|\Theta\varphi\|^2 = \langle \Theta'\Theta\varphi, \varphi\rangle$; use Problems 23.2.4 and 23.2.5. For the middle expression use $\langle u^a, v^a\rangle = \langle u, v\rangle^a$.

Theorem 23.3.1: Combine Problems 23.2.3, 23.2.6 and 23.3.2 with $\binom{a}{j} j!(a-j)! = a!$ and Stirling's formula.

23.3.3: Separate the units, and compare the other terms with Problem 11.3.4 at $s = 2$.

23.3.4: Problem 23.2.1, the expression of $L(\bar{v}_n, n)$ by H_n, and Problem 23.3.3. For κ_8: $H_{16} = 43659/170$.

§23.4.

23.4.1: How does $\mathrm{Hom}_{\mathcal{O}}(L, L_1 \perp L_2)$ decompose, and what happens to h and $\mathrm{tr}(Zx)$?

23.4.2: Problems 23.2.3, 23.2.4 and 21.3.2.

23.4.3: Problems 23.2.1 and 15.1.2.

§23.5.

23.5.1: Substitute (1) into itself.

23.5.2: Expand a single monomial coefficient of $\mathrm{Sym}^a(x)\, e^\mu$, sum it over x, and compare with Problem 23.2.1.

23.5.3: Induction on m: move D_1 inside the first sum.

23.5.4: In orthonormal bases $\det(u^* u) = |\det u|^2$. For the lifts use Problem 23.2.3.

23.5.5: Express the Gram identity through the adjoint.

References

[GL] L. Sernau, *GRH for Dirichlet L-functions, in Lean 4*, a shorter rewriting of the Lean proof, text by Claude, `https://github.com/lsernau/grh-lean`, commit `72fead1`, readable edition `grh/`.

[Ku] S. S. Kudla, *Seesaw dual reductive pairs*, in *Automorphic Forms of Several Variables (Katata, 1983)*, Progr. Math. 46, Birkhäuser, 1984, 244–268.

[Ra] S. Rallis, *Injectivity properties of liftings associated to Weil representations*, Compositio Math. **52** (1984), 139–169.

[We65] A. Weil, *Sur la formule de Siegel dans la théorie des groupes classiques*, Acta Math. **113** (1965), 1–87.

HECKE OPERATORS AND THETA LIFTS

Prerequisites. Even unimodular lattices, E_8, theta series and the Hecke operators T_n on modular forms of level one [SeA, Ch. V and VII]. Quadratic forms over $\mathbb{F}_p$ and the number of their isotropic vectors (for split forms, Problem 22.2.2). Gaussian binomial coefficients $\begin{bmatrix} a \\ b \end{bmatrix}_Q$, which count the b-dimensional subspaces of $\mathbb{F}_Q^a$ [Andr, Ch. 3]. From Chapter 21, *Masses and the count of forms*: Section 21.1, in particular Problems 21.1.1, 21.1.2 and 21.2.3. From Chapter 22, *The Siegel–Weil formula in the smallest case*: Problems 22.1.2 and 22.3.7. From Chapter 23, *Definite theta lifts and their norms*: Section 23.1. For Section 24.4, maximal orders in a definite quaternion algebra over $\mathbb{Q}$ [Gr], [Pi].

A theta lift is a sum over classes of lattices. A Hecke operator on a class set is also a sum over lattices, namely over the neighbours of a lattice. How do the two interact? Eichler found that a theta series summed over the neighbours of a lattice is a Hecke transform of the theta series of the lattice, up to an explicit multiple of the identity [Ei52], [Ei73]; see [An] for Siegel modular forms and [Ra] for the general theta correspondence. We prove this in degree one, and check it on class sets with two elements, where the Hecke operator is a 2×2 matrix.

24.1. Neighbours

How does one move from a lattice to the other lattices of its genus? Kneser's answer is to change it at one prime [Kn].

Let L be a positive definite even unimodular lattice of positive rank $n = 2k$, with $8 \mid n$, and let p be a prime. A *p-neighbour* of L is an even unimodular lattice $M \subset L \otimes \mathbb{Q}$ with $[L : L \cap M] = [M : L \cap M] = p$. Let $\mathcal{N}_p(L)$ be the set of p-neighbours.

Problem 24.1.1. Let p be odd. For $v \in L \setminus pL$ with $v \cdot v \equiv 0 \pmod{2p^2}$, let $L_v := \{x \in L : x \cdot v \equiv 0 \pmod{p}\}$. Then $M_v := L_v + \mathbb{Z}\, v/p$ is a p-neighbour of L, and M_v depends only on the line $\mathbb{F}_p \bar{v} \subset L/pL$. Every p-neighbour arises in this way, from exactly one isotropic line of L/pL.

Problem 24.1.2. For odd p, the quadratic space L/pL over $\mathbb{F}_p$ is split, so that

$$|\mathcal{N}_p(L)| = \frac{(p^k - 1)(p^{k-1} + 1)}{p - 1}.$$

For $L = E_8$ and $p = 3, 5$ this is 1120 and 19656.

For $p = 2$ the same count holds, if v is chosen with $v \cdot v \equiv 0 \pmod 8$ [CL]; for E_8 it is 135. Since E_8 is the only even unimodular lattice of rank 8, all its neighbours are copies of E_8. In each even unimodular genus considered here, the graph on isometry classes defined by p-neighbours is connected for every prime p, by Kneser's theorem [Kn], [CL].

Let Cl be the set of isometry classes in the genus of L, and let $\Gamma_L := \mathrm{O}(L)$. The *neighbour operator* on functions $\varphi\colon \mathrm{Cl} \to \mathbb{C}$ is $(T_p\varphi)(L) := \sum_{M \in \mathcal{N}_p(L)} \varphi(M)$, and

Date: November 25, 2026.

its matrix $N_p(L,M) := \#\{M' \in \mathcal{N}_p(L) : M' \cong M\}$ is the *Brandt matrix* of the class set at p. Let $\langle \varphi, \psi \rangle := \sum_{L \in \mathrm{Cl}} \varphi(L)\overline{\psi(L)}/|\Gamma_L|$, as in Chapter 21.

Problem 24.1.3. $N_p(L,M)/|\Gamma_L| = N_p(M,L)/|\Gamma_M|$. Hence T_p is self-adjoint for $\langle\,,\rangle$, and the constant function is an eigenvector with eigenvalue $|\mathcal{N}_p(L)|$.

In rank 16 the class set is $\{E_8 \perp E_8,\ D_{16}^+\}$, with $|\Gamma| = 2 \cdot 696729600^2$ and $2^{15} \cdot 16!$ [CoS].

Problem 24.1.4. The Brandt matrix of the class set of rank 16 at $p = 2$ is $\begin{pmatrix} 14670 & 18225 \\ 12870 & 20025 \end{pmatrix}$, with eigenvalues 32895 and 1800.

The eigenvalue 1800 is $15\,\tau(2) + (2^4 + 2^5 + \cdots + 2^{10}) + 2^7$, where $\tau(2) = -24$ is the coefficient of Ramanujan's Δ. Chenevier and Lannes explain such identities by the Arthur parameters of the eigenvectors [CL]. In Section 24.2 we show that the theta series of degree one cannot see this eigenvector.

24.2. Eichler's commutation relation in degree one

For L as in Section 24.1, let $r_L(m) := \#\{x \in L : x \cdot x = 2m\}$, with $r_L(m) := 0$ unless $m \in \mathbb{Z}_{\geq 0}$, and let $\theta_L := \sum_m r_L(m)\, q^m$. It is a modular form of weight k for $\mathrm{SL}_2(\mathbb{Z})$ [SeA, Ch. VII], and T_{p^2} acts on its coefficients by

$$a(m) \mapsto a(p^2 m) + p^{k-1} a(m)\,[p \mid m] + p^{2k-2} a(m/p^2).$$

For the remainder of the neighbour count, let p be odd.

Problem 24.2.1. Let $x \in L \setminus pL$ with $x \cdot x = 2m$. The number of $M \in \mathcal{N}_p(L)$ with $x \in M$ is $(p^{2k-2} - 1)/(p-1)$ if $p \nmid m$, and $1 + p(p^{k-1} - 1)(p^{k-2} + 1)/(p-1)$ if $p \mid m$.

Problem 24.2.2. The vectors of $\bigcup_{M \in \mathcal{N}_p(L)} M \setminus L$ are the y/p with $y \in L \setminus pL$ and $y \cdot y \equiv 0 \pmod{2p^2}$, and each lies in exactly one neighbour. Deduce Theorem 24.2.1.

Theorem 24.2.1 (Eichler)**.** *For odd p,* $$\sum_{M \in \mathcal{N}_p(L)} \theta_M = T_{p^2}\theta_L + \frac{p^{2k-2} - p}{p-1}\,\theta_L.$$

Problem 24.2.3. The constant-term identity in Theorem 24.2.1 for $L = E_8$ and $p = 3$ reads $1120 = 757 + 363$. The same identity of constant terms holds for $p = 2$: $135 = 73 + 62$.

Let $\theta(\varphi) := \sum_{L \in \mathrm{Cl}} \varphi(L)\,\theta_L/|\Gamma_L|$ be the *theta lift* of a function on the class set. It is the analogue for these lattices of the lift of Chapter 23 to rank one in weight zero, with the vectors sorted by norm into a q-series instead of weighted by a Gaussian.

Problem 24.2.4. Let p be odd. Then $\theta(T_p\varphi) = \big(T_{p^2} + \frac{p^{2k-2}-p}{p-1}\big)\theta(\varphi)$. If $\theta(\varphi) \neq 0$ and $T_p\varphi = \mu\varphi$, and $\theta(\varphi)$ is an eigenform with $T_p\theta(\varphi) = \lambda\theta(\varphi)$, then $\mu = \lambda^2 - p^{k-1} + (p^{2k-2} - p)/(p-1)$.

For odd p, the theta lift intertwines the neighbour operator with $T_p^2 - p^{k-1} + (p^{2k-2} - p)/(p-1)$ on modular forms.

In rank 16, $\theta_{E_8 \perp E_8} = \theta_{D_{16}^+}$ by Problem 22.1.2 of Chapter 22.

Problem 24.2.5. The eigenvector of Problem 24.1.4 with eigenvalue 1800 lies in the kernel of θ. For the constant function, the eigenvalue 32895 agrees with the formula of Problem 24.2.4 read at $p = 2$, where we have not proved it: $129^2 - 2^7 + (2^{14} - 2) = 32895$.

The two lattices are distinguished by their theta series of degree 4, and not before [CL]. To detect this eigenspace by theta series one can pass to higher degree; for lift norms see Section 23.3.

24.3. Hermitian lattices of rank five

Let $\mathcal{O} = \mathbb{Z}[\mathrm{i}]$, let $p \equiv 1 \pmod 4$ be a prime, and let $p = \pi\bar\pi$ in $\mathcal{O}$. Let L be a unimodular Hermitian lattice of rank $n \geq 1$, as in Chapter 21, and let $L^\sharp$ denote duals. Then $L/\pi L$ is an n-dimensional vector space over $\mathcal{O}/\pi = \mathbb{F}_p$. For a hyperplane $H \subset L/\pi L$ let L_H be its preimage in L, and

$$L'_H := L_H + \pi L_H^\sharp.$$

Problem 24.3.1. L'_H is unimodular and lies in the genus of L, with $L \cap L'_H = L_H$ of index p in both. Moreover $L'_H \subset \bar\pi^{-1}L$, and L is obtained from L'_H by the same construction with $\bar\pi$ in place of π.

We call L'_H a *π-neighbour* of L. There are $(p^n - 1)/(p - 1)$ of them. For L representing a class in Cl_n, the genus of I_n in Chapter 21, set $T_\pi\varphi(L) := \sum_H \varphi(L'_H)$. For the mass inner product, the adjoint of T_π is $T_{\bar\pi}$. Let $r_L(m) := \#\{x \in L : h(x,x) = m\}$ for $m \in \mathbb{Z}_{\geq 0}$ and $r_L(m) := 0$ otherwise, and let $\theta_L := \sum_m r_L(m)\, q^m$, a modular form of weight n for $\Gamma_0(4)$ with character χ^n, where χ is the character modulo 4 [Iw, Ch. 10]. Since $\chi(p) = 1$, T_p acts on such forms by $a(m) \mapsto a(pm) + p^{n-1}a(m/p)$.

Problem 24.3.2. For $x \in L$, the number of H with $x \in L'_H$ is $(p^{n-1} - 1)/(p - 1)$ if $x \notin \pi L$, and $(p^n - 1)/(p - 1)$ if $x \in \pi L$. A vector $x \notin L$ lies in some L'_H exactly when $y := \bar\pi x \in L \setminus \bar\pi L$ and $p \mid h(y,y)$, and then in exactly one.

Problem 24.3.3. $\displaystyle\sum_H \theta_{L'_H} = T_p\theta_L + \frac{p^{n-1} - p}{p - 1}\,\theta_L$. Hence, with $\theta(\varphi) := \sum_{L \in \mathrm{Cl}_n} \varphi(L)\theta_L/|\Gamma_L|$, one has $\theta(T_\pi\varphi) = \big(T_p + \frac{p^{n-1}-p}{p-1}\big)\theta(\varphi)$, and likewise for $\bar\pi$.

Here the factor is linear in T_p. At p the unitary group is $\mathrm{GL}_n(\mathbb{Q}_p)$. In the component corresponding to π, L'_H and L form an edge of type one in the sense of Section 24.5.

Now take $n = 5$, $p = 5$ and $\pi = 2 + \mathrm{i}$. By Problem 21.2.3, $\mathrm{Cl}_5 = \{I_5, \Lambda \perp I_1\}$, where Λ is the Gaussian Hermitian lattice of Section 21.1 with underlying real lattice E_8. By Problems 21.1.2 and 21.2.3 and $|\Gamma_\Lambda| = 46080$ (loc. cit.), $|\Gamma| = 122880$ and 184320, and $r(1) = 20$ and 4.

Problem 24.3.4. The matrix of T_π on Cl_5 is $\begin{pmatrix} 525 & 256 \\ 384 & 397 \end{pmatrix}$, with eigenvalues 781 and 141.

Let g be the cusp form called f in Chapter 22,

$$g = \frac{1}{4}\sum_{\alpha \in \mathcal{O}} \alpha^4 q^{|\alpha|^2} = \eta(\tau)^4\eta(2\tau)^2\eta(4\tau)^4 = q - 4q^2 + 16q^4 - 14q^5 - 64q^8 + 81q^9 + \cdots;$$

here η is Dedekind's function. The form g spans the cusp forms of weight 5 for $\Gamma_0(4)$ with character χ, and it has complex multiplication by $\mathbb{Q}(\mathrm{i})$. By Problem 22.3.7, $\theta_{I_5} - \theta_{\Lambda\perp I_1} = 16\,g$.

Problem 24.3.5. The 141-eigenspace of T_π is spanned by $\varphi = (2,-3)$, and $\theta(\varphi) = g/3840$.

Problem 24.3.6. $a_5(g) = -14 = 2\,\mathrm{Re}\big((2+\mathrm{i})^4\big)$, and $141 = -14 + 155$, as Problem 24.3.3 predicts.

The lift identifies the two class functions supported on single classes, with value 1 there, with the basis $(\theta_{I_5}/122880, \theta_{\Lambda\perp I_1}/184320)$ of its image. In this basis the matrix of $T_5 + 155$ is the matrix of T_π in Problem 24.3.4. Neither theta series is an eigenform; the eigenforms are g and the lift of the constant function, with T_5-eigenvalues -14 and $626 = 781 - 155$.

24.4. Brandt matrices

The original setting of Eichler's relation is a quaternion algebra, where the theta series of the ideal lattices between ideal-class representatives give modular forms of weight two and prime level [Ei73], [Pi], [Gr]. We follow Gross [Gr, §§1–2] in the smallest case with two classes.

Let $B = (-1,-11)/\mathbb{Q}$, with $\mathrm{i}^2 = -1$, $j^2 = -11$ and $k = \mathrm{i}j$; it is ramified exactly at 11 and ∞. Let $\mathcal{O}_1 := \mathbb{Z} + \mathbb{Z}\mathrm{i} + \mathbb{Z}\frac{1+j}{2} + \mathbb{Z}\frac{\mathrm{i}+k}{2}$. There is one other class of maximal orders, represented by an order $\mathcal{O}_2$ with $\Theta_{\mathcal{O}_2} := \sum_{x\in\mathcal{O}_2} q^{N(x)} = 1 + 6q + 6q^3 + 24q^4 + 18q^5 + \cdots$. Let $w_i := |\mathcal{O}_i^\times|/2$. Gross defines the Brandt matrices $B(m)$, $m \ge 1$, whose entries $B_{ij}(m)$ count the elements $b \in M_{ij} := I_j^{-1} I_i$ with $N(b) = m\,N(M_{ij})$, divided by $2w_j$, where $N(M_{ij})$ is the positive generator of the ideal generated by the reduced norms of elements of M_{ij}, for left ideals I_i of a fixed maximal order with right orders $\mathcal{O}_i$; he shows that $B_{ii}(m) = r_{\mathcal{O}_i}(m)/2w_i$, that $w_j B_{ij}(m) = w_i B_{ji}(m)$, and that $\sum_j B_{ij}(m) = \sigma(m)$ for $11 \nmid m$ [Gr, §§1–2]. The assignment $T_m \mapsto B(m)$ identifies the Hecke action on $M_2(\Gamma_0(11))$ with the Brandt action [Gr]. For a prime $\ell \ne 11$, $B_{ij}(\ell)$ counts the left ideals $J \subset I_i$ of the fixed order with $[I_i : J] = \ell^2$ and $J \cong I_j$; there are $\ell + 1$ such J in all, and they play the role of the ℓ-neighbours of Section 24.1.

Problem 24.4.1. $\mathcal{O}_1$ is an order, its norm form is $(a^2+ac+3c^2)+(b^2+bd+3d^2)$, and $\mathcal{O}_1^\times = \{\pm1, \pm\mathrm{i}\}$. Thus $\Theta_{\mathcal{O}_1} = \big(\sum_{a,c} q^{a^2+ac+3c^2}\big)^2$.

Eichler's mass formula $\sum_i 1/w_i = (11-1)/12$ then gives $w_2 = 3$ [Gr].

Problem 24.4.2. $B(2) = \begin{pmatrix} 1 & 2 \\ 3 & 0 \end{pmatrix}$ and $B(3) = \begin{pmatrix} 2 & 2 \\ 3 & 1 \end{pmatrix}$, with eigenvalues $3, -2$ and $4, -1$.

Problem 24.4.3. Let $f := q\prod_{n\ge1}(1-q^n)^2(1-q^{11n})^2 = q - 2q^2 - q^3 + 2q^4 + q^5 + \cdots$. Then $\Theta_{\mathcal{O}_1} - \Theta_{\mathcal{O}_2} = -2f$, and $(1,-1)\,B(\ell) = a_\ell(f)\,(1,-1)$ for $\ell = 2, 3$.

The eigenvalues -2 and -1 are the traces of Frobenius of the elliptic curve $X_0(11)$ at 2 and 3.

24.5. A split place

Consider a theta lift at a split place whose local kernel is the indicator of $xL \subset L'$ for a matrix x; the Hecke operators are sums over edges of lattices. The following subspace count includes the local count in Problem 24.3.2 when the source has rank one.

Let Q be a power of p, and let W be the unramified extension of $\mathbb{Z}_p$ with residue field $\mathbb{F}_Q$. For lattices $L'' \subseteq L$ in a $W[1/p]$-vector space, (L'', L) is an *edge of type* i if $pL \subseteq L'' \subseteq L$ and $\dim_{\mathbb{F}_Q}(L/L'') = i$. Let $L \subset W[1/p]^N$ and $L' \subset W[1/p]^{N+g}$ be lattices, let x be an $(N+g) \times N$ matrix with $xL \subset L'$, and let ρ be the rank of x modulo p as a map $L/pL \to L'/pL'$. Here $N \geq 1$, $g \geq 0$, and $i \geq 0$ are integers, and $\begin{bmatrix} a \\ b \end{bmatrix}_Q = 0$ for $b < 0$ or $b > a$.

Problem 24.5.1. The number of edges (L_1, L') of type i with $xL \subset L_1$ is $\begin{bmatrix} N+g-\rho \\ i \end{bmatrix}_Q$. The number of edges (L, A_1) of type i with $xA_1 \subset L'$ is $\begin{bmatrix} N-\rho \\ i \end{bmatrix}_Q$.

Problem 24.5.2. For every $(N+g) \times N$ matrix x over $W[1/p]$, with $\mathbf{1}_{L,L'}(x) := [xL \subseteq L']$, one has

$$\sum_{(L_1,L') \text{ of type } i} \mathbf{1}_{L,L_1} = \sum_{l=0}^{i} Q^{(i-l)(g-l)} \begin{bmatrix} g \\ l \end{bmatrix}_Q \sum_{(L,A_1) \text{ of type } i-l} \mathbf{1}_{A_1,L'}.$$

For $N = i = 1$, $g = n-1$ and $Q = p$, this gives the count for $x \in L$ in Problem 24.3.2, with ρ the rank of the vector reduced modulo π.

Problem 24.5.3. For $0 \leq l \leq g$, the elementary symmetric polynomial e_l satisfies

$$e_l\big((Q^{(g-1)/2-s})_{0 \leq s < g}\big) = Q^{-l(g-l)/2} \begin{bmatrix} g \\ l \end{bmatrix}_Q.$$

The family of arguments is empty if $g = 0$.

Under the split-kernel hypotheses (S1)–(S3) of [Adr, §§10.3–10.4], write $Q = z^2$ for the residue-field order, with $z = p^{d/2}$ and d the even residue degree, $N_j = N_0 + jg$ with $g \geq 1$ for the ranks, and $T_i^{(j)}$ for the raw edge sums. For $0 \leq r \leq N_0$ set $\mathcal{E}_i^{(j)} = z^{-i(N_j-i)} T_i^{(j)}$ and $E_j(X) := \sum_{i=0}^{r} \mathcal{E}_i^{(j)} X^i$. For $0 \leq j < m$, the lift K_j satisfies $E_{j+1}(X) K_j = P_{j+1}(X) K_j E_j(u_{j+1} X)$ modulo X^{r+1}. If a, a' and μ are the length-weight parameters in (S3) for this lift, then $u_{j+1} = (aa')^{-1}$ is a unit, $m_{j+1} = ap^{\mu}$, and $P_{j+1}(X)$ is the product of $1 + u_{j+1} m_{j+1} \alpha X$ over the arguments α of Problem 24.5.3.

Problem 24.5.4. Suppose that $E_{j+1}(X)\, K_j = K_j\, P_{j+1}(X)\, E_j(X)$ modulo X^{r+1} for $0 \leq j < m$, with $P_{j+1}(X) = \prod_{a \in x_{j+1}} (1 + aX)$, and where $E_j(X) = \sum_i \mathcal{E}_i^{(j)} X^i$, and let Y be the concatenation, with multiplicities, of the families $x_1, \ldots, x_m$ and $\mathcal{K} := K_{m-1} \cdots K_0$. Then $\mathcal{K}\, \mathcal{E}_r^{(0)} = \sum_{l=0}^{r} (-1)^l h_l(Y)\, \mathcal{E}_{r-l}^{(m)}\, \mathcal{K}$, where h_l is the complete symmetric polynomial.

The coefficient of $\mathcal{E}_{r-l}^{(m)} \mathcal{K}$ is $(-1)^l h_l(Y)$. Problem 24.2.4 gives an analogous relation for a single orthogonal theta lift.

This chapter serves one step of the proof: at the exceptional primes below the second cutoff, Section 48.4 of Chapter 48, it transfers the split Hecke operators at the members of a full mark through the chain.

In the Lean formalization. The corresponding statements of the Lean proof [GL] are `New.Data.IsWeakChainDatum.exists_heckePolyOp_lift` for one lift and `New.Data.IsWeakChainDatum.exists_hecke_transfer` for the first $j+1$ lifts, both in `New/UpperBound/Divisibility/ValuationAtNonSplitPrimes.lean`. The full-mark bound for the restricted chain is `New.Data.IsWeakChainDatum.gaugeLe_restrictedChain_of_is` in `New/UpperBound/Divisibility/LocalDivisibility.lean`.

Hints

§24.1.

24.1.1: Compare the two indices at the intersection. For the converse consider $v \in pM \setminus pL$. For the lifting step try $v + ptw$, where $v \cdot w \not\equiv 0 \pmod p$ and $t \in \mathbb{Z}$ is to be chosen.

24.1.2: The discriminant of L/pL is $(-1)^k$ times a square. A split space of dimension $2k$ has $p^{2k-1} + p^k - p^{k-1}$ isotropic vectors, counting 0.

24.1.3: Count the orbits of pairs (L, M) with $M \in \mathcal{N}_p(L)$ under the rational orthogonal group of $L \otimes \mathbb{Q}$, weighted by the inverse order of the stabilizer of the pair, in two ways. The relation is symmetric because $L \in \mathcal{N}_p(M)$.

24.1.4: Chenevier and Lannes give the orbit sizes for the two-neighbours of $E_8 \perp E_8$: 270 and 14400 for the orbits returning to its class, and 135^2 for the orbit reaching D_{16}^+ [CL, Ch. III, §3.1]. The row sums are 32895. Use Problem 24.1.3 for the second row.

§24.2.

24.2.1: Count isotropic lines in $\bar{x}^\perp$, first finding its radical in each case.

24.2.2: Use the description of M_v in Problem 24.1.1. For the theorem, separate $x \in pL$, $x \in L \setminus pL$, and $x \notin L$.

24.2.3: $\sigma_3(9) = 757$ and $\sigma_3(4) = 73$.

24.2.4: Exchange the sums by Problem 24.1.3, then use Theorem 24.2.1. On an eigenform, $T_{p^2} = T_p^2 - p^{k-1}$.

24.2.5: $M_8(\mathrm{SL}_2(\mathbb{Z}))$ is spanned by E_4^2, and $T_2 E_4^2 = (1 + 2^7) E_4^2$. The eigenvector is orthogonal to the constants.

§24.3.

24.3.1: Work locally. Over $\mathbb{Z}_p$, $\mathcal{O} \otimes \mathbb{Z}_p = \mathbb{Z}_p \times \mathbb{Z}_p$, and a self-dual lattice is $A \oplus A^\vee$ for a $\mathbb{Z}_p$-lattice A.

24.3.2: Use the local description of L'_H from Problem 24.3.1, one component at a time.

24.3.3: Sum Problem 24.3.2 over the vectors of norm m, using $h(\bar{\pi}y, \bar{\pi}y) = p\, h(y, y)$ and $r_{\pi L}(m) = r_L(m/p)$. For the identity on class functions, reverse a neighbour edge.

24.3.4: Compare the coefficients of q in Problem 24.3.3 for $L = I_5$, using $r_{I_5}(5) = 8424$ and the values of $r(1)$. For the second row, do the same for $L = \Lambda \perp I_1$, with $r_{\Lambda \perp I_1}(5) = 8648$; or use Problem 24.1.3 together with complex conjugation, which exchanges π- and $\bar{\pi}$-neighbours and fixes both classes.

24.3.5: Use $122880 = 2 \cdot 61440$ and $184320 = 3 \cdot 61440$.

24.3.6: Compute $a_5(g)$ from the product. Then apply Problem 24.3.3 to φ and compare with Problem 24.3.5.

§24.4.

24.4.1: Write an element as $(a + c/2) + (b + d/2)\mathrm{i} + (c/2)j + (d/2)k$.

24.4.2: Find the diagonal entries from $r_{\mathcal{O}_1}(m)$ and from $\Theta_{\mathcal{O}_2}$, and the others from the row sums. Check $w_2 B_{12} = w_1 B_{21}$.

24.4.3: Both sides lie in $M_2(\Gamma_0(11))$, which has dimension 2; compare the coefficients of q^0, q^1, q^2.

§24.5.

24.5.1: Reduce the two edges modulo p and use the image and kernel of $\bar{x}$, respectively.

24.5.2: Problem 24.5.1 and the q-Vandermonde identity [Andr, Ch. 3]

$$\begin{bmatrix} a+b \\ i \end{bmatrix}_Q = \sum_l Q^{(i-l)(b-l)} \begin{bmatrix} b \\ l \end{bmatrix}_Q \begin{bmatrix} a \\ i-l \end{bmatrix}_Q .$$

24.5.3: Use the Gaussian binomial theorem

$$\prod_{s=0}^{g-1} (1 + Q^s z) = \sum_l Q^{l(l-1)/2} \begin{bmatrix} g \\ l \end{bmatrix}_Q z^l .$$

24.5.4: Compose the identities in increasing stage order and invert the resulting scalar series.

References

[Adr] J. Adriazola, *The Alpöge proof of the Riemann hypothesis*, manuscript, revised 24 November 2026, `https://github.com/jimjamzola/RH-Alpoge-Reconstruction`.

[An] A. N. Andrianov, *Quadratic Forms and Hecke Operators*, Grundlehren Math. Wiss. 286, Springer, 1987.

[Andr] G. E. Andrews, *The Theory of Partitions*, Encyclopedia Math. Appl. 2, Addison-Wesley, 1976.

[CL] G. Chenevier and J. Lannes, *Automorphic Forms and Even Unimodular Lattices*, Ergeb. Math. Grenzgeb. (3) 69, Springer, 2019.

[CoS] J. H. Conway and N. J. A. Sloane, *Sphere Packings, Lattices and Groups*, 3rd ed., Grundlehren Math. Wiss. 290, Springer, 1999.

[Ei52] M. Eichler, *Quadratische Formen und orthogonale Gruppen*, Grundlehren Math. Wiss. 63, Springer, 1952.

[Ei73] M. Eichler, *The basis problem for modular forms and the traces of the Hecke operators*, in *Modular Functions of One Variable I*, Lecture Notes in Math. 320, Springer, 1973, 75–151.

[GL] L. Sernau, *GRH for Dirichlet L-functions, in Lean 4*, a shorter rewriting of the Lean proof, text by Claude, `https://github.com/lsernau/grh-lean`, commit `72fead1`, readable edition `grh/`.

[Gr] B. H. Gross, *Heights and the special values of L-series*, in *Number Theory (Montreal, 1985)*, CMS Conf. Proc. 7, Amer. Math. Soc., 1987, 115–187.

[Iw] H. Iwaniec, *Topics in Classical Automorphic Forms*, Grad. Stud. Math. 17, Amer. Math. Soc., 1997.

[Kn] M. Kneser, *Klassenzahlen definiter quadratischer Formen*, Arch. Math. **8** (1957), 241–250.

[Pi] A. Pizer, *An algorithm for computing modular forms on* $\Gamma_0(N)$, J. Algebra **64** (1980), 340–390.

[Ra] S. Rallis, *Langlands' functoriality and the Weil representation*, Amer. J. Math. **104** (1982), 469–515.

[SeA] J.-P. Serre, *A Course in Arithmetic*, Grad. Texts in Math. 7, Springer, 1973.

DIVISIBILITY ALONG THE CHAIN

Prerequisites. Formal power series over a commutative ring. Finite extensions of $\mathbb{Q}_p$, their valuations, and lattices over their rings of integers; the length of a module of finite length. Gaussian binomial coefficients $\begin{bmatrix} n \\ l \end{bmatrix}_Q$ [Mac, Ch. I, §2, Example 3]. From Chapter 5, *Size against divisibility*: that a sublattice of small colength has small index, so that a gain on it is charged its colength. From Chapter 8, *The chain and the square root*: Section 8.4. From Chapter 18, *Hecke nondegeneracy on the tree*: the loss, defined in Section 18.1. From Chapter 24, *Hecke operators and theta lifts*: Section 24.5, in particular Problems 24.5.3 and 24.5.4. Section 25.6 says where the proof uses this transfer; the step in the generality of the proof is Theorem 53.4.1 of Chapter 53, and the rest of the chapter does not use it.

Problem 8.4.3 adds the divisibility exponents that hold on the whole lattice at each step of the chain. In the proof, Theorem 53.4.1 bounds the gauge of the restricted chain on the image of the integral source forms under a power of a product of Hecke operators. The local model in Chapter 18 measures the colength of the values of a Hecke operator at a single lattice. How does a gain on a sublattice at the start of a chain become a gain of the composite? In the model of Problem 24.5.4, moving the source operator through the chain introduces signed complete symmetric functions. Their valuations enter the bound in Section 25.4. The model below uses one Hecke operator. Theorem 53.4.1 uses a product indexed by a full mark above p.

25.1. Elementary and complete symmetric functions

Let $x = (x_1, \dots, x_n)$ be a finite family in a commutative ring. The *elementary* and *complete symmetric functions* $e_l(x)$ and $h_l(x)$ are the sums of the products $x_{i_1} \cdots x_{i_l}$ over $i_1 < \cdots < i_l$ and over $i_1 \le \cdots \le i_l$ respectively, with $e_0 = h_0 = 1$. Their generating series are

$$E_x(X) := \prod_i (1+x_iX) = \sum_{l \ge 0} e_l(x) X^l, \qquad H_x(X) := \prod_i (1-x_iX)^{-1} = \sum_{l \ge 0} h_l(x) X^l.$$

All degrees l are nonnegative integers, and $\begin{bmatrix} n \\ l \end{bmatrix}_Q = 0$ for $l > n$.

Problem 25.1.1. $E_x(X)H_x(-X) = 1$, that is, $\sum_{l=0}^{r} (-1)^l e_{r-l}(x)\, h_l(x) = 0$ for $r \ge 1$. For $x = (a, b)$, $h_2(x) = a^2 + ab + b^2$.

This is [Mac, Ch. I, (2.6)]. For families x and y write $x \sqcup y$ for the concatenated family.

Problem 25.1.2.

$$e_r(x \sqcup y) = \sum_{l=0}^{r} e_l(x)\, e_{r-l}(y), \qquad h_r(x \sqcup y) = \sum_{l=0}^{r} h_l(x)\, h_{r-l}(y).$$

The families that occur are geometric progressions.

Date: November 25, 2026.

Problem 25.1.3. For $t \geq 0$,

$$e_l(1, Q, \ldots, Q^t) = Q^{l(l-1)/2} \begin{bmatrix} t+1 \\ l \end{bmatrix}_Q, \qquad h_l(1, Q, \ldots, Q^t) = \begin{bmatrix} t+l \\ l \end{bmatrix}_Q.$$

For instance $h_2(1, Q) = 1 + Q + Q^2$.

These are [Mac, Ch. I, §2, Example 3]. Let q be invertible, $Q := q^2$, $g \geq 1$ and $t := g - 1$. A *block* is a family

$$x = \beta\,(q^t, q^{t-2}, \ldots, q^{-t}) \tag{1}$$

of g terms with ratio Q^{-1}, where β is invertible. For $\beta = 1$ this is the family in Problem 24.5.3, where q^t is written $Q^{t/2}$.

Problem 25.1.4. For the block (1), $e_l(x) = \beta^l q^{-l(g-l)} \begin{bmatrix} g \\ l \end{bmatrix}_Q$ and $h_l(x) = \beta^l q^{-lt} \begin{bmatrix} t+l \\ l \end{bmatrix}_Q$.

For $\beta = 1$ the first formula, in degrees $0 \leq l \leq g$, is Problem 24.5.3.

25.2. Valuations

Let k be a finite extension of $\mathbb{Q}_p$, with ring of integers $\mathcal{O}$ and valuation v normalized by $v(p) = 1$.

Problem 25.2.1. $\begin{bmatrix} n \\ l \end{bmatrix}_Q$ is a polynomial in Q with integer coefficients and constant term 1, for $0 \leq l \leq n$. Hence $v\big(\begin{bmatrix} n \\ l \end{bmatrix}_Q\big) = 0$ if $Q \in k$ and $v(Q) > 0$.

Problem 25.2.2. Let $a \in k^\times$ and $Q \in k^\times$ with $v(Q) = v_Q > 0$. Then

$$\begin{aligned} v\big(e_l(a, aQ, \ldots, aQ^t)\big) &= l\,v(a) + v_Q\,\frac{l(l-1)}{2} && (0 \leq l \leq t+1), \\ v\big(h_l(a, aQ, \ldots, aQ^t)\big) &= l\,v(a) && (l \geq 0). \end{aligned}$$

For $0 \leq l \leq t+1$, the difference $v(e_l) - v(h_l)$ for this family is $v_Q\,l(l-1)/2$.

Problem 25.2.3. Let x be the block (1) with $\beta, q \in k^\times$ and $v(q) = \nu > 0$. Then $v(h_l(x)) = l\,(v(\beta) - t\nu)$ for $l \geq 0$, and $v(e_l(x)) = l\,(v(\beta) - t\nu) + \nu\,l(l-1)$ for $0 \leq l \leq g$. In particular every $h_l(x)$ lies in $\mathcal{O}$ if and only if $v(\beta) \geq t\nu$.

For a union of blocks only a bound survives.

Problem 25.2.4. Let Z be a finite family in k whose least valuation is a real number μ. Then $v(h_l(Z)) \geq l\mu$, with equality if exactly one member of Z has valuation μ. For $Z = (1, 1)$ and $Z = (1, -1)$ one has $h_l(Z) = l + 1$ and $h_l(Z) = (1 + (-1)^l)/2$.

Problem 25.2.5. Let $Z = x_1 \sqcup x_2$, where $x_i = \beta_i\,(q, q^{-1})$ are blocks with $g = 2$, and let $v(q) = \nu > 0$ and $v(\beta_1) = v(\beta_2) = 0$. Then $h_1(Z) = (\beta_1 + \beta_2)(q + q^{-1})$, so $v(h_1(Z)) = v(\beta_1 + \beta_2) - \nu$, which exceeds $-\nu$ exactly when $\beta_1 \equiv -\beta_2$ modulo the maximal ideal of $\mathcal{O}$.

25.3. Moving a Hecke operator along a chain

We use the setting of Problem 24.5.4. Let $F_0, \dots, F_m$ be finite-dimensional k-vector spaces, let $K_j \colon F_j \to F_{j+1}$ be linear maps, and let $\mathcal{K}_j := K_{j-1} \cdots K_0$, with $\mathcal{K}_0 := 1$. Fix $r \geq 1$. For each j let $\mathcal{E}_0^{(j)} = 1, \mathcal{E}_1^{(j)}, \dots, \mathcal{E}_r^{(j)}$ be operators on F_j, and let $x_1, \dots, x_m$ be finite families in k with

$$\mathcal{E}_i^{(j+1)} K_j = K_j \sum_{l=0}^{i} e_l(x_{j+1})\, \mathcal{E}_{i-l}^{(j)} \qquad (0 \leq i \leq r,\ 0 \leq j < m). \tag{2}$$

This is the case with source argument X of the split relation in Section 24.5. Under the hypotheses of Theorem 53.4.1, statement (B) of Chapter 53 gives this relation for every translation in the support of the datum, at every prime of a mark, on forms spherical there, for $r \leq N_0$. The family at each step is a block (1). Let $Z_j := x_1 \sqcup \cdots \sqcup x_j$. In (2) the operators at the target are expressed through those at the source. We need the converse.

Problem 25.3.1. Let $r = 1$ and $m \geq 2$. Then $K_0 \mathcal{E}_1^{(0)} = \big(\mathcal{E}_1^{(1)} - e_1(x_1)\big) K_0$, and $\mathcal{K}_2 \mathcal{E}_1^{(0)} = \big(\mathcal{E}_1^{(2)} - h_1(Z_2)\big) \mathcal{K}_2$.

Problem 25.3.2. Let $r = 2$ and $m \geq 1$. Then $K_0 \mathcal{E}_2^{(0)} = \big(\mathcal{E}_2^{(1)} - h_1(x_1)\, \mathcal{E}_1^{(1)} + h_2(x_1)\big) K_0$.

Problem 25.3.3. $\mathcal{E}_i^{(j)}\, \mathcal{K}_j = \mathcal{K}_j \sum_{l=0}^{i} e_l(Z_j)\, \mathcal{E}_{i-l}^{(0)}$ for $0 \leq i \leq r$.

Problem 24.5.4, applied to the first j maps, gives the following identity.

Theorem 25.3.1. *For $1 \leq j \leq m$,* $\mathcal{K}_j\, \mathcal{E}_r^{(0)} = \displaystyle\sum_{l=0}^{r} (-1)^l h_l(Z_j)\, \mathcal{E}_{r-l}^{(j)}\, \mathcal{K}_j$.

The relation for one lift has the elementary functions of a block. For a block x with $v(q) = \nu > 0$ and $0 \leq l \leq g$, one has $v(e_l(x)) - v(h_l(x)) = \nu\, l(l-1)$ (Problem 25.2.3). The inverse relation has the complete functions, which may have denominators. For the lattice normalization in the next two problems assume $1 \leq r \leq N_0$, where N_0 is defined below. The operators $\mathcal{E}_i^{(j)}$ are normalized forms of the sums $T_i^{(j)}$ over edges of type i of Section 24.5: when F_j consists of functions of lattices in a space of dimension N_j, with $N_0 < N_1 < \cdots < N_m$, one takes $\mathcal{E}_i^{(j)} = q^{-i(N_j - i)}\, T_i^{(j)}$ for $0 \leq i \leq N_j$.

Problem 25.3.4. With this normalization, Theorem 25.3.1 reads

$$\sum_{l=0}^{r} (-1)^l h_l(Z_j)\, q^{l(N_j - 2r + l)}\, T_{r-l}^{(j)}\, \mathcal{K}_j = q^{r(N_j - N_0)}\, \mathcal{K}_j\, T_r^{(0)}.$$

Problem 25.3.5. Suppose that Z_j is a union of blocks (1) with the same t, that $v(q) > 0$, that $v(\beta) \geq 0$ for each block, and that $N_j \geq 2r + t - 1$. Then every coefficient $h_l(Z_j)\, q^{l(N_j - 2r + l)}$ in Problem 25.3.4 lies in $\mathcal{O}$.

25.4. A gain on a sublattice

For each j let $\mathrm{Int}_j \subset F_j$ be an $\mathcal{O}$-lattice of full rank. For $w \in F_j$ let $\mathrm{ord}(w)$ be the least valuation of a coordinate of w in a basis of Int_j, with $\mathrm{ord}(0) = \infty$; we use $v(0) = +\infty$ and $\min \varnothing = +\infty$. For a linear map $\phi \colon F_i \to F_j$ let $\mathrm{gain}(\phi)$ be the

least value of $\mathrm{ord}(\phi y)$ over the members y of a basis of Int_i. For $k = \mathbb{Q}_p$ and $\phi \neq 0$, $\mathrm{gain}(\phi)$ is the largest integer n with $\phi(\mathrm{Int}_i) \subseteq p^n \mathrm{Int}_j$; so $\mathrm{gain}(\phi) \log p$ plays at p the role of the divisibility $-h_{\mathrm{fin}}$ of Section 8.4.

Problem 25.4.1. ord and gain do not depend on the bases. $\mathrm{ord}(\phi w) \geq \mathrm{ord}(w) + \mathrm{gain}(\phi)$, $\mathrm{gain}(\phi\psi) \geq \mathrm{gain}(\phi) + \mathrm{gain}(\psi)$, $\mathrm{gain}(\phi + \psi) \geq \min(\mathrm{gain}(\phi), \mathrm{gain}(\psi))$, and $\mathrm{gain}(c\phi) = v(c) + \mathrm{gain}(\phi)$ for $c \in k^\times$.

Assume (2). For $1 \leq j \leq m$ and $0 \leq i \leq r$ let

$$\gamma_j(i) := \mathrm{gain}\big(\mathcal{E}_i^{(j)} K_{j-1}\big),$$

so that $\gamma_j(0) = \mathrm{gain}(K_{j-1})$ is the gain of the jth step on the whole lattice, and $\gamma_j(r)$ its gain after the Hecke operator $\mathcal{E}_r^{(j)}$ at the target. Let $c \in k^\times$ be such that $Y := c\,\mathcal{E}_r^{(0)}$ maps Int_0 into itself, and let $A := v(c)$. To bound $\mathrm{ord}(\mathcal{K}_j\, \mathcal{E}_r^{(0)} w)$ in terms of $\mathrm{ord}(\mathcal{K}_{j-1} w)$, define

$$\delta_j := \min_{0 \leq l \leq r} \big(v(h_l(Z_j)) + \gamma_j(r - l)\big).$$

When $\gamma_j(r) < +\infty$, the *price* of the jth step is $\mathrm{Pr}_j := \gamma_j(r) - \delta_j$. It is nonnegative.

Problem 25.4.2. For $w \in F_0$ and $1 \leq j \leq m$, $\mathrm{ord}\big(\mathcal{K}_j\, \mathcal{E}_r^{(0)} w\big) \geq \mathrm{ord}\big(\mathcal{K}_{j-1} w\big) + \delta_j$.

Problem 25.4.3. Let $S \subseteq \{1, \ldots, m\}$, and let n_j be the number of elements of S that are at most j. For $G \in \mathrm{Int}_0$ and $0 \leq j \leq m$,

$$\mathrm{ord}\big(\mathcal{K}_j\, Y^{n_j} G\big) \geq \sum_{1 \leq i \leq j,\ i \in S} \big(A + \delta_i\big) + \sum_{1 \leq i \leq j,\ i \notin S} \gamma_i(0).$$

Theorem 25.4.1. *For every $F \in \mathrm{Int}_0$,*

$$\mathrm{ord}\big(\mathcal{K}_m\, Y^m F\big) \geq \sum_{j=1}^{m} \max\big(\gamma_j(0),\ A + \delta_j\big).$$

The gain holds on the image $Y^m \mathrm{Int}_0$. When Y is injective this is a sublattice of full rank, and in Chapter 5 the gain on such a sublattice is charged its colength. In the proof one copy of the product $Y_{\mathfrak{M}}$ of Hecke operators of a full mark (Section 25.6) goes into the datum of every lift, and the transfer is cleared by a power of p fixed in advance (Problem 53.4.2).

Problem 25.4.4. If Y is injective, then the length of $\mathrm{Int}_0 / Y^m \mathrm{Int}_0$ is m times the length of $\mathrm{Int}_0 / Y\, \mathrm{Int}_0$.

In the tree model of Chapter 18, as F ranges over all integral forms the values $(YF)(L)$ fill $S(L)$, and the loss at L is the length of $H(L)/S(L)$. The proof does not assume that Y is injective; the colength bound it uses is in Chapter 48, Section 48.4.

25.5. Stepwise maxima overcount

Theorem 25.4.1 uses δ_j at step j. Can one replace its lower bound for $\mathrm{gain}(\mathcal{K}_m Y^m)$ by $\sum_{j=1}^m \max(\gamma_j(0), A + \gamma_j(r))$? We compare two chains with the same numbers $\gamma_j(i)$. Let p be any prime, $k = \mathbb{Q}_p$, $m = 2$, $r = 1$, $F_j = \mathbb{Q}_p^2$ and $\mathrm{Int}_j = \mathbb{Z}_p^2$. Let $K_0 = K_1 = K$ be a diagonal matrix, let $x_1 = (\alpha_1)$ and $x_2 = (\alpha_2)$ be families of one element, and let

$$Y := \mathcal{E}_1^{(0)} := \mathrm{diag}(p, 1), \qquad \mathcal{E}_1^{(j)} := Y + h_1(Z_j) \quad (j = 1, 2),$$

so that $A = 0$.

Problem 25.5.1. These data satisfy (2), and length $\mathbb{Z}_p^2/Y\mathbb{Z}_p^2 = 1$.

Problem 25.5.2. Let $K = \mathrm{diag}(1, p)$ and $\alpha_1 = \alpha_2 = p$. Then $\gamma_j(0) = 0$, $\gamma_j(1) = 1$ and $\Pr_j = 0$ for $j = 1, 2$, and $\mathrm{gain}(\mathcal{K}_2\, Y^2) = 2$.

Problem 25.5.3. Let $K = \mathrm{diag}(p, 1)$, $\alpha_1 = p - 1$ and $\alpha_2 = -2p$. Then $\gamma_j(0) = 0$, $\gamma_j(1) = 1$ and $\Pr_j = 1$ for $j = 1, 2$, and $\mathrm{gain}(\mathcal{K}_2\, Y^2) = 0$.

The sum of the stepwise maxima is 2 in both chains. Theorem 25.4.1 gives the exact gain in each case.

Theorem 25.4.1 uses the gains $\gamma_j(i)$, the scaling valuation A, and the coefficients $h_l(Z_j)$. Chapters 15 and 16 model divisibility for a single theta kernel. If Z_j has finite least valuation μ_j, then $v(h_l(Z_j)) \geq l\mu_j$ (Problem 25.2.4). A separate colength estimate enters when the gain on the image is used; Chapter 18 computes a local colength at one lattice.

Exercises.

(1) The Newton polygon of $\prod_{i=0}^{t}(1 + aQ^iX)$ over k, with $a \in k^\times$, $Q \in k^\times$ and $v(Q) > 0$, has the vertices $\big(l, l\,v(a) + v(Q)\,l(l-1)/2\big)$ for $0 \leq l \leq t+1$.

(2) Suppose that (2) holds with $u_{j+1}^i K_j$ in place of K_j on the right, for units $u_j \in \mathcal{O}^\times$. Write $E_j(X) := \sum_{i=0}^{r} \mathcal{E}_i^{(j)} X^i$. Show first that the relation is equivalent modulo X^{r+1} to $E_{j+1}(X)K_j = K_j E_{x_{j+1}}(u_{j+1}X)E_j(u_{j+1}X)$, the relation of Section 24.5 with $P(X) = E_{u_{j+1}x_{j+1}}(X)$. Then Theorem 25.3.1 holds with $\mathcal{K}_j\mathcal{E}_r^{(0)}$ multiplied by $(u_1 \cdots u_j)^r$, and with Z_j replaced by the family Z_j' of the $u_l u_{l+1} \cdots u_j\, a$ for $l \leq j$ and a in x_l. Theorem 25.4.1 holds with δ_j computed from Z_j'. For the same gains $\gamma_j(i)$, the two values of δ_j agree when Z_j has exactly one member of least valuation. For $r = 1$, p odd, $x_1 = (1)$, $x_2 = (-1)$, $u_1 = -1$, $u_2 = 1$ and $\gamma_2(1) > \gamma_2(0)$, the two values of δ_2 differ.

25.6. The step in the proof

At an exceptional prime $p < x_1$ the proof [GL] applies this transfer to the Hecke operators of a full mark and to the chain of m lifts, and obtains Theorem 53.4.1; Chapter 53 states and develops it, and Chapter 48, Section 48.4, uses it. There the relation (2) appears for the lift $X_j \to X_{j+1}$ with one polynomial for all translations, in degrees $i \leq r_p$, with a block $\chi(q^t, q^{t-2}, \ldots, q^{-t})$ in place of x_{j+1}, χ a p-adic unit (this comparison is ours); the proof inverts that polynomial over the ring $\mathcal{O}_\eta$ of Chapter 34 and puts one copy of the product of Hecke operators into the datum of every lift, as in the choice $S = \{1, \ldots, m\}$ of Problem 25.4.3.

Hints

§25.1.

25.1.1: Compare the product formulas.

25.1.2: $E_{x \sqcup y} = E_x E_y$.

25.1.3: Induction on t and l together, using $\begin{bmatrix} n \\ 0 \end{bmatrix}_Q = 1$ at the boundary and, for $1 \leq l \leq n$, the rule $\begin{bmatrix} n \\ l \end{bmatrix}_Q = \begin{bmatrix} n-1 \\ l-1 \end{bmatrix}_Q + Q^l \begin{bmatrix} n-1 \\ l \end{bmatrix}_Q$ and its companion $\begin{bmatrix} n \\ l \end{bmatrix}_Q = Q^{n-l} \begin{bmatrix} n-1 \\ l-1 \end{bmatrix}_Q + \begin{bmatrix} n-1 \\ l \end{bmatrix}_Q$.

25.1.4: Problem 25.1.3 for the family $\beta q^{-t}(1, Q, \ldots, Q^t)$; e_l and h_l are homogeneous of degree l.

§25.2.

25.2.1: The first rule in the hint to Problem 25.1.3.
25.2.2: Problems 25.1.3 and 25.2.1.
25.2.3: Problems 25.1.4 and 25.2.1.
25.2.4: Which monomial of degree l has the least valuation?
25.2.5: Problem 25.1.2.

§25.3.

25.3.1: Apply (2) with $i = 1$ once for each step.
25.3.2: Use (2) with $i = 1$ to remove $K_0\mathcal{E}_1^{(0)}$, then Problem 25.1.1.
25.3.3: Write (2) as an identity of polynomials in X modulo X^{r+1}, as in the hint to Problem 24.5.4, and use Problem 25.1.2.
25.3.4: Multiply Theorem 25.3.1 by $q^{r(N_j-r)}$.
25.3.5: Problems 25.2.3 and 25.2.4; look at $l = 1$.

§25.4.

25.4.1: Write w in coordinates.
25.4.2: Apply Theorem 25.3.1 to w, write $\mathcal{K}_j = K_{j-1}\mathcal{K}_{j-1}$, and use Problem 25.4.1.
25.4.3: Induction on j. For $j \in S$ write $Y^{n_j} = c\,\mathcal{E}_r^{(0)}\,Y^{n_{j-1}}$ and use Problem 25.4.2. For Theorem 25.4.1, compare $A + \delta_j$ with $\gamma_j(0)$ when choosing S, and apply the problem to $Y^{m-n_m}F$.
25.4.4: $Y^i\mathrm{Int}_0/Y^{i+1}\mathrm{Int}_0 \cong \mathrm{Int}_0/Y\,\mathrm{Int}_0$.

§25.5.

25.5.1: Diagonal matrices commute.
25.5.2: Compute $\mathcal{K}_2\,Y^2$.
25.5.3: Compute $\mathcal{E}_1^{(1)}$ and $\mathcal{E}_1^{(2)}$ first.

References

[Mac] I. G. Macdonald, *Symmetric Functions and Hall Polynomials*, 2nd ed., Oxford Math. Monogr., Clarendon Press, Oxford, 1995.

[GL] L. Sernau, *GRH for Dirichlet L-functions, in Lean 4*, a shorter rewriting of the Lean proof, text by Claude, `https://github.com/lsernau/grh-lean`, commit `72fead1`, readable edition `grh/`.

DENOMINATORS AND THE STICKELBERGER ELEMENT

Prerequisites. Ideal class groups [Ne, Ch. I, §§3, 6] and the norm of ideals in an extension of number fields. Cyclotomic fields, Bernoulli numbers and generalized Bernoulli numbers [Wa, Ch. 4–6]. Euclidean lattices, their covolumes and the indices of sublattices, as in Chapter 5, *Size against divisibility*. Chapter 27, *Odd Tate twists*, continues this one.

26.1. Denominators of linear maps

A linear map between $\mathbb{Q}$-vector spaces with integral structures need not respect them. What does that cost when size is compared with divisibility, and how can it be reduced? The simplest example is differentiation. Let Int be the set of polynomials $f \in \mathbb{Q}[x]$ with $f(\mathbb{Z}) \subseteq \mathbb{Z}$, and for an integer $n \geq 0$ let Int_n be its elements of degree at most n.

Problem 26.1.1. The binomial polynomials $\binom{x}{k}$, $0 \leq k \leq n$, form a $\mathbb{Z}$-basis of Int_n.

Problem 26.1.2. Let $D = d/dx$. Then

$$D\binom{x}{n} = \sum_{k=1}^{n} \frac{(-1)^{k-1}}{k} \binom{x}{n-k}.$$

Hence the least positive integer c with $c\,D(\mathrm{Int}_n) \subseteq \mathrm{Int}$ is $\mathrm{lcm}(1, 2, \ldots, n)$, with the empty least common multiple equal to 1.

The logarithm of this denominator is $\sum_{p^a \leq n} \log p$, of the size of n. The announcement [Alp, item 14] records a "need for division". Chapter 29, *Congruence modules*, models the denominator of a projection of a whole lattice by a congruence module.

An integral structure can be built one prime at a time. For a lattice $L \subset \mathbb{Q}^r$ and a prime p, write $L_p := L \otimes \mathbb{Z}_p \subset \mathbb{Q}_p^r$.

Problem 26.1.3. For every family $(\Lambda_p)_p$ of $\mathbb{Z}_p$-lattices $\Lambda_p \subset \mathbb{Q}_p^r$ with $\Lambda_p = \mathbb{Z}_p^r$ for all but finitely many p, there is exactly one lattice $L \subset \mathbb{Q}^r$ with $L_p = \Lambda_p$ for every p, namely $L = \bigcap_p (\Lambda_p \cap \mathbb{Q}^r)$. If $\Lambda_2 = \frac{1}{2}\mathbb{Z}_2 \oplus \mathbb{Z}_2$, $\Lambda_3 = \mathbb{Z}_3 \oplus \frac{1}{3}\mathbb{Z}_3$, and $\Lambda_p = \mathbb{Z}_p^2$ otherwise, then $L = \frac{1}{2}\mathbb{Z} \oplus \frac{1}{3}\mathbb{Z}$.

For a finitely generated torsion $\mathbb{Z}_p$-module T let $\mathrm{len}_{\mathbb{Z}_p} T$ be its length.

Problem 26.1.4. If T is a finite abelian group, then $\log|T| = \sum_p \mathrm{len}_{\mathbb{Z}_p}(T \otimes \mathbb{Z}_p) \log p$. If $M' \subseteq M$ are lattices of the same rank, then $\log[M : M'] = \sum_p \mathrm{len}_{\mathbb{Z}_p}(M_p/M'_p) \log p$.

Let L and M be Euclidean lattices and $T\colon L_{\mathbb{Q}} \to M_{\mathbb{Q}}$ an injective linear map. If $T(L) \not\subseteq M$, one may replace M by the lattice $M + T(L)$, with the same norm.

Date: November 25, 2026.

Problem 26.1.5. Suppose that L and M have the same rank. Then $\operatorname{covol}(M + T(L)) = \operatorname{covol}(M)/[M + T(L) : M]$, and

$$\operatorname{covol}(M) \le [M + T(L) : M]\,|\det T|\,\operatorname{covol}(L),$$

where $\det T$ is taken in orthonormal bases of $L \otimes \mathbb{R}$ and $M \otimes \mathbb{R}$.

The logarithmic cost of a denominator is $\log[(M + T(L)) : M]$. Suppose that several maps $T_1, \dots, T_k$ serve equally well, for instance because they have the same period. How small an index can one obtain by choosing a lattice separately at each prime? A map taking L into the resulting lattice must still be found. The Stickelberger example below uses combinations of twists on individual character components.

Problem 26.1.6. Let $M_j := M + T_j(L)$, and let M^* be the lattice with $M^*_p = (M_j)_p$ for a $j = j(p)$ that minimizes $\operatorname{len}_{\mathbb{Z}_p}\big((M_j)_p/M_p\big)$. Then $M^* \supseteq M$ and

$$\log[M^* : M] = \sum_p \min_j \operatorname{len}_{\mathbb{Z}_p}\big((M_j)_p/M_p\big)\log p.$$

If $M = \mathbb{Z}$ and $M_j = D_j^{-1}\mathbb{Z}$ with positive integers D_j, then $[M^* : M] = \gcd(D_1, \dots, D_k)$. For $D_j = 6, 10, 15$ each map alone costs at least $\log 6$, and together they cost nothing.

The announcement [Alp, item 15] describes gluing an integral structure across Hecke characters to obtain a gcd; Problem 26.1.6 gives a lattice model for this. It also mentions Galois cohomology classes "that we couldn't kill by twisting" [Alp, item 17]. This chapter serves the denominator step of the proof; the corresponding statements are named in the remark below, and the odd classes are treated in Chapter 27 and Chapter 28, *Odd classes by Gauss sums*. In the cyclotomic example below, integral twists of the Stickelberger element annihilate the class group, and their eigenvalues on the odd characters illustrate the connection with class groups. In the Lean formalization. Paths are relative to `grh/src/` of the Lean proof [GL]. The corresponding statements are as follows. The predicates `New.Data.ClearsProjection`, `New.Data.HasDenominatorsLe` and `New.Data.IsDenominatorBound` are in `New/Determinant/Twist/FitTwists.lean`. The length bound `New.exists_length_shaOdd_le` is in `Lib/Cyclotomic/OddSha.lean`. The module of Definition 27.3.1 is a special case of `New.Selmer.shaOdd` in `Lib/GaloisRep/Main/SelmerModules.lean`. The definitions `New.Selmer.oddClassBound` and `New.Selmer.denominatorError` are in `New/Congruences/FirstOrder/TraceRelations.lean`.

26.2. The Stickelberger element

Let p be an odd prime, $F := \mathbb{Q}(\zeta_p)$, $G := \operatorname{Gal}(F/\mathbb{Q})$, and let $\sigma_a \in G$ be the automorphism with $\sigma_a(\zeta_p) = \zeta_p^a$. Let A be the p-primary part of $\mathrm{Cl}(F)$, a $\mathbb{Z}_p[G]$-module. Let $\omega\colon (\mathbb{Z}/p\mathbb{Z})^\times \to \mathbb{Z}_p^\times$ be the Teichmüller character, with $\omega(a) \equiv a \pmod p$, and view it as a character of G. For $i \in \mathbb{Z}/(p-1)\mathbb{Z}$ let $A^{(i)} := \{z \in A : \sigma_a z = \omega(a)^i z \text{ for all } a\}$, and

$$\varepsilon_i := \frac{1}{p-1}\sum_{a=1}^{p-1} \omega(a)^i \sigma_a^{-1} \in \mathbb{Z}_p[G].$$

Problem 26.2.1. The ε_i are orthogonal idempotents with sum 1, $\sigma_a\varepsilon_i = \omega(a)^i\varepsilon_i$, and $A = \bigoplus_i \varepsilon_i A = \bigoplus_i A^{(i)}$. Complex conjugation σ_{-1} acts on $A^{(i)}$ by $(-1)^i$.

Write A^+ and A^- for the sums of the $A^{(i)}$ with i even and with i odd.

Problem 26.2.2. If $K \subseteq F$, then extension of ideals identifies the p-primary part of $\mathrm{Cl}(K)$ with $A^{\mathrm{Gal}(F/K)}$. Hence $A^{(0)} = 0$, A^+ is the p-primary part of the class group of $F^+ := \mathbb{Q}(\zeta_p + \zeta_p^{-1})$, and if $p \equiv 1 \pmod 4$, then $A^{((p-1)/2)}$ is the p-primary part of $\mathrm{Cl}(\mathbb{Q}(\sqrt{p}))$.

The *Stickelberger element* is

$$\theta := \frac{1}{p} \sum_{a=1}^{p-1} a\, \sigma_a^{-1} \in \mathbb{Q}[G],$$

with the denominator p. We use Stickelberger's theorem as a black box [Wa, Thm. 6.10].

Theorem 26.2.1 (Stickelberger)**.** *If $\beta \in \mathbb{Z}[G]$ and $\beta\theta \in \mathbb{Z}[G]$, then $\beta\theta$ annihilates $\mathrm{Cl}(F)$.*

We shall use the following integral multiples of θ, indexed by integers c prime to p.

Problem 26.2.3. For c prime to p, $(c - \sigma_c)\theta = \sum_{b=1}^{p-1} \lfloor cb/p \rfloor\, \sigma_b^{-1}$. In particular $(c - \sigma_c)\theta \in \mathbb{Z}[G]$.

For a nontrivial Dirichlet character χ modulo p let $B_{1,\chi} := \frac{1}{p} \sum_{a=1}^{p-1} \chi(a)\, a$.

Problem 26.2.4. $\varepsilon_i \theta = B_{1,\omega^{-i}} \varepsilon_i$ for $i \not\equiv 0$. If $i \not\equiv 0$ is even, then $B_{1,\omega^{-i}} = 0$.

So θ says nothing about A^+. For $i \not\equiv 0 \pmod{p-1}$, the twist $(c - \sigma_c)\theta$ acts on $A^{(i)}$ as $(c - \omega(c)^i) B_{1,\omega^{-i}}$, and the gluing of Problem 26.1.6 asks for the ideal generated by the factors $c - \omega(c)^i$.

Problem 26.2.5. The ideal of $\mathbb{Z}_p$ generated by the numbers $c - \omega(c)^i$, c prime to p, is $\mathbb{Z}_p$ if $i \not\equiv 1$ and $p\mathbb{Z}_p$ if $i \equiv 1$. Moreover $v_p(B_{1,\omega^{-1}}) = -1$.

For $i \not\equiv 0, 1 \pmod{p-1}$, the eigenvalues of the integral twists generate $B_{1,\omega^{-i}} \mathbb{Z}_p$, so a $\mathbb{Z}_p$-linear combination recovers the eigenvalue of θ. For $i \equiv 1 \pmod{p-1}$ the twist eigenvalues generate $\mathbb{Z}_p$, whereas $B_{1,\omega^{-1}}$ has denominator p. This p is the order of μ_p, on which G acts by ω. In particular $A^{(1)} = 0$ [Wa, Prop. 6.16]. By Kummer's congruences [Wa, Ch. 5], if i is odd and $3 \le i \le p-2$, then

$$B_{1,\omega^{-i}} \equiv \frac{B_{p-i}}{p-i} \pmod p. \tag{1}$$

Problem 26.2.6. For $p = 7$ the character ω^{-3} is the Legendre symbol, $B_{1,\omega^{-3}} = -1$, and $B_4/4 = -1/120 \equiv -1 \pmod 7$.

Problem 26.2.7. Let i be odd with $3 \le i \le p-2$. If $p \nmid B_{p-i}$, then $A^{(i)} = 0$.

This is Herbrand's theorem [Wa, Thm. 6.17]. Its converse is due to Ribet [Ri], and the exact order to Mazur and Wiles [MW]; see [Wa, Ch. 15]. We use them as a black box.

Theorem 26.2.2 (Herbrand, Ribet, Mazur–Wiles)**.** *Let i be odd with $3 \le i \le p-2$. Then $A^{(i)} \ne 0$ if and only if $p \mid B_{p-i}$, and $|A^{(i)}| = |B_{1,\omega^{-i}}|_p^{-1}$.*

Problem 26.2.8. For $p < 100$, the pairs (p, k) with k even, $2 \le k \le p-3$ and $p \mid B_k$ are $(37, 32)$, $(59, 44)$ and $(67, 58)$. Hence for $p < 100$ the group A^- is nonzero only for $p = 37, 59, 67$, and then exactly one odd eigenspace is nonzero, $A^{(5)}$, $A^{(15)}$ and $A^{(9)}$ respectively.

The plus part A^+ is not seen by θ (Problem 26.2.4). Its order is the p-part of an index of cyclotomic units in the units of F^+ [Wa, Thm. 8.2]. Vandiver's conjecture, that $A^+ = 0$ for every p, has not been proved; it has been verified for $p < 2^{31}$ [HHO]. The next chapter meets the same division between minus and plus parts in Galois cohomology; for $e > 0$ the modules of Definition 27.3.1 carry an oddness condition under complex conjugation.

Hints

§26.1.

26.1.1: Use the difference operator $\Delta f(x) := f(x+1) - f(x)$. It kills constants and satisfies $\Delta\binom{x}{k} = \binom{x}{k-1}$ for $k \ge 1$.

26.1.2: Formally $D = \log(1 + \Delta)$. For the sharpness, use the uniqueness in Problem 26.1.1.

26.1.3: Choose an integer N with $N\mathbb{Z}_p^r \subseteq \Lambda_p \subseteq N^{-1}\mathbb{Z}_p^r$ for all p, and work in $N^{-1}\mathbb{Z}^r/N\mathbb{Z}^r$.

26.1.4: The p-primary part of T is $T \otimes \mathbb{Z}_p$.

26.1.5: M and $T(L)$ are sublattices of finite index of $M + T(L)$.

26.1.6: Apply Problem 26.1.4 to M^*/M.

§26.2.

26.2.1: Orthogonality of the characters ω^i of the cyclic group G, whose order is prime to p.

26.2.2: Compose extension of ideal classes with the norm, in both orders; $[F : K]$ is prime to p. For the last claim, find the subfield fixed by the squares in G.

26.2.4: Use $\sigma_a^{-1}\varepsilon_i = \omega(a)^{-i}\varepsilon_i$. For even χ, pair a with $p - a$.

26.2.5: Reduce $c - \omega(c)^i$ modulo p. For $B_{1,\omega^{-1}}$, reduce $pB_{1,\omega^{-1}}$ modulo p.

26.2.7: Apply Theorem 26.2.1 to $\beta = c - \sigma_c$, project with ε_i, choose c by Problem 26.2.5, and use (1).

26.2.8: The first part is a finite computation. For the second use Theorem 26.2.2 with $k = p - i$, and $A^{(1)} = 0$ [Wa, Prop. 6.16].

References

[Alp] L. Alpöge, untitled note announcing a proof of the Riemann hypothesis, 20 November 2026, `https://alpo.ge/remark.pdf`.

[GL] L. Sernau, *GRH for Dirichlet L-functions, in Lean 4*, a shorter rewriting of the Lean proof, text by Claude, `https://github.com/lsernau/grh-lean`, commit `72fead1`, readable edition `grh/`.

[HHO] W. Hart, D. Harvey and W. Ong, *Irregular primes to two billion*, Math. Comp. **86** (2017), 3031–3049.

[MW] B. Mazur and A. Wiles, *Class fields of abelian extensions of* $\mathbf{Q}$, Invent. Math. **76** (1984), 179–330.

[Ne] J. Neukirch, *Algebraic Number Theory*, Grundlehren Math. Wiss. 322, Springer, 1999.

[Ri] K. A. Ribet, *A modular construction of unramified p-extensions of* $\mathbf{Q}(\mu_p)$, Invent. Math. **34** (1976), 151–162.

[Wa] L. C. Washington, *Introduction to Cyclotomic Fields*, 2nd ed., Grad. Texts in Math. 83, Springer, 1997.

ODD TATE TWISTS

Prerequisites. This chapter continues Chapter 26, *Denominators and the Stickelberger element*, whose notation A, $A^{(i)}$, $A^{\pm}$, ω, σ_a (Section 26.2, with $p = \ell$), Theorem 26.2.2 and Problem 26.2.8 we use. Continuous cohomology of profinite groups [NSW, Ch. I; Ch. II, §7], inflation–restriction, and the vanishing of $H^q(G, M)$, $q \geq 1$, for finite G of order invertible on M [SeL, Ch. VII–VIII]. Decomposition and inertia groups [Ne, Ch. I, §9], and the Artin isomorphism between the ideal class group of a number field and the Galois group of its Hilbert class field [Ne, Ch. VI, §6]. The duality theorems for Galois cohomology of number fields are stated in the text with references. In Sections 27.1 and 27.2, ℓ is an odd prime; $\mathrm{num}(r)$ is the numerator of a rational number r in lowest terms.

27.1. Tate twists over $\mathbb{Q}$

In the previous chapter Bernoulli values gave the orders of odd eigenspaces of a class group. Which Galois cohomology groups account for the numerators and denominators of zeta values? Let $\mathbb{Q}_S$ be the largest extension of $\mathbb{Q}$ unramified outside ℓ and ∞, $G_{\mathbb{Q},\ell} := \mathrm{Gal}(\mathbb{Q}_S/\mathbb{Q})$, and $\chi_\ell\colon \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathbb{Z}_\ell^\times$ the cyclotomic character, which factors through $G_{\mathbb{Q},\ell}$. For $k \in \mathbb{Z}$, $\mathbb{Z}_\ell(k)$ is $\mathbb{Z}_\ell$ with σ acting by $\chi_\ell(\sigma)^k$, and similarly for $\mathbb{Q}_\ell(k)$, $\mathbb{Q}_\ell/\mathbb{Z}_\ell(k)$ and $\mathbb{Z}/\ell(k)$. Let $W_e := \mathbb{Q}_\ell/\mathbb{Z}_\ell(-e)$, and let $G_\ell := \mathrm{Gal}(\overline{\mathbb{Q}}_\ell/\mathbb{Q}_\ell)$, mapped to $G_{\mathbb{Q},\ell}$ by restriction along a fixed embedding $\overline{\mathbb{Q}} \to \overline{\mathbb{Q}}_\ell$.

Definition. The *Tate–Shafarevich group of the twist* e is

$$\mathrm{Sha}_\ell(\mathbb{Q}, e) := \ker\big(H^1(G_{\mathbb{Q},\ell}, W_e) \to H^1(G_\ell, W_e)\big),$$

and $h_{\ell,e}(\mathbb{Q}) \in \{0, 1, 2, \ldots, \infty\}$ is its length as a $\mathbb{Z}_\ell$-module. For a number field E one defines $\mathrm{Sha}_\ell(E, e)$ and $h_{\ell,e}(E)$ in the same way, with the local Galois groups at all primes of E above ℓ.

Problem 27.1.1. If $(\ell - 1) \nmid k$, then $H^0(G_{\mathbb{Q},\ell}, \mathbb{Q}_\ell/\mathbb{Z}_\ell(k)) = 0$. If $(\ell - 1) \mid k$ and $k \neq 0$, it is cyclic of order $\ell^{1+v_\ell(k)}$. The same holds for G_ℓ in place of $G_{\mathbb{Q},\ell}$.

By von Staudt and Clausen [Wa, Thm. 5.10], the denominator of B_k, $k \geq 2$ even, is the product of the primes p with $(p - 1) \mid k$.

Problem 27.1.2. For even $k \geq 2$, the power of ℓ in the denominator of $\zeta(1-k) = -B_k/k$ is $|H^0(G_{\mathbb{Q},\ell}, \mathbb{Q}_\ell/\mathbb{Z}_\ell(k))|$.

For even $k \geq 2$, the ℓ-part of the denominator of $\zeta(1 - k)$ is the order of $H^0(G_{\mathbb{Q},\ell}, \mathbb{Q}_\ell/\mathbb{Z}_\ell(k))$. The ℓ-part of its numerator will be the order of $\mathrm{Sha}_\ell(\mathbb{Q}, k-1)$.

Problem 27.1.3. Let $p \neq \ell$, $e \neq 0$, and $G_p := \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$. Every unramified class in $H^1(G_p, W_e)$ is zero. Hence $\mathrm{Sha}_\ell(\mathbb{Q}, e)$ is the group of classes in $H^1(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}), W_e)$ that vanish at every prime.

Let $F := \mathbb{Q}(\zeta_\ell)$.

Date: November 26, 2026.

Problem 27.1.4. Suppose that $(\ell-1) \nmid e$. Then $H^1(G_{\mathbb{Q},\ell}, \mathbb{Z}/\ell(-e)) \to H^1(G_{\mathbb{Q},\ell}, W_e)[\ell]$ is an isomorphism, and so is its analogue for G_ℓ. Hence $\mathrm{Sha}_\ell(\mathbb{Q}, e)[\ell]$ is the group of classes in $H^1(G_{\mathbb{Q},\ell}, \mathbb{Z}/\ell(-e))$ that vanish on G_ℓ.

Problem 27.1.5. Suppose that $(\ell-1) \nmid e$. Restriction to $\mathrm{Gal}(\mathbb{Q}_S/F)$, followed by the Artin map, identifies the group of Problem 27.1.4 with the group of homomorphisms $\phi\colon A \to \mathbb{F}_\ell$ such that $\phi(\sigma_a z) = \omega(a)^{-e}\phi(z)$, that is, with $\mathrm{Hom}(A^{(-e)}, \mathbb{F}_\ell)$.

Problems 27.1.4 and 27.1.5 prove the following.

Theorem 27.1.1. *Let* $(\ell-1) \nmid e$. *Then* $\mathrm{Sha}_\ell(\mathbb{Q}, e)[\ell] \cong \mathrm{Hom}(A^{(-e)}, \mathbb{F}_\ell)$. *In particular* $\mathrm{Sha}_\ell(\mathbb{Q}, e) = 0$ *if and only if* $A^{(-e)} = 0$.

Problem 27.1.6. Let $e \geq 1$ be odd. Then $\mathrm{Sha}_\ell(\mathbb{Q}, e) \neq 0$ if and only if $\ell \mid \mathrm{num}(B_{e+1}/(e+1))$. For example, $\mathrm{Sha}_{691}(\mathbb{Q}, 11) \neq 0$ and $\mathrm{Sha}_{37}(\mathbb{Q}, 31) \neq 0$.

We state four inputs as black boxes. By Soulé [So], $H^2(G_{\mathbb{Q},\ell}, \mathbb{Z}_\ell(k))$ is finite for $k \geq 2$. By Poitou–Tate duality [NSW, Ch. VIII, §6], $\mathrm{Sha}_\ell(\mathbb{Q}, e)$ is dual to the kernel of $H^2(G_{\mathbb{Q},\ell}, \mathbb{Z}_\ell(e+1)) \to H^2(G_\ell, \mathbb{Z}_\ell(e+1))$, and by local duality [NSW, Ch. VII, §2] $H^2(G_\ell, \mathbb{Z}_\ell(k))$ is dual to $H^0(G_\ell, \mathbb{Q}_\ell/\mathbb{Z}_\ell(1-k))$. By Tate's global Euler characteristic formula [NSW, Ch. VIII, §7], for every finite $G_{\mathbb{Q},\ell}$-module M of ℓ-power order, $|H^0(M)||H^2(M)|/|H^1(M)| = |M^{c=1}|/|M|$, where c is a complex conjugation. Since ℓ is odd, $G_{\mathbb{Q},\ell}$ has ℓ-cohomological dimension at most 2 [NSW, Ch. VIII, §3], so $H^3(G_{\mathbb{Q},\ell}, M) = 0$ for every ℓ-primary M.

Problem 27.1.7. Let $e \geq 1$ be odd. Then $H^2(G_\ell, \mathbb{Z}_\ell(e+1)) = 0$, and $\mathrm{Sha}_\ell(\mathbb{Q}, e)$ is dual to $H^2(G_{\mathbb{Q},\ell}, \mathbb{Z}_\ell(e+1))$.

Problem 27.1.8. Let $k \geq 2$. The $\mathbb{Z}_\ell$-module $H^1(G_{\mathbb{Q},\ell}, \mathbb{Z}_\ell(k))$ has rank 1 if k is odd and rank 0 if k is even, and its torsion subgroup is isomorphic to $H^0(G_{\mathbb{Q},\ell}, \mathbb{Q}_\ell/\mathbb{Z}_\ell(k))$.

The main conjecture of Iwasawa theory, proved by Mazur and Wiles [MW], gives the order; see [Wa, Ch. 15].

Theorem 27.1.2 (Mazur–Wiles)**.** *Let* $e \geq 1$ *be odd. Then*

$$h_{\ell,e}(\mathbb{Q}) = v_\ell\big(\mathrm{num}(B_{e+1}/(e+1))\big).$$

Problem 27.1.9. Let $k \geq 2$ be even. Then

$$\frac{|H^2(G_{\mathbb{Q},\ell}, \mathbb{Z}_\ell(k))|}{|H^1(G_{\mathbb{Q},\ell}, \mathbb{Z}_\ell(k))|} = |\zeta(1-k)|_\ell^{-1}.$$

For $k = 12$ and $\ell = 691$ both sides are 691.

This is the simplest case of the Bloch–Kato conjecture [BK].

27.2. Odd characters

Over $\mathbb{Q}$ the odd twists are controlled by Bernoulli numbers. How does this look over an abelian field, and what does it say about sums over all ℓ?

Let $E \subseteq \mathbb{Q}(\zeta_\ell)$ and $\Delta_E := \mathrm{Gal}(E/\mathbb{Q})$. Then Δ_E acts on $\mathrm{Sha}_\ell(E, e)$, by $(\delta z)(g) := \tilde{\delta}\, z(\tilde{\delta}^{-1} g \tilde{\delta})$ for a lift $\tilde{\delta}$ of δ, which is the direct sum of its η-parts over the characters η of Δ_E, with values in $\mu_{\ell-1} \subset \mathbb{Z}_\ell^\times$. Let $\mathrm{Sha}_\ell(\mathbb{Q}, e; \eta)$ be defined as $\mathrm{Sha}_\ell(\mathbb{Q}, e)$, with W_e replaced by $W_e \otimes \eta^{-1}$. A character η is *critical for* e if $\eta(-1) = (-1)^{e+1}$, and *plus for* e otherwise. The *minus part* of $\mathrm{Sha}_\ell(E, e)$ is the sum of the η-parts over the critical characters; it is the part on which complex conjugation acts by $(-1)^{e+1}$.

Problem 27.2.1. The η-part of $\mathrm{Sha}_\ell(E,e)$ is isomorphic to $\mathrm{Sha}_\ell(\mathbb{Q},e;\eta)$. In particular $\mathrm{Sha}_\ell(\mathbb{Q},e)$ is the part fixed by Δ_E.

Problem 27.2.2. Let $\eta=\omega^j$ with $(\ell-1)\nmid(e+j)$. Then $\mathrm{Sha}_\ell(\mathbb{Q},e;\eta)[\ell]\cong \mathrm{Hom}(A^{(-e-j)},\mathbb{F}_\ell)$, and η is critical for e if and only if $-e-j$ is odd.

Problem 27.2.3. For every $e\neq 0$, the minus part of $\mathrm{Sha}_\ell(\mathbb{Q}(\zeta_\ell),e)$ has the same ℓ-rank as A^-.

Over $\mathbb{Q}(\zeta_\ell)$ the critical characters account for the ℓ-rank of A^-. Over $\mathbb{Q}$, for each fixed positive odd e, one Bernoulli numerator controls all odd primes.

Problem 27.2.4. For a nonzero integer Y, $\sum_\ell v_\ell(Y)\log\ell\le\log|Y|$. Hence, for odd $e\ge 1$,

$$\sum_{\ell\ \mathrm{odd}} h_{\ell,e}(\mathbb{Q})\log\ell\le\log\Big|\mathrm{num}\Big(\frac{B_{e+1}}{e+1}\Big)\Big|.$$

Problem 27.2.5. For $k\ge 1$, $\log|\mathrm{num}(B_{2k}/2k)|\le 2k\log(2k)+3$.

For the data of Chapter 33, the proof uses a CM subfield of a cyclotomic field and the twists $0\le e<5r$, where r is the target rank of that chapter. The counterpart of Problem 27.2.4 there is Theorem 27.3.2 below. It gives one positive integer X_{odd} of controlled size such that, for every prime ℓ and every coefficient ring $\mathcal{O}$ allowed in the theorem, $v_{\mathcal{O}}(X_{\mathrm{odd}})$ bounds the $\mathcal{O}$-length of the module of cocycles of Definition 27.3.1 at every level n. The argument does not prove the main conjecture.

27.3. Odd cocycles

In this section ℓ is any prime. Fix an embedding $\overline{\mathbb{Q}}\subset\mathbb{C}$, and let $c\in\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ be complex conjugation. Let $E\subset\overline{\mathbb{Q}}$ be a CM field, $G_E:=\mathrm{Gal}(\overline{\mathbb{Q}}/E)$, and $\chi:=\chi_\ell|_{G_E}$. Then $cG_Ec=G_E$ and $\chi(cgc)=\chi(g)$. For a place $\mathfrak{P}$ of $\overline{\mathbb{Q}}$ let $D_\mathfrak{P}\supseteq I_\mathfrak{P}$ be its decomposition and inertia groups in G_E. Let $\mathcal{O}$ be the ring of integers of a finite extension of $\mathbb{Q}_\ell$, with valuation $v_\mathcal{O}$ normalized by $v_\mathcal{O}(\pi)=1$ on a uniformizer π and $v_\mathcal{O}(0)=\infty$; for $n\ge 0$ let $\mathcal{O}_n:=\mathcal{O}/\ell^n\mathcal{O}$, and write $\mathcal{O}_n(-e)$ for this quotient with $g\in G_E$ acting by $\chi(g)^{-e}$. We write len for length over $\mathcal{O}$, with values in $\{0,1,\dots,\infty\}$.

Definition 27.3.1. For integers $e,n\ge 0$, $\mathrm{Sha}^{\mathrm{odd}}_\ell(E,\mathcal{O};e,n)$ is the $\mathcal{O}$-module of maps $z\colon G_E\to\mathcal{O}_n$ such that:

(a) z is locally constant and $z(gh)=z(g)+\chi(g)^{-e}z(h)$ for all $g,h\in G_E$;
(b) $z=0$ on $I_\mathfrak{P}$ for every $\mathfrak{P}$ above a prime other than ℓ;
(c) for every $\mathfrak{P}$ above ℓ: $z=0$ on $I_\mathfrak{P}$ if $e=0$, and $z=0$ on $D_\mathfrak{P}\cap\ker\chi$ if $e>0$;
(d) if $e>0$, then $z(cgc)=-z(g)$ for all $g\in G_E$.

These are cocycles, not classes: nothing is divided out. In (c) the kernel is that of the ℓ-adic character, not of its reduction modulo ℓ^n. For $e>0$ this module is modelled on the odd part of $\mathrm{Sha}^1(E,\mathcal{O}_n(-e))$; the proof does not compare the two. Problems 27.3.1 and 27.3.2 explain the shape of the definition.

Problem 27.3.1. Let ℓ be odd and $e>0$. For $b\in\mathcal{O}_n$, the coboundary $z_b(g):=(\chi(g)^{-e}-1)b$ satisfies (a)–(c), and it satisfies (d) only if $z_b=0$.

Problem 27.3.2. For z satisfying (a)–(c) put $(c\cdot z)(g):=(-1)^e z(cgc)$. Then $c\cdot z$ satisfies (a)–(c) and $c\cdot(c\cdot z)=z$. For $e>0$, condition (d) is equivalent to $c\cdot z=(-1)^{e+1}z$. For odd ℓ this is the sign of the minus part in Section 27.2.

The twist $e = 0$. Then (a) says that z is a continuous homomorphism, (d) is void, and (b), (c) together say that z vanishes on every inertia group.

Problem 27.3.3. The Artin map identifies $\mathrm{Sha}_\ell^{\mathrm{odd}}(E, \mathcal{O}; 0, n)$ with $\mathrm{Hom}(\mathrm{Cl}(E), \mathcal{O}_n)$.

Problem 27.3.4. Let $C \cong \bigoplus_i \mathbb{Z}/m_i\mathbb{Z}$ be a finite abelian group. Then

$$\operatorname{len} \mathrm{Hom}(C, \mathcal{O}_n) = \sum_i \min\big(v_{\mathcal{O}}(m_i),\, n\, v_{\mathcal{O}}(\ell)\big) \le v_{\mathcal{O}}(|C|),$$

with equality for all large n.

Problem 27.3.5. For $E = \mathbb{Q}(\sqrt{-23})$, $\ell = 3$ and $\mathcal{O} = \mathbb{Z}_3$, the length of $\mathrm{Sha}_3^{\mathrm{odd}}(E, \mathbb{Z}_3; 0, n)$ is $\min(1, n)$; for $\ell \neq 3$ and every $\mathcal{O}$ it is 0.

Let $h_E := |\mathrm{Cl}(E)|$. Problems 27.3.3 and 27.3.4 prove the following.

Theorem 27.3.1. *Let $E \subset \overline{\mathbb{Q}}$ be a CM field, ℓ a prime, $\mathcal{O}$ the ring of integers of a finite extension of $\mathbb{Q}_\ell$, and $n \ge 0$. Then* $\operatorname{len} \mathrm{Sha}_\ell^{\mathrm{odd}}(E, \mathcal{O}; 0, n) \le v_{\mathcal{O}}(h_E)$.

The field $\mathbb{Q}(\zeta_\ell)$ modulo ℓ. Now let ℓ be odd, $E = F := \mathbb{Q}(\zeta_\ell)$, $\mathcal{O} = \mathbb{Z}_\ell$, $n = 1$ and $e > 0$, and let λ be the prime of F above ℓ.

Problem 27.3.6. Every $z \in \mathrm{Sha}_\ell^{\mathrm{odd}}(F, \mathbb{Z}_\ell; e, 1)$ is a homomorphism $G_F \to \mathbb{F}_\ell$. The module $\mathrm{Sha}_\ell^{\mathrm{odd}}(F, \mathbb{Z}_\ell; e, 1)$ does not depend on $e > 0$.

Problem 27.3.7. The map $z_{\mathrm{cyc}}(g) := (\chi(g) - 1)/\ell \bmod \ell$ is a homomorphism $G_F \to \mathbb{F}_\ell$ satisfying (b) and (c), it is nonzero on $D_{\mathfrak{P}}$ for every $\mathfrak{P}$ above ℓ, and $z_{\mathrm{cyc}}(cgc) = z_{\mathrm{cyc}}(g)$. So $z_{\mathrm{cyc}} \notin \mathrm{Sha}_\ell^{\mathrm{odd}}(F, \mathbb{Z}_\ell; e, 1)$.

Problem 27.3.8. Every $z \in \mathrm{Sha}_\ell^{\mathrm{odd}}(F, \mathbb{Z}_\ell; e, 1)$ vanishes on all of $D_{\mathfrak{P}}$, for every $\mathfrak{P}$ above ℓ.

Problem 27.3.9. The Artin map identifies $\mathrm{Sha}_\ell^{\mathrm{odd}}(F, \mathbb{Z}_\ell; e, 1)$ with $\mathrm{Hom}(A^-, \mathbb{F}_\ell)$, for every $e > 0$. Hence its length is the ℓ-rank of A^-.

By Problem 27.2.3, this is also the ℓ-rank of the minus part of $\mathrm{Sha}_\ell(F, e)$. So in this case the odd cocycles see what the minus part sees modulo ℓ: condition (d) removes the plus part, and (c) and (d) together remove the cyclotomic homomorphism z_{cyc}.

One integer for all ℓ. For a CM field in $\mathbb{Q}(\zeta_N)$, the following theorem gives one integer for every prime ℓ, every coefficient ring specified below, every $0 \le e < t$, and every $n \ge 0$.

Theorem 27.3.2. *Let $N \ge 1$ and $t \ge 0$ be integers (in the application, $t = 5r$), let d_N be the exponent of the group $(\mathbb{Z}/N\mathbb{Z})^\times$, and let $E \subset \overline{\mathbb{Q}}$ be a CM field contained in $\mathbb{Q}(\zeta_N)$. There is an integer X_{odd} with*

$$1 \le X_{\mathrm{odd}} \le 2^{4(N+t+3)^{27}} h_E$$

such that for every prime ℓ (including $\ell = 2$), every ring of integers $\mathcal{O}$ of a finite extension of $\mathbb{Q}_\ell$ that contains a primitive d_N-th root of unity, every integer e with $0 \le e < t$, and every $n \ge 0$,

$$\operatorname{len} \mathrm{Sha}_\ell^{\mathrm{odd}}(E, \mathcal{O}; e, n) \le v_{\mathcal{O}}(X_{\mathrm{odd}}).$$

In particular these lengths are finite. Here N is a cyclotomic modulus, not the level of Chapter 33. For $e = 0$ the bound follows from Theorem 27.3.1, and for $t = 1$ one may take $X_{\mathrm{odd}} = h_E$. For $0 < e < t$ the proof argues through twisted Stickelberger sums, Jacobi-type quotients of Gauss sums and Kolyvagin's derivative cocycles; Chapter 28 illustrates the Gauss-sum method. It proves no equality of characteristic ideals, only this upper bound at finite level.

In the Lean formalization. In the Lean proof [GL], Theorem 27.3.2 is `New.exists_length_shaOdd_le` and Theorem 27.3.1 is `New.length_shaOdd_zero_le_addVal_classNumber`, both in `grh/src/Lib/Cyclotomic/OddSha.lean`, and Definition 27.3.1 is the case $\Lambda = \mathcal{O}$ of `New.Selmer.shaOdd` in `grh/src/Lib/GaloisRep/Main/SelmerModules.lean`.

Problem 27.3.10. Let $E = \mathbb{Q}(\zeta_{37})$, $N = 37$ and $t \geq 2$. Then $\mathbb{Z}_{37}$ satisfies the hypotheses of Theorem 27.3.2, and every integer X_{odd} as in that theorem is divisible by 37.

Problem 27.3.11. Let N, t, d_N, E, X_{odd} be as in Theorem 27.3.2, and for each prime ℓ let $\mathcal{O}_{(\ell)}$ be the ring of integers of $\mathbb{Q}_\ell(\zeta_{d_N})$. Then $\mathcal{O}_{(\ell)}$ satisfies the hypotheses of the theorem, and for $0 \leq e < t$, $n \geq 0$ and every finite set T of primes,

$$\sum_{\ell \in T} \frac{\operatorname{len} \mathrm{Sha}_\ell^{\mathrm{odd}}(E, \mathcal{O}_{(\ell)}; e, n)}{v_{\mathcal{O}_{(\ell)}}(\ell)} \log \ell \leq \log X_{\mathrm{odd}} \leq 4(N + t + 3)^{27} \log 2 + \log h_E.$$

This is the analogue of Problem 27.2.4. Chapter 65 applies Theorem 27.3.2 to the field E of Chapter 33, with $t = 5r$. In the proof, the resulting term in the denominator error at ℓ is $t\, v_\ell(X_{\mathrm{odd}})$. For every finite set T of primes its contribution to the weighted sum is $t \sum_{\ell \in T} v_\ell(X_{\mathrm{odd}}) \log \ell \leq t \log X_{\mathrm{odd}}$.

Hints

§27.1.

27.1.1: χ_ℓ maps $G_{\mathbb{Q},\ell}$ and G_ℓ onto $\mathbb{Z}_\ell^\times$. Compute the least $v_\ell(u^k - 1)$ over $u \in \mathbb{Z}_\ell^\times$.

27.1.2: Combine Problem 27.1.1 with the theorem of von Staudt and Clausen. If $(\ell - 1) \nmid k$, then B_k/k is ℓ-integral [Wa, Cor. 5.14].

27.1.3: An unramified class lies in $H^1(\hat{\mathbb{Z}}, W_e) = W_e/(\varphi - 1)W_e$, where Frobenius φ acts by p^{-e}. For the second statement, inflate from $G_{\mathbb{Q},\ell}$; conversely, by inflation–restriction a class that is unramified outside ℓ comes from $G_{\mathbb{Q},\ell}$, since $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}_S)$ is generated as a closed normal subgroup by the inertia groups at primes $p \neq \ell$.

27.1.4: Use the sequence $0 \to \mathbb{Z}/\ell(-e) \to W_e \xrightarrow{\ell} W_e \to 0$ and Problem 27.1.1.

27.1.5: Use inflation–restriction to $G_F := \mathrm{Gal}(\mathbb{Q}_S/F)$, which acts trivially on $\mathbb{Z}/\ell(-e)$. The prime above ℓ in F is principal, and $[F_\lambda : \mathbb{Q}_\ell] = \ell - 1$ is prime to ℓ.

27.1.6: Let $i \equiv -e \pmod{\ell - 1}$. Use Theorem 27.1.1, Theorem 26.2.2, and Kummer's congruence $B_m/m \equiv B_n/n \pmod{\ell}$ for even $m, n \geq 2$ with $m \equiv n \not\equiv 0 \pmod{\ell - 1}$ [Wa, Ch. 5]; treat $i \equiv 1$ separately, using $A^{(1)} = 0$ [Wa, Prop. 6.16].

27.1.7: Problem 27.1.1 with $k = -e$, and local duality.

27.1.8: Apply the Euler characteristic formula to $\mathbb{Z}_\ell(k)/\ell^n$ and let $n \to \infty$; since the groups $H^i(G_{\mathbb{Q},\ell}, \mathbb{Z}_\ell(k)/\ell^n)$ are finite, their inverse limit is $H^i(G_{\mathbb{Q},\ell}, \mathbb{Z}_\ell(k))$ [NSW, Ch. II, §7]. For the upper bound on the rank, show that $H^2(G_{\mathbb{Q},\ell}, \mathbb{Z}_\ell(k)/\ell^n) = H^2(G_{\mathbb{Q},\ell}, \mathbb{Z}_\ell(k))/\ell^n$, which is bounded by Soulé's theorem. For the torsion, use $0 \to \mathbb{Z}_\ell(k) \to \mathbb{Q}_\ell(k) \to \mathbb{Q}_\ell/\mathbb{Z}_\ell(k) \to 0$. The groups $H^i(G_{\mathbb{Q},\ell}, M)$ are finite for finite $G_{\mathbb{Q},\ell}$-modules M of ℓ-power order [NSW, Ch. VIII, §3]; finite generation of $H^1(G_{\mathbb{Q},\ell}, \mathbb{Z}_\ell(k))$ follows from finiteness of its reduction modulo ℓ by Nakayama's lemma, and $H^3 = 0$ passes to the limit.

27.1.9: Problems 27.1.7, 27.1.8 and 27.1.2, and Theorem 27.1.2 with $e = k-1$.

§27.2.

27.2.1: Shapiro's lemma for $\mathrm{Ind}_{G_{E,\ell}}^{G_{\mathbb{Q},\ell}} W_e \cong \bigoplus_\eta W_e \otimes \eta$. The field E has one prime above ℓ.

27.2.2: Repeat Problems 27.1.4 and 27.1.5 with the twisted coefficients. On $(W_e \otimes \eta^{-1})[\ell]$, the action is through the reduction of ω^{-e-j}.

27.2.3: Sum Problem 27.2.2 over the critical j. The one character ω^{-e} not covered there is plus for e.

27.2.4: For the second part, Theorem 27.1.2.

27.2.5: $B_{2k} = (-1)^{k+1} 2(2k)!\zeta(2k)/(2\pi)^{2k}$, and bound the denominator by von Staudt–Clausen and $\prod_{p \le n} p \le 4^n$.

§27.3.

27.3.1: χ is trivial on inertia at primes other than ℓ, and $\chi(cgc) = \chi(g)$; 2 is a unit in $\mathcal{O}_n$.

27.3.2: $\chi_\ell(c) = -1$. Conjugation by c carries $D_\mathfrak{P}$, $I_\mathfrak{P}$ to $D_{c\mathfrak{P}}$, $I_{c\mathfrak{P}}$.

27.3.3: A homomorphism killing all inertia groups factors through the Galois group of the Hilbert class field; E has no real places.

27.3.4: $\mathrm{Hom}(\mathbb{Z}/m\mathbb{Z}, \mathcal{O}_n) \cong \mathcal{O}/(m, \ell^n)$, and $\mathcal{O}/\pi^k\mathcal{O}$ has length k.

27.3.5: The class number of $\mathbb{Q}(\sqrt{-23})$ is 3.

27.3.6: $\chi(g) \equiv 1 \pmod{\ell}$ on G_F.

27.3.7: $\chi(D_\mathfrak{P}) = 1 + \ell\mathbb{Z}_\ell$, since $\mathbb{Q}_\ell(\zeta_{\ell^2})$ has degree ℓ over $\mathbb{Q}_\ell(\zeta_\ell)$.

27.3.8: On $D_\mathfrak{P}$, z factors through $\chi(D_\mathfrak{P}) = 1 + \ell\mathbb{Z}_\ell$, so it is a multiple of z_{cyc} there. Compare at $\mathfrak{P}$ and $c\mathfrak{P}$, which are conjugate under G_F.

27.3.9: Problems 27.3.8 and 27.3.2; $\lambda = (1 - \zeta_\ell)$ is principal, the Artin map satisfies $\mathrm{Art}(\sigma\mathfrak{a}) = \tilde{\sigma}\,\mathrm{Art}(\mathfrak{a})\,\tilde{\sigma}^{-1}$, and $c = \sigma_{-1}$ acts on $A^{(i)}$ by $(-1)^i$.

27.3.10: Problems 27.3.9 and 26.2.8.

27.3.11: $v_\mathcal{O}(X_{\mathrm{odd}}) = v_\mathcal{O}(\ell)\, v_\ell(X_{\mathrm{odd}})$, and Problem 27.2.4.

References

[BK] S. Bloch and K. Kato, *L-functions and Tamagawa numbers of motives*, in: The Grothendieck Festschrift, Vol. I, Progr. Math. 86, Birkhäuser, 1990, 333–400.

[GL] L. Sernau, *GRH for Dirichlet L-functions, in Lean 4*, a shorter rewriting of the Lean proof, text by Claude, `https://github.com/lsernau/grh-lean`, commit `72fead1`, readable edition `grh/`.

[MW] B. Mazur and A. Wiles, *Class fields of abelian extensions of* **Q**, Invent. Math. **76** (1984), 179–330.

[Ne] J. Neukirch, *Algebraic Number Theory*, Grundlehren Math. Wiss. 322, Springer, 1999.

[NSW] J. Neukirch, A. Schmidt and K. Wingberg, *Cohomology of Number Fields*, 2nd ed., Grundlehren Math. Wiss. 323, Springer, 2008.

[SeL] J.-P. Serre, *Local Fields*, Grad. Texts in Math. 67, Springer, 1979.
[So] C. Soulé, *K-théorie des anneaux d'entiers de corps de nombres et cohomologie étale*, Invent. Math. **55** (1979), 251–295.
[Wa] L. C. Washington, *Introduction to Cyclotomic Fields*, 2nd ed., Grad. Texts in Math. 83, Springer, 1997.

ODD CLASSES BY GAUSS SUMS

Prerequisites. Chapter 27: Theorem 27.1.2, and from Section 27.3 the notation, Definition 27.3.1, Problem 27.3.2, Theorem 27.3.1 and Problem 27.3.11. Chapter 26: the Stickelberger element and Problems 26.2.3 and 26.2.8. Generalized Bernoulli numbers and the Hurwitz zeta function [Wa, Ch. 4], Gauss sums [Wa, Ch. 6], and Hilbert symbols [Se, Ch. III]. Throughout, ℓ is a prime, 2 included unless said otherwise, and $\mathcal{O}$ is the ring of integers of a finite extension of $\mathbb{Q}_\ell$, with valuation $v_\mathcal{O}$ normalized by $v_\mathcal{O}(\pi) = 1$ on a uniformizer; for an integer $X \neq 0$, $v_\mathcal{O}(X) = v_\mathcal{O}(\ell)\, v_\ell(X)$.

28.1. Odd classes

For odd primes ℓ and odd $e \geq 1$, Theorem 27.1.2 gives the length $h_{\ell,e}(\mathbb{Q})$ in terms of $B_{e+1}/(e+1)$. The proof needs a bound of this kind over a CM field E, for all ℓ at once, and for cocycles with values in $\mathcal{O}/\ell^n$. Which module is bounded, and by what?

Recall from Section 27.3 the CM field $E \subset \overline{\mathbb{Q}}$, $G_E = \mathrm{Gal}(\overline{\mathbb{Q}}/E)$, complex conjugation c, $\chi = \chi_\ell|_{G_E}$, the groups $D_\mathfrak{P} \supseteq I_\mathfrak{P}$ in G_E of a place $\mathfrak{P}$ of $\overline{\mathbb{Q}}$, and $\mathcal{O}_n = \mathcal{O}/\ell^n\mathcal{O}$. For $e, n \geq 0$, $\mathrm{Sha}_\ell^{\mathrm{odd}}(E, \mathcal{O}; e, n)$ is the $\mathcal{O}$-module of maps $z\colon G_E \to \mathcal{O}_n$ such that (Definition 27.3.1)

(a) z is locally constant and $z(gh) = z(g) + \chi(g)^{-e} z(h)$ for all $g, h \in G_E$;
(b) $z = 0$ on $I_\mathfrak{P}$ for every $\mathfrak{P}$ above a prime other than ℓ;
(c) for every $\mathfrak{P}$ above ℓ: $z = 0$ on $I_\mathfrak{P}$ if $e = 0$, and $z = 0$ on $D_\mathfrak{P} \cap \ker\chi$ if $e > 0$;
(d) if $e > 0$, then $z(cgc) = -z(g)$ for all $g \in G_E$.

We write $\mathrm{Sha}_{e,n}^{\mathrm{odd}}$ when ℓ, E and $\mathcal{O}$ are fixed. For $e = 0$, Theorem 27.3.1 gives $\mathrm{len}_\mathcal{O} \mathrm{Sha}_{0,n}^{\mathrm{odd}} \leq v_\mathcal{O}(h_E)$ for every CM field E. This chapter treats $e > 0$.

Problem 28.1.1. Let R be a commutative ring with $2 \in R^\times$, M an R-module of finite length, and σ an R-linear involution of M. Then $M = M^{\sigma=1} \oplus M^{\sigma=-1}$ and $\mathrm{len}\, M = \mathrm{len}\, M^{\sigma=1} + \mathrm{len}\, M^{\sigma=-1}$.

By Problem 27.3.2, for odd ℓ and $e > 0$ the module of maps satisfying (a)–(c) therefore splits, when it has finite length, into $\mathrm{Sha}_{e,n}^{\mathrm{odd}}$ and the part where $z(cgc) = z(g)$. Over $\mathbb{Q}$ the odd cocycles are seen through characters. Let $e > 0$ and $E \subseteq \mathbb{Q}(\mu_N)$; in this chapter N is such a modulus, as in Theorem 27.3.2, not the level of Chapter 33. Suppose that $\mathcal{O}$ contains the values of all characters modulo N. Write $H = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}(\mu_N))$. For an $\mathcal{O}$-valued Dirichlet character ψ modulo N, put $\Upsilon = \chi_\ell^e \cdot (\psi \circ \chi_N)$, where χ_N is the cyclotomic character modulo N. The *component* of ψ consists of the locally constant Υ^{-1}-cocycles $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathcal{O}_n$ that vanish at c and at the elements of H that lie in an inertia group at a place away from ℓ, or in a decomposition group above ℓ with $\chi_\ell(g) = 1$; here inertia and decomposition groups are taken in $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. The proof associates to each $z \in \mathrm{Sha}_{e,n}^{\mathrm{odd}}$ a cocycle

Date: November 26, 2026.

in each component; if the associated cocycles vanish for every ψ with $\Upsilon(c) = -1$, then $4\varphi(N)z = 0$.

Problem 28.1.2. $\chi_\ell(c) = -1$. Hence $\Upsilon(c) = -1$ if and only if $\psi(-1) = (-1)^{e+1}$, that is, if and only if ψ is *critical* for e.

Problem 28.1.3. Let χ be a primitive Dirichlet character and $k \geq 2$. Then $B_{k,\chi} = 0$ if $\chi(-1) \neq (-1)^k$, and $B_{k,\chi} \neq 0$ if $\chi(-1) = (-1)^k$. So $L(-e, \chi) \neq 0$, for $e \geq 1$, exactly when χ is critical for e.

The next problem describes the kind of field used in the proof.

Problem 28.1.4. Let $d \equiv 3 \pmod 4$ be prime and $q \geq 1$. Then $\mathbb{Q}(\sqrt{-d}) \subseteq \mathbb{Q}(\mu_d)$, and $\mathbb{Q}(\sqrt{-d}, \mu_q)$ is a CM field contained in $\mathbb{Q}(\mu_{qd})$.

The proof specializes the theorem of this chapter to $E = \mathbb{Q}(\sqrt{-d}, \mu_{q_1})$, $N = q_1 d$, and the integer t of its admissible data; the chosen embedding of E has image in $\mathbb{Q}(\mu_N)$ [GL].

28.2. One integer for all characters

On the components of the critical characters an L-value is available. How can one integer serve for all the characters modulo N at once? Fix $N, e \geq 1$; for $N = 1$ the character modulo 1 takes the value 1 at 0. For $0 \leq a < N$ put

$$\beta_a = (e+2)!\, N^{e+1} B_{e+1}(a/N).$$

Problem 28.2.1. For integers $k \geq 1$, $N \geq 1$ and a, the number $(k+1)!\, N^k B_k(a/N)$ is an integer. In particular $\beta_a \in \mathbb{Z}$.

Problem 28.2.2. Let χ be a Dirichlet character modulo N, not necessarily primitive. Then $\sum_{0 \leq a < N} \chi(a)\beta_a = -(e+2)!\,(e+1)\, N\, L(-e, \chi)$. For $N = 3$, $e = 1$ and χ trivial both sides are -6.

Problem 28.2.3. For $k \geq 2$ and $0 \leq s \leq 1$, $|B_k(s)| \leq 4\, k!/(2\pi)^k$. Hence $|\beta_a| < (e+2)!\,(e+1)!\, N^{e+1}$.

Let $U_N = (\mathbb{Z}/N)^\times$. For $t \in U_N$ put $\kappa(t) = 2\beta_t + (-1)^e[t = 1] + [t = -1]$, where β_t is taken at the representative of t in $[0, N)$ and $[\,\cdot\,]$ is 1 or 0 as the condition holds or not. Let T be the integer matrix with entries $T_{s,t} = \kappa(t/s)$, $s, t \in U_N$. In this chapter T and κ denote this matrix and this function.

Problem 28.2.4. For each Dirichlet character ψ modulo N, the vector $(\psi(t))_{t \in U_N}$ is an eigenvector of T with eigenvalue $\lambda_\psi = \sum_{t \in U_N} \psi(t)\kappa(t)$, and $\det T = \prod_\psi \lambda_\psi$.

Problem 28.2.5. $\lambda_\psi = 2\sum_{0 \leq a < N} \psi(a)\beta_a + (-1)^e + \psi(-1)$. It equals $2\sum_a \psi(a)\beta_a \neq 0$ if ψ is critical for e, and $2(-1)^e$ otherwise. In particular $\det T \neq 0$.

The correction $(-1)^e[t = 1] + [t = -1]$ does nothing on the critical characters and replaces the zeros of Problem 28.1.3 by ± 2. One integer is divisible by every eigenvalue.

Problem 28.2.6. Let R be a commutative ring, A a commutative R-algebra, free of finite rank as an R-module, $z \in A$, and $\Delta = \det_R(z \mid A)$. Then $\Delta \in zA$. Hence every A-module killed by z is killed by Δ, and, with $A = \mathbb{Z}[U_N]$ and $z = \sum_t \kappa(t)\, t$, every λ_ψ divides $\det T$ in $\mathbb{Z}[\psi]$.

Problem 28.2.7. For $N = 3$ and $e = 1$: $\beta_1 = \beta_2 = -3$, $\kappa(1) = -7$, $\kappa(2) = -5$, $\lambda_\psi = -12$ for the trivial character, which is critical, $\lambda_\psi = -2$ for the other, and $\det T = 24$.

The eigenvalues are tied to Stickelberger sums by a character-weighted form of Voronoi's congruence, as in the proof [GL]; for the classical congruence see [IR, Ch. 15, §2].

Problem 28.2.8. Let $u \geq 0$ be an integer with $u \equiv 1 \pmod N$, let $F \geq 1$ be prime to u, and let χ be a Dirichlet character modulo N. Then, in $\mathbb{Z}[\chi]$,

$$(e+2)!\,(e+1)\,N\,u^e \sum_{0 \leq a < NF} \Big\lfloor \frac{ua}{NF} \Big\rfloor a^e \chi(a) \equiv (u^{e+1}-1) \sum_{0 \leq a < N} \chi(a)\beta_a \pmod F.$$

For $N = 1$, $e = 1$, $u = 2$, $F = 5$ the two sides are 168 and 3; for $N = 3$, $e = 1$, $u = 4$, $F = 5$ and χ trivial they are 22320 and -90.

Problem 28.2.9. Let ψ be critical for e, let X be an integer divisible by $\det T$, and let $u \geq 0$, $u \equiv 1 \pmod N$. There is $w \in \mathbb{Z}[\psi]$ such that for every $F \geq 1$ prime to u,

$$(u^{e+1}-1)X \equiv 2w \sum_{0 \leq a < NF} \Big\lfloor \frac{ua}{NF} \Big\rfloor a^e \psi(a) \pmod F.$$

For fixed $N, e \geq 1$, the proof uses the integer

$$X = \big((1+N)^e - 1\big)\big((1+N)^{e+1} - 1\big)\big((1+2N)^e - 1\big)\big((1+2N)^{e+1} - 1\big)\,|\det T|,$$

so that for every prime ℓ one of $u = 1+N$, $u = 1+2N$ is prime to ℓ and $(u^e-1)(u^{e+1}-1) \mid X$. It bounds $|\det T|$ through the entries of T, using $|B_{e+1}(s)| < 17\,(e+1)!$ on $[0,1]$, and obtains the following.

Theorem 28.2.1 (Stickelberger bound)**.** *Let $N, e \geq 1$. There is an integer X with $1 \leq X \leq 2^{(N+e+3)^6}$ such that*

(a) *for every prime ℓ there is an integer $u \geq 1$ with $u \equiv 1 \pmod N$, $\ell \nmid u$ and $(u^e-1)(u^{e+1}-1) \mid X$;*

(b) *for every integer $u \geq 0$ with $u \equiv 1 \pmod N$, every integral domain Λ of characteristic 0, and every Dirichlet character ψ modulo N with values in Λ and $\psi(-1) = -(-1)^e$, there is $w \in \Lambda$ such that for every integer $F \geq 1$ prime to u, in Λ,*

$$F \;\Big|\; (u^{e+1}-1)X - 2w \sum_{0 \leq a < NF} \Big\lfloor \frac{ua}{NF} \Big\rfloor a^e \psi(a).$$

For $N = 3$ and $e = 1$ this X is 311040.

28.3. Gauss sums and the Euler system

How does an integer such as X bound a module of cocycles from above, without the main conjecture? The proof uses Kolyvagin's method for Gauss sums, in Rubin's version for class groups [Ru91], [La, Appendix], [Gr], with a Tate twist as in [BG]. At level ℓ^n, let $u \geq 1$ be an auxiliary exponent, P a finite set of primes $q \equiv 1 \pmod{uN\ell^n}$, and p a prime congruent to 1 modulo $N\ell^n \prod_{q \in P} q$. The Gauss sums at p give elements of known valuation. For $S \subseteq P$ the derivative cocycle κ_S has character $\chi_\ell^{e+1}(\psi \circ \chi_N)$; over $\mathbb{Q}(\mu_N)$ it is unramified outside ℓ, p and S; and at $q \in P \setminus S$ its value at a Frobenius is a value of $\kappa_{S \cup \{q\}}$ on inertia at the same place.

For $x \in \mathbb{Q}/\mathbb{Z}$ let $\langle x \rangle \in [0,1)$ be its representative, and for an integer $u \geq 0$ put

$$\vartheta_u(x) = \lfloor u\langle x \rangle \rfloor - \lfloor u\langle -x \rangle \rfloor.$$

For $F \geq 2$ let $\theta_F = \sum_a \langle a/F \rangle \, \sigma_a^{-1} \in \mathbb{Q}[(\mathbb{Z}/F)^\times]$, the sum over $a \in (\mathbb{Z}/F)^\times$, be the Stickelberger element at modulus F, extending the prime-modulus definition of Chapter 26.

Problem 28.3.1. Let $u \geq 1$ be prime to F. For a prime to F, $\vartheta_u(a/F) = 2\lfloor u\langle a/F \rangle \rfloor - u + 1$, and $\sum_a \vartheta_u(a/F)\, \sigma_a^{-1} = 2(u - \sigma_u)\theta_F - (u-1)\sum_a \sigma_a$. For $F = 5$, $u = 2$ the values at $a = 1, 2, 3, 4$ are $-1, -1, 1, 1$.

Fix a place $\mathfrak{P}$ of $\overline{\mathbb{Q}}$ above p, normalize its valuation by $v_{\mathfrak{P}}(p) = 1$, and form all Gauss sums $g(\chi)$ with the same nontrivial additive character of $\mathbb{F}_p$. By Stickelberger's factorization [Wa, Ch. 6], the characters χ of $\mathbb{F}_p^\times$ can be indexed by the points $x \in \mathbb{Q}/\mathbb{Z}$ of order dividing $p-1$ so that $j(\chi) = g(\chi)^u / g(\chi^u)$ satisfies $v_{\mathfrak{P}}(j(\chi)) = \lfloor u\langle x \rangle \rfloor$ and $v_{\mathfrak{P}}(j(\chi)/j(\chi^{-1})) = \vartheta_u(x)$. The proof builds its elements of known valuation from these quotients. The next problem is a cyclic group-ring model for the derivative operator.

Problem 28.3.2. Let σ generate a cyclic group of order M, $D = \sum_{i=1}^{M-1} i\sigma^i$ and $\mathcal{N} = \sum_{i=0}^{M-1} \sigma^i$. Then $(\sigma - 1)D = M - \mathcal{N}$.

The Hilbert symbol over $\mathbb{Q}$ gives a classical example of global reciprocity [Se, Ch. III].

Problem 28.3.3. The Hilbert symbol $(-1,-1)_v$ is -1 for $v = \infty$ and $v = 2$, and 1 for odd v. If $a, b \in \mathbb{Q}^\times$ and $(a,b)_v = 1$ for all places $v \neq r$, then $(a,b)_r = 1$.

The reciprocity law used in the proof is Artin reciprocity over $\mathbb{Q}(\mu_{Nm})$ at primes $q \equiv 1 \pmod{Nm}$, where $m \geq 1$ kills the component cocycle. Let $e \geq 1$, ψ critical for e, and X as in Theorem 28.2.1. Then $4X^2$ kills the component of ψ, an analogue of Stickelberger's theorem; and if $\ell > N + e + 3$, Kolyvagin's descent gives a family $(\gamma_i)_{0 \leq i \leq v_\ell(X)}$ in $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ such that every cocycle in the component of ψ vanishing at all the γ_i is zero. For a CM field $E \subseteq \mathbb{Q}(\mu_N)$ and $\mathcal{O}$ containing the values of the characters modulo N, it follows that $Y_e = 4\varphi(N) \cdot 4X^2$ kills $\mathrm{Sha}^{\mathrm{odd}}_{e,n}$, and that for $\ell > y^2$, where $y \geq N+e+3$, the elements of G_E obtained from triples (a unit modulo N, a character ψ, an index $0 \leq i \leq v_\ell(X)$) detect $\mathrm{Sha}^{\mathrm{odd}}_{e,n}$. For each $E \subseteq \mathbb{Q}(\mu_N)$ and each prime ℓ, there is a finite set in G_E detecting all maps satisfying (a) and (b), simultaneously for all $\mathcal{O}$, n, e; for every integer $y \geq N$ with $\ell \leq y^2$, it has at most y^{20} elements.

Problem 28.3.4. Let Z be an $\mathcal{O}$-submodule of the functions $G_E \to \mathcal{O}_n$, killed by an integer $m \geq 1$, and let $g_1, \ldots, g_k \in G_E$ be such that the only $z \in Z$ with $z(g_1) = \cdots = z(g_k) = 0$ is $z = 0$. Then $\mathrm{len}_{\mathcal{O}} Z \leq v_{\mathcal{O}}(m^k)$.

If $X \leq 2^{y^6}$, $y \geq 4$ and $N \leq y$, there are at most $\varphi(N)^2(y^6+1) \leq y^{20}$ triples. So for $0 < e < t$, every ℓ and $y = N + t + 3$, $\mathrm{len}_{\mathcal{O}} \mathrm{Sha}^{\mathrm{odd}}_{e,n} \leq v_{\mathcal{O}}(Y_e^{y^{20}})$, where X_e is an integer as in Theorem 28.2.1 for N and e, and $Y_e = 4\varphi(N) \cdot 4X_e^2$. One integer for all $0 < e < t$ is $\left(\prod_{0<e<t} Y_e\right)^{y^{20}}$.

Problem 28.3.5. Let $N \ge 1$, $t \ge 0$, $y = N + t + 3$, and let $1 \le X_e \le 2^{(N+e+3)^6}$ for $0 < e < t$. Then

$$\Big(\prod_{0<e<t} 4\varphi(N) \cdot 4X_e^2 \Big)^{y^{20}} \le 2^{4y^{27}}.$$

Theorem 27.3.1, Problems 28.3.4 and 28.3.5, Theorem 28.2.1 and the statements above prove Theorem 27.3.2, with $X_{\rm odd} = \big(\prod_{0<e<t} Y_e\big)^{y^{20}} h_E$: one integer $X_{\rm odd} \le 2^{4(N+t+3)^{27}} h_E$ bounds $\operatorname{len}_{\mathcal O} \operatorname{Sha}_\ell^{\rm odd}(E, \mathcal O; e, n)$ by $v_{\mathcal O}(X_{\rm odd})$ for every prime ℓ, 2 and the primes dividing N included, every $\mathcal O$ as in that theorem, every $0 \le e < t$ and every $n \ge 0$.

28.4. Examples, and the main conjecture

How much is lost? For odd ℓ and odd $e \ge 1$, we can compare the eigenvalue for the principal character modulo ℓ with the exact value of $h_{\ell,e}(\mathbb Q)$ in Theorem 27.1.2. First we compute the 37-adic valuations of the eigenvalues for all critical characters modulo 37 at $e = 1$. For $N > 1$ and ψ critical, $\lambda_\psi = 2\,(e+2)!\,N\,B_{e+1,\psi}^{(N)}$ with $B_{k,\psi}^{(N)} = N^{k-1} \sum_{a=1}^{N} \psi(a) B_k(a/N)$, which is $B_{k,\psi}$ when ψ is primitive of conductor N. Let ω be the Teichmüller character modulo ℓ.

Problem 28.4.1. Let $\ell = N = 37$, $e = 1$, and $\psi = \omega^j$ with j even, $0 \le j < 36$. Then $v_{37}(\lambda_\psi) = 1 + v_{37}(B_{2,\omega^j})$ for $j \ne 0$, and $v_{37}(\lambda_\psi) = 1$ for $j = 0$. It equals 2 for $j = 30$, 0 for $j = 34$, and 1 for the other j.

At $j = 30$ the value reflects the irregular pair $(37, 32)$ of Problem 26.2.8, through Kummer's congruences [Wa, Ch. 5].

Problem 28.4.2. Let ℓ be odd, $N = \ell$, $\psi = 1$ and e odd. Then $v_\ell(\lambda_\psi) = v_\ell(B_{e+1}) + 1 + v_\ell\big((e+2)!\big)$. For $\ell = 691$, $e = 11$ this is 2, while $h_{691,11}(\mathbb Q) = 1$.

Problem 28.4.3. If ℓ is odd, e is odd and $(\ell - 1) \nmid (e + 1)$ (so $\ell \ge 5$), the value of Problem 28.4.2 exceeds the value $h_{\ell,e}(\mathbb Q)$ given by Theorem 27.1.2 by exactly $1 + v_\ell\big((e+2)!\big) + v_\ell(e+1)$.

For each $0 < e < t$, one may take X_e to be the determinant multiple of Section 28.2; each eigenvalue for that e divides X_e in its character ring, and the witness above contains the squares X_e^2 in a product raised to the power y^{20}. Why is so coarse a bound good enough, and why does a bound at finite level replace the main conjecture? The proof uses Theorem 27.3.2 only as an upper bound, at every prime ℓ, for the integer $X_{\rm odd}$ that it chooses for the data of Chapter 33; the denominator error at ℓ includes the term $t\, v_\ell(X_{\rm odd})$ (Chapter 65) [GL]. The main conjecture of Mazur and Wiles [MW] gives the formula of Theorem 27.1.2 for the rational Tate twists; the proof notes that for large ℓ a bound of this kind follows from it, and proves only an upper bound at finite level. To bound the valuations $v_\ell(X_{\rm odd})$ with weights $\log \ell$ it uses the size of $X_{\rm odd}$, by Problem 27.2.4:

$$\sum_{\ell \in \mathcal L} v_\ell(X) \log \ell \le \log X \le 4(N+t+3)^{27} \log 2 + \log h_E$$

for every finite set $\mathcal L$ of primes. For the data, $\log h_E \le x^{30}$, the sum is at most x^{2000}, and $x^{10^6} \le x_1$, $x_1^{10^6} \le b$ [GL]. So the sum is at most $b^{1/(5\cdot 10^8)}$, and its contribution to the denominator errors, weighted by $\log \ell$, is at most $t\, x^{2000}$.

In the Lean formalization. In the Lean proof [GL], Theorem 27.3.2 is `New.exists_length_shaOdd_le`, in `Lib/Cyclotomic/OddSha.lean`, and Theorem 28.2.1 is `New.OddPart.exists_isStickelbergerBound`, in `Lib/Cyclotomic/Voronoi.lean`.

Hints

§28.1.

28.1.1: The projections $(1 \pm \sigma)/2$.

28.1.2: c acts on roots of unity by inversion.

28.1.3: $B_k(1-s) = (-1)^k B_k(s)$; for the nonvanishing, $L(1-k,\chi) = -B_{k,\chi}/k$ [Wa, Thm. 4.2] and the functional equation relating $L(1-k,\chi)$ to $L(k,\bar{\chi}) \neq 0$.

28.1.4: The quadratic Gauss sum.

§28.2.

28.2.1: Expand $B_k(a/N)$ in powers of a/N, and apply von Staudt–Clausen to the coefficients.

28.2.2: $L(s,\chi) = N^{-s}\sum_{a=1}^{N}\chi(a)\zeta(s,a/N)$ and $\zeta(-e,x) = -B_{e+1}(x)/(e+1)$ [Wa, Ch. 4].

28.2.3: The Fourier series of $B_k(s)$ on $[0,1]$, obtained by integrating by parts with $B_k' = kB_{k-1}$; and $\zeta(k) \le \zeta(2)$.

28.2.4: Substitute $t = st'$; then orthogonality of characters.

28.2.5: Problems 28.2.2 and 28.1.3, and $L(-e,\chi) = L(-e,\chi_0)\prod_{p\mid N}(1-\chi_0(p)p^e)$ for the primitive χ_0 inducing χ.

28.2.6: The Cayley–Hamilton theorem for multiplication by z; in the basis U_N its matrix is the transpose of T.

28.2.8: Write $ua = r_a + NFq_a$ with $0 \le r_a < NF$, expand $(ua)^{e+1}$ modulo $(NF)^2$ and sum against $\chi(a)$; $a \mapsto r_a$ permutes the residues. Evaluate $\sum_{0\le a<NF}\chi(a)a^{e+1}$ by $\sum_{0\le i<n}(x+i)^k = \big(B_{k+1}(x+n) - B_{k+1}(x)\big)/(k+1)$, and control denominators with Problem 28.2.1.

28.2.9: Problems 28.2.6 and 28.2.8.

§28.3.

28.3.1: Here $F \nmid ua$. For the group-ring identity, reindex the sum over units as in the prime-modulus Problem 26.2.3.

28.3.2: Telescope, using $\sigma^M = 1$.

28.3.3: The formulas for $(a,b)_v$ and the product formula [Se, Ch. III, §2].

28.3.4: Evaluate at $g_1, \dots, g_k$.

28.3.5: Bound one factor by a power of 2.

§28.4.

28.4.1: Compute $\lambda_\psi = 2\sum_{t=1}^{36}\omega(t)^j(6t^2 - 222t + 1369)$ in $\mathbb{Z}_{37}$ to a few digits.

28.4.2: $B_{k,1}^{(\ell)} = (1-\ell^{k-1})B_k$, $B_{12} = -691/2730$, and Theorem 27.1.2.

28.4.3: $B_{e+1}/(e+1)$ is ℓ-integral when $(\ell-1) \nmid (e+1)$ [Wa, Cor. 5.14].

References

[BG] G. Banaszak and W. Gajda, *Euler systems for higher K-theory of number fields*, J. Number Theory **58** (1996), 213–252.

[GL] L. Sernau, *GRH for Dirichlet L-functions, in Lean 4*, a shorter rewriting of the Lean proof, text by Claude, `https://github.com/lsernau/grh-lean`, commit `72fead1`, readable edition `grh/`.

[Gr] C. Greither, *Class groups of abelian fields, and the main conjecture*, Ann. Inst. Fourier (Grenoble) **42** (1992), 449–499.

[IR] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, 2nd ed., Grad. Texts in Math. 84, Springer, 1990.

[La] S. Lang, *Cyclotomic Fields I and II*, combined 2nd ed., with an appendix by K. Rubin, Grad. Texts in Math. 121, Springer, 1990.

[MW] B. Mazur and A. Wiles, *Class fields of abelian extensions of* **Q**, Invent. Math. **76** (1984), 179–330.

[Ru91] K. Rubin, *Kolyvagin's system of Gauss sums*, in: Arithmetic Algebraic Geometry (Texel, 1989), Progr. Math. 89, Birkhäuser, 1991, 309–324.

[Se] J.-P. Serre, *A Course in Arithmetic*, Grad. Texts in Math. 7, Springer, 1973.

[Wa] L. C. Washington, *Introduction to Cyclotomic Fields*, 2nd ed., Grad. Texts in Math. 83, Springer, 1997.

CONGRUENCE MODULES

Prerequisites. Modules over a Dedekind domain and the elementary divisor theorem. Ideals in quadratic fields. Modular forms of level 1: the structure of M_k and S_k [SeA, Ch. VII, §3.2, Thm. 4], Eisenstein series and Δ [SeA, Ch. VII, §§4.2–4.3], Hecke operators and their action on q-expansions, and normalized eigenforms [SeA, Ch. VII, §§5.3–5.5]; Serre writes the weight as $2k$ and numbers the Bernoulli numbers differently. The Petersson product, for which the Hecke operators are self-adjoint [DS, §5.5]. From Chapter 26, *Denominators and the Stickelberger element*: the cost of a denominator (Problem 26.1.5) and Theorem 26.2.2.

In Chapter 26 a linear map that does not respect integral structures cost $\log[M + T(L) : M]$. One step of the proof asks for an operator clearing the denominators of an orthogonal projection onto the image of a theta lift restricted to good forms. It tests that operator on a restricted set of integral forms. Projection onto a sum of whole Hecke eigenspaces is a model for this problem. What does such a projection cost, and what controls the cost? On the full lattice the answer is a congruence module. We compute it for level 1, in weight 12, where it is $\mathbb{Z}/691\mathbb{Z}$, and in weight 24, where it detects a congruence modulo the unique prime ideal above 144169 between the two newforms.

29.1. Congruence modules

Let $\mathcal{O}$ be a Dedekind domain with fraction field K. A *lattice* in a finite-dimensional K-vector space V is a finitely generated $\mathcal{O}$-submodule that spans V. Let $V = V_1 \oplus V_2$, let π_1, π_2 be the two projections, and let $\Lambda \subset V$ be a lattice. The *congruence module* of V_1 in Λ is

$$\mathrm{C}(\Lambda; V_1) := \pi_1(\Lambda)/(\Lambda \cap V_1).$$

Problem 29.1.1. $\pi_1(\Lambda) = V_1 \cap (\Lambda + V_2)$, and

$$\mathrm{C}(\Lambda; V_1) \cong \Lambda/\big((\Lambda \cap V_1) \oplus (\Lambda \cap V_2)\big) \cong \mathrm{C}(\Lambda; V_2).$$

In particular $\mathrm{C}(\Lambda; V_1)$ is a finitely generated torsion $\mathcal{O}$-module, and it vanishes exactly when $\Lambda = (\Lambda \cap V_1) \oplus (\Lambda \cap V_2)$.

Problem 29.1.2. $(\Lambda + \pi_1(\Lambda))/\Lambda \cong \mathrm{C}(\Lambda; V_1)$. For $\mathcal{O} = \mathbb{Z}$, the least positive integer c with $c\,\pi_1(\Lambda) \subseteq \Lambda$ is the exponent of $\mathrm{C}(\Lambda; V_1)$.

So for $\mathcal{O} = \mathbb{Z}$ the index $[\Lambda + \pi_1(\Lambda) : \Lambda]$ is $|\mathrm{C}(\Lambda; V_1)|$: measured like the index cost of Problem 26.1.5 (stated there for injective maps), the projection costs $\log|\mathrm{C}(\Lambda; V_1)|$.

Problem 29.1.3. Let $N \geq 1$, $V = \mathbb{Q}^2 = \mathbb{Q}e_1 \oplus \mathbb{Q}e_2$, and $\Lambda = \{(a, b) \in \mathbb{Z}^2 : a \equiv b \pmod N\}$. Then $\mathrm{C}(\Lambda; \mathbb{Q}e_1) \cong \mathbb{Z}/N\mathbb{Z}$, whereas $\mathrm{C}(\mathbb{Z}^2; \mathbb{Q}e_1) = 0$.

The lattices of interest carry an action of a Hecke algebra. Let X be a finite set, and let $\mathbf{T} \subseteq \prod_{x \in X} \mathcal{O}$ be an $\mathcal{O}$-subalgebra, finitely generated as an $\mathcal{O}$-module, which separates the points of X. Write $t(x)$ for the coordinates of $t \in \mathbf{T}$. Let $\mathbf{T}$

Date: November 25, 2026.

act on $V = \bigoplus_{x\in X} V_x$ by $t \cdot v = (t(x)v_x)_x$, and let Λ be a $\mathbf{T}$-stable lattice. The *congruence ideal* of x is

$$\mathfrak{c}_x := \{t(x) : t \in \mathbf{T},\ t(y) = 0 \text{ for all } y \neq x\} \subseteq \mathcal{O},$$

and we write $\mathrm{C}(\Lambda; V_x)$ for the congruence module with respect to $V = V_x \oplus \bigoplus_{y\neq x} V_y$.

Problem 29.1.4. $\mathfrak{c}_x$ annihilates $\mathrm{C}(\Lambda; V_x)$. If $\mathcal{O}$ is a discrete valuation ring with normalized valuation v, then $\mathrm{len}_{\mathcal{O}} \mathrm{C}(\Lambda; V_x) \leq \dim V_x \cdot \min v(\mathfrak{c}_x)$.

Problem 29.1.5. If $\Lambda \cong \mathbf{T}$ as a $\mathbf{T}$-module, then $\mathrm{C}(\Lambda; V_x) \cong \mathcal{O}/\mathfrak{c}_x$. For $\mathbf{T} = \{(a, b) \in \mathbb{Z}^2 : a \equiv b \pmod N\}$ acting on itself, $\mathfrak{c}_x = N\mathbb{Z}$ at both points.

Thus $\mathfrak{c}_x$ annihilates the obstruction to integral projection onto V_x. When the lattice is free of rank one over $\mathbf{T}$, this obstruction module is isomorphic to $\mathcal{O}/\mathfrak{c}_x$.

A congruence module can also be read off from a pairing. Suppose that Λ carries a *perfect* pairing $\langle\,,\rangle\colon \Lambda \times \Lambda \to \mathcal{O}$, that is, an $\mathcal{O}$-bilinear form for which $\lambda \mapsto \langle\lambda, \cdot\rangle$ is an isomorphism $\Lambda \to \mathrm{Hom}_{\mathcal{O}}(\Lambda, \mathcal{O})$, and that $\langle V_1, V_2\rangle = \langle V_2, V_1\rangle = 0$. For a lattice $L \subset V_1$ let $L^\vee := \{v \in V_1 : \langle v, L\rangle \subseteq \mathcal{O}\}$.

Problem 29.1.6. $\pi_1(\Lambda) = (\Lambda \cap V_1)^\vee$. Hence $\mathrm{C}(\Lambda; V_1) \cong (\Lambda \cap V_1)^\vee/(\Lambda \cap V_1)$.

Problem 29.1.7. In the setting of Problem 29.1.6: (i) if f is a basis of $\Lambda \cap V_1$ over $\mathcal{O}$, then $\mathrm{C}(\Lambda; V_1) \cong \mathcal{O}/\langle f, f\rangle\mathcal{O}$; (ii) if x, y form an $\mathcal{O}$-basis of $\Lambda \cap V_1$ with $\langle x, x\rangle = \langle y, y\rangle = 0$, then $\mathrm{C}(\Lambda; V_1) \cong (\mathcal{O}/\langle x, y\rangle\mathcal{O}) \oplus (\mathcal{O}/\langle y, x\rangle\mathcal{O})$. For $\Lambda = \mathbb{Z}^2$ with the dot product and $V_1 = \mathbb{Q}(1, 1)$, $V_2 = \mathbb{Q}(1, -1)$, the congruence module is $\mathbb{Z}/2\mathbb{Z}$.

For a self-dual lattice the congruence module of an orthogonal summand is its discriminant module, the quotient in Problem 29.1.6. In Section 29.4 the discriminant of the cohomological eigenlattice detects the primes in the support of the eigenform's congruence module in the range of Hida's theorem. Compare [DDT, §4.4, Lemma 4.17], where a power of the congruence ideal of the Hecke algebra is shown to lie in the discriminant ideal of the eigenform's piece of a self-dual lattice, with equality when the lattice is free over the Hecke algebra.

29.2. The Eisenstein line in weight 12

For even $k \geq 4$ let M_k and S_k be the spaces of modular forms and cusp forms of weight k for $\mathrm{SL}_2(\mathbb{Z})$, identified with their q-expansions, and let $M_k(\mathbb{Z}) := M_k \cap \mathbb{Z}[[q]]$ and $S_k(\mathbb{Z}) := S_k \cap \mathbb{Z}[[q]]$. Let $\sigma_{k-1}(n) := \sum_{d|n} d^{k-1}$ and

$$E_k := 1 - \frac{2k}{B_k} \sum_{n\geq 1} \sigma_{k-1}(n) q^n, \qquad \Delta := q \prod_{n\geq 1} (1 - q^n)^{24} = \sum_{n\geq 1} \tau(n) q^n,$$

so that $E_4 = 1 + 240 \sum \sigma_3(n) q^n$, $E_6 = 1 - 504 \sum \sigma_5(n) q^n$, and $B_{12} = -691/2730$ [SeA, Ch. VII, §4]. Write $M_k(\mathbb{Q}) := M_k \cap \mathbb{Q}[[q]]$ and $S_k(\mathbb{Q}) := S_k \cap \mathbb{Q}[[q]]$. We use the decomposition $M_k(\mathbb{Q}) = \mathbb{Q}E_k \oplus S_k(\mathbb{Q})$, in which both summands are stable under the Hecke operators.

Problem 29.2.1. $M_{12}(\mathbb{Z}) = \mathbb{Z}E_4^3 \oplus \mathbb{Z}\Delta$.

Problem 29.2.2. $E_4^3 = E_{12} + \frac{432000}{691}\Delta$. Hence $\pi_\Delta(M_{12}(\mathbb{Z})) = \frac{1}{691}\mathbb{Z}\Delta$, and $\mathrm{C}(M_{12}(\mathbb{Z}); \mathbb{Q}\Delta) \cong \mathbb{Z}/691\mathbb{Z}$.

The same computation for the Eisenstein line works in every weight.

Problem 29.2.3. Let $k \geq 4$ be even, and let N_k be the numerator of $B_k/2k$ in lowest terms. Then $\mathrm{C}(M_k(\mathbb{Z}); \mathbb{Q}E_k) \cong \mathbb{Z}/N_k\mathbb{Z}$. For $k = 4, 6, 8, 10, 14$ one has $N_k = \pm 1$, and $|N_{16}| = 3617$, $|N_{22}| = 77683 = 131{\cdot}593$, $|N_{24}| = 236364091 = 103{\cdot}2294797$.

Let $\mathbf{T}_{12}$ be the $\mathbb{Z}$-algebra of endomorphisms of $M_{12}(\mathbb{Q})$ generated by the Hecke operators T_n, $n \geq 1$, normalized so that $T_n\Delta = \tau(n)\Delta$ and $T_nE_{12} = \sigma_{11}(n)E_{12}$ [SeA, Ch. VII, §5]. Map $\mathbf{T}_{12}$ to $\mathbb{Z} \times \mathbb{Z}$ by its eigenvalues on (Δ, E_{12}).

Problem 29.2.4. Each T_n preserves $M_{12}(\mathbb{Z})$, and $\mathbf{T}_{12} = \{(a, b) \in \mathbb{Z}^2 : a \equiv b \pmod{691}\}$. Thus the congruence ideal of Δ is $691\mathbb{Z}$.

After localization at 691, the length bound of Problem 29.1.4 is attained. Consider now the global $\mathbf{T}_{12}$-module.

Problem 29.2.5. $M_{12}(\mathbb{Z})$ is not free of rank one over $\mathbf{T}_{12}$.

The prime 691 is also the one in Theorem 26.2.2: since $691 \mid B_{12}$, the eigenspace $A^{(679)}$ of the 691-part of the class group of $\mathbb{Q}(\zeta_{691})$ is nonzero. That the same prime measures both is not an accident; Chapter 30 builds the class from the congruence.

29.3. Two newforms of weight 24

The space S_{24} has dimension 2 [SeA, Ch. VII, §3.2], and its two normalized eigenforms are not rational. Let $D := 144169$, a prime with $D \equiv 1 \pmod{24}$, let $K := \mathbb{Q}(\sqrt{D})$, $\mathcal{O} := \mathcal{O}_K$, and $\mathfrak{p} := \sqrt{D}\,\mathcal{O}$.

Problem 29.3.1. $S_{24}(\mathbb{Z}) = \mathbb{Z}g_1 \oplus \mathbb{Z}g_2$, where $g_1 = \Delta E_4^3 - 696\Delta^2 = q + 195660q^3 + \cdots$ and $g_2 = \Delta^2 = q^2 - 48q^3 + \cdots$.

On S_{24} one has $a_n(T_2 f) = a_{2n}(f) + 2^{23}a_{n/2}(f)$, with $a_{n/2} := 0$ for odd n.

Problem 29.3.2. $T_2 g_1 = 20468736\, g_2$ and $T_2 g_2 = g_1 + 1080\, g_2$. The characteristic polynomial of T_2 on S_{24} is $x^2 - 1080x - 20468736$, with discriminant $24^2 D$ and roots $\lambda_\pm = 540 \pm 12\sqrt{D}$. The normalized eigenforms are $f_\pm = g_1 + \lambda_\pm g_2$.

Let $\mathbf{T}_{24}$ be the $\mathbb{Z}$-algebra generated by the T_n on S_{24}.

Problem 29.3.3. $\mathbf{T}_{24} = \mathbb{Z}[T_2] = \mathbb{Z} \oplus \mathbb{Z}T_2$, and $S_{24}(\mathbb{Z}) = \mathbf{T}_{24}\, g_2$ is free of rank one over $\mathbf{T}_{24}$.

Let $\Lambda := S_{24}(\mathbb{Z}) \otimes \mathcal{O}$ in $V := S_{24}(\mathbb{Z}) \otimes K = Kf_+ \oplus Kf_-$, and let $\mathbf{T}_{24} \otimes \mathcal{O}$ act on it, through its eigenvalues, as a subalgebra of $\mathcal{O} \times \mathcal{O}$.

Problem 29.3.4. The congruence ideal of f_+ is $(\lambda_+ - \lambda_-)\mathcal{O} = 24\sqrt{D}\,\mathcal{O}$. Hence $\mathrm{C}(\Lambda; Kf_+) \cong \mathcal{O}/24\sqrt{D}\,\mathcal{O}$. Verify the module isomorphism also by direct projection.

Problem 29.3.5. $a_n(f_+) \equiv a_n(f_-) \pmod{24\sqrt{D}\,\mathcal{O}}$ for all n. The primes 2 and 3 split in K, and $\mathrm{C}(\Lambda; Kf_+)$ has length 1 at $\mathfrak{p}$, length 3 at each prime above 2, and length 1 at each prime above 3.

The congruence modulo $\mathfrak{p}$, the ramified prime of the Hecke field, is the interesting one. The primes 2 and 3 are smaller than the weight, outside the range $p > k$ of Hida's theorem below (Theorem 29.4.1).

29.4. Hida's identity

Which primes occur in the congruence module of a cuspidal eigenform? Let $k \geq 12$ be even, let $f = \sum a(n)q^n \in S_k$ be a normalized eigenform, let $K \subset \mathbb{C}$ be a number field containing the coefficients of all normalized eigenforms in S_k, $\mathcal{O} := \mathcal{O}_K$, and $\Lambda := S_k(\mathbb{Z}) \otimes \mathcal{O}$. Let $Y \subset S_k(\mathbb{Z}) \otimes K$ be the span of the other normalized eigenforms, and write $\mathrm{C}(f) := \mathrm{C}(\Lambda; Kf)$ for the decomposition $S_k(\mathbb{Z}) \otimes K = Kf \oplus Y$. Let

$$\langle g, h \rangle := \int_{\mathrm{SL}_2(\mathbb{Z})\backslash\mathcal{H}} g(z)\,\overline{h(z)}\,y^k\,\frac{dx\,dy}{y^2}$$

be the Petersson product.

Problem 29.4.1. Y is the orthogonal complement of f, and the projection to Kf is $g \mapsto \frac{\langle g,f\rangle}{\langle f,f\rangle} f$. Hence $\mathrm{C}(f) \cong J_f/\mathcal{O}$, where J_f is the $\mathcal{O}$-module generated by the numbers $\langle g, f\rangle/\langle f, f\rangle$ with $g \in S_k(\mathbb{Z})$. For $f = f_+$ of Section 29.3, $J_f = (24\sqrt{D})^{-1}\mathcal{O}$.

The projection divides by $\langle f, f\rangle$. Hida's theorem detects the primes above $p > k$ at which the projection fails to preserve the lattice. For p prime write $a(p) = \alpha_p + \beta_p$ with $\alpha_p\beta_p = p^{k-1}$, and let

$$L(\mathrm{Sym}^2 f, s) := \prod_p \bigl(1 - \alpha_p^2 p^{-s}\bigr)^{-1}\bigl(1 - p^{k-1-s}\bigr)^{-1}\bigl(1 - \beta_p^2 p^{-s}\bigr)^{-1} \qquad (\mathrm{Re}\, s > k).$$

In the unitary normalization, the *adjoint L-function* is $L(s, \mathrm{Ad}\, f) := L(\mathrm{Sym}^2 f, s + k - 1)$; its value at $s = 1$ is $L(\mathrm{Sym}^2 f, k)$.

Problem 29.4.2. Let $\alpha, \beta \in \mathbb{C}$, $w := \alpha\beta$, and $a_m := \sum_{i=0}^m \alpha^i\beta^{m-i}$. Then, as a formal power series in X,

$$\sum_{m\geq 0} a_m^2 X^m = \frac{1 + wX}{(1 - \alpha^2 X)(1 - wX)(1 - \beta^2 X)}.$$

Hence, for $\mathrm{Re}\, s > k$, $\sum_{n\geq 1} a(n)^2 n^{-s} = \zeta(s - k + 1)\, L(\mathrm{Sym}^2 f, s)/\zeta(2s - 2k + 2)$.

Rankin's method [Ra] computes the residue of this Dirichlet series at $s = k$; in terms of $L(\mathrm{Sym}^2 f, s)$, which is holomorphic there [Sh],

$$\langle f, f\rangle = \frac{(k-1)!}{2^{2k-1}\pi^{k+1}}\, L(\mathrm{Sym}^2 f, k) \tag{1}$$

[Za, p. 109, (3)–(5)]. For $f = \Delta$ both sides equal $1.0353620568\ldots \times 10^{-6}$, the value of $\|\Delta\|^2$ found from Petersson's formula in Section 10.2 of Chapter 10.

The transcendental part of $\langle f, f\rangle$ is measured by periods. Let

$$r_f(X) := \int_0^{i\infty} f(z)(X - z)^{k-2}\,dz,$$

and let r_f^+ and r_f^- be its even and odd parts in X. By Manin's theorem there are $\omega_f^\pm \in \mathbb{C}^\times$ with $r_f^\pm \in \omega_f^\pm K[X]$ [Mn]. For $f = \Delta$ one has [KZ]

$$r_\Delta^+ = \omega^+\Bigl(\tfrac{36}{691}(X^{10} - 1) + X^2 - 3X^4 + 3X^6 - X^8\Bigr),$$
$$r_\Delta^- = \omega^-\bigl(4X^9 - 25X^7 + 42X^5 - 25X^3 + 4X\bigr).$$

Problem 29.4.3. The two polynomials in parentheses, and $X^{10}-1$, satisfy $P(X)+X^{10}P(-1/X)=0$.

The polynomial $X^{10}-1$ is a coboundary in the Eichler–Shimura cohomology, and the prime in front of it is the 691 of Problem 29.2.2. For a cusp form one discards this direction. Fix a prime $\mathfrak{p}$ of $\mathcal{O}$ above a prime $p>k$, let $\mathcal{O}_{\mathfrak{p}}$ be the localization of $\mathcal{O}$ at $\mathfrak{p}$, and let $\Omega_f^{\pm}\in\mathbb{C}^{\times}$ be Hida's periods, defined by generators of the f-eigenlines in the parabolic cohomology of $\mathrm{SL}_2(\mathbb{Z})$ with coefficients in polynomials of degree at most $k-2$ over $\mathcal{O}_{\mathfrak{p}}$; the period polynomial represents the class of f there, modulo the coboundary $X^{k-2}-1$. For the numerical checks below we use instead the displayed period-polynomial coefficients: $\Omega_f^{\pm}$ such that the coefficients of X^n in $r_f^{\pm}$ with $0<n<k-2$ lie in $\Omega_f^{\pm}\mathcal{O}_{\mathfrak{p}}$ and generate it. Identifying this normalization with Hida's in general requires an integral comparison of period polynomials and cohomology classes modulo $X^{k-2}-1$. The following theorem is due to Hida [Hi1, Hi2], with a contribution of Ribet [Ri]; see [Gh, Thm. 1]. We use it as a black box.

Theorem 29.4.1 (Hida)**.** *The number $\eta_f:=\langle f,f\rangle/(\mathrm{i}\,\Omega_f^{+}\Omega_f^{-})$ lies in K. If $\mathfrak{p}$ lies above a prime $p>k$, then $\mathrm{C}(f)\otimes\mathcal{O}_{\mathfrak{p}}\neq 0$ if and only if $\eta_f\in\mathfrak{p}\mathcal{O}_{\mathfrak{p}}$.*

By (1), η_f is, up to a $\mathfrak{p}$-adic unit, the algebraic part $L(1,\mathrm{Ad}\,f)/(\pi^{k+1}\mathrm{i}\,\Omega_f^{+}\Omega_f^{-})$ of the adjoint L-value. In outline, the proof applies Problem 29.1.7(ii) to the parabolic cohomology lattice, self-dual for $p>k$, whose f-part is spanned by isotropic $\pm$ lines; the main difficulty is to compare this cohomological congruence module with $\mathrm{C}(f)$ [Gh, §3]; in weight 2 see [DDT, §4.4]. Two checks with PARI/GP [PARI]. For $f=\Delta$, take the coefficient of X^2 in r_{Δ}^{+} as Ω^{+} and take $\Omega^{-}=\omega^{-}$. The computation gives $\eta_{\Delta}=\pm 2^{-10}$, in agreement with the absence of cuspidal congruence primes for $S_{12}=\mathbb{C}\Delta$. Replacing Ω^{+} by $(36/691)\Omega^{+}$ would give $v_{691}(\eta_{\Delta})=1$. For $f=f_{+}$ of Section 29.3, take $K=\mathbb{Q}(\sqrt{D})$ and use the coefficients of X^2 in r_f^{+} and of X in r_f^{-} for Ω^{+} and Ω^{-}, respectively. These coefficients generate the respective fractional ideals of the interior coefficients at every prime above $p>24$. The norm $N_{K/\mathbb{Q}}(\eta_f)$ is D times a rational number whose numerator and denominator have no prime factor greater than 24. Thus $v_{\mathfrak{p}}(\eta_f)=1$ at $\mathfrak{p}=\sqrt{D}\,\mathcal{O}$, as in Problem 29.3.5.

Comparison with the full lattice. For a Hecke-stable lattice Λ as in Section 29.1, let $V_1=\bigoplus_{x\in I}V_x$ for a nonempty subset I of X, and project along the sum of the remaining eigenspaces. On the full lattice the obstruction is $\mathrm{C}(\Lambda;V_1)$, by Problems 29.1.1 and 29.1.2, and the ideal $\bigcap_{x\in I}\mathfrak{c}_x$ annihilates it, as in Problem 29.1.4. For a single cuspidal eigenline, Theorem 29.4.1 detects its congruence primes above $p>k$ by an adjoint L-value. For the Eisenstein congruence of Δ at 691, Ribet's construction gives an unramified quotient of order 691 of $A^{(679)}$ (Chapter 30). For odd primes ℓ, Chapter 27 gives the Selmer length over $\mathbb{Q}$ for positive odd twists e and identifies the classes killed by ℓ with homomorphisms on a class-group eigenspace when $(\ell-1)\nmid e$. Chapter 30 constructs a class from an Eisenstein congruence, and Problem 31.3.3 of Chapter 31 bounds the congruence length of one eigenform by a Selmer length.

The step this chapter serves. The chapter serves one step of the proof: clearing the denominators of an orthogonal projection onto a space of theta lifts. The corresponding statement of the Lean proof [GL] is `ClearsProjection`, in `grh/src/New/Determinant/Twist/FitTwists.lean`; the corresponding bound is `denominatorLe_clearingBound`, in `grh/src/New/Congruences/FirstOrder/DenominatorBound.lean`, with its specialization `denominatorLe_range_goodLift`, in `grh/src/New/Congruences/FitTwistsExist.lean`.

Exercise. For $k = 16, 18, 20, 22, 26$ the space S_k is spanned by one normalized eigenform f_k, and $a_\ell(f_k) \equiv 1 + \ell^{k-1} \pmod{N_k}$ for every prime ℓ.

Hints

§29.1.

29.1.1: Consider $\Lambda \to \pi_1(\Lambda)/(\Lambda \cap V_1)$, $\lambda \mapsto \pi_1(\lambda)$, and compute its kernel.
29.1.2: The map $\pi_1(\Lambda) \to (\Lambda + \pi_1(\Lambda))/\Lambda$.
29.1.3: $\pi_1(\Lambda) = \mathbb{Z}e_1$.
29.1.4: Apply to Λ an element of $\mathbf{T}$ that vanishes off x. For the length, $\pi_x(\Lambda)$ is free of rank $\dim V_x$.
29.1.5: Identify V_x with K by $t \mapsto t(x)$; then $\pi_x(\mathbf{T}) = \mathcal{O}$.
29.1.6: $\Lambda \cap V_1$ is a direct summand of Λ, so an $\mathcal{O}$-valued functional on it extends to Λ; then use that the pairing is perfect.
29.1.7: Compute the dual basis.

§29.2.

29.2.1: Subtract a multiple of E_4^3 to kill the constant term; $S_{12} = \mathbb{C}\Delta$.
29.2.2: Compare the coefficients of 1 and q. Then use $\gcd(432000, 691) = 1$.
29.2.3: The projection to $\mathbb{Q}E_k$ is $g \mapsto a_0(g)E_k$, and some $E_4^a E_6^b$ lies in $M_k(\mathbb{Z})$ with constant term 1.
29.2.4: For the first claim use the formula for $a_n(T_m f)$ in [SeA, Ch. VII, §5.3]. For the second, Problem 29.2.2 gives one inclusion; for the other use T_2, T_3 and $\gcd(2073, 176896) = 691$. Here $\tau(2) = -24$ and $\tau(3) = 252$.
29.2.5: For $g = aE_4^3 + b\Delta$, compute the index of $\mathbf{T}_{12}\, g$ in $M_{12}(\mathbb{Z})$ using $(1, 1)$ and $(691, 0)$; note $432000 \equiv 125 \pmod{691}$.

§29.3.

29.3.1: As in Problem 29.2.1, with $S_{24} = \Delta M_{12}$.
29.3.2: By Problem 29.3.1 the first two coefficients of $Ag_1 + Bg_2$ are A, B; a normalized eigenform has $a_1 = 1$ and $a_2 =$ its T_2-eigenvalue [SeA, Ch. VII, §5.4]. One has $a_4(g_1) = 12080128$ and $a_4(g_2) = 1080$.
29.3.3: $\mathbf{T}_{24} \otimes \mathbb{Q} = \mathbb{Q}[T_2]$, and the matrix of T_2 in the basis g_1, g_2 has an entry 1.
29.3.4: Write $t = a + bT_2$ with $a, b \in \mathcal{O}$, and apply Problem 29.1.5. For the direct check, write g_1, g_2 in terms of $f_\pm$.
29.3.5: Write $f_+ - f_-$ in the basis g_1, g_2. For the splitting, reduce D modulo 8 and 3.

§29.4.

29.4.1: Use simultaneous Hecke eigenspaces. For the integral lattice use a basis with $a_i(g_j) = \delta_{ij}$ in the first $\dim S_k$ coefficients, and recall $a_1(f) = 1$. For the example use Problem 29.3.4.
29.4.2: First take $\alpha \neq \beta$ and use the difference of powers: expand a_m^2 as a combination of α^{2m}, w^m and β^{2m}, and sum three geometric series. Both sides of the resulting coefficient identities are polynomials in α, β.

References

[DDT] H. Darmon, F. Diamond and R. Taylor, *Fermat's Last Theorem*, Current Developments in Mathematics **1995** (1995), no. 1, 1–154.

[DS] F. Diamond and J. Shurman, *A First Course in Modular Forms*, Grad. Texts in Math. 228, Springer, 2005.

[Gh] E. Ghate, *An introduction to congruences between modular forms*, in: Current Trends in Number Theory (Allahabad, 2000), Hindustan Book Agency, New Delhi, 2002, 39–58.

[GL] L. Sernau, *GRH for Dirichlet L-functions, in Lean 4*, a shorter rewriting of the Lean proof, text by Claude, `https://github.com/lsernau/grh-lean`, commit `72fead1`, readable edition `grh/`.

[Hi1] H. Hida, *Congruences of cusp forms and special values of their zeta functions*, Invent. Math. **63** (1981), 225–261.

[Hi2] H. Hida, *On congruence divisors of cusp forms as factors of the special values of their zeta functions*, Invent. Math. **64** (1981), 221–262.

[KZ] W. Kohnen and D. Zagier, *Modular forms with rational periods*, in: Modular Forms (Durham, 1983), R. A. Rankin (ed.), Ellis Horwood, Chichester, 1984, 197–249.

[Mn] Yu. I. Manin, *Periods of parabolic forms and p-adic Hecke series*, Math. USSR-Sb. **21** (1973), 371–393.

[PARI] The PARI Group, *PARI/GP*, version 2.17.1, Univ. Bordeaux, `https://pari.math.u-bordeaux.fr/`.

[Ra] R. A. Rankin, *Contributions to the theory of Ramanujan's function $\tau(n)$ and similar arithmetical functions. I, II*, Proc. Cambridge Philos. Soc. **35** (1939), 351–356 and 357–372.

[Ri] K. A. Ribet, *Mod p Hecke operators and congruences between modular forms*, Invent. Math. **71** (1983), 193–205.

[SeA] J.-P. Serre, *A Course in Arithmetic*, Grad. Texts in Math. 7, Springer, 1973.

[Sh] G. Shimura, *On the holomorphy of certain Dirichlet series*, Proc. London Math. Soc. (3) **31** (1975), 79–98.

[Za] D. Zagier, *Modular forms whose Fourier coefficients involve zeta-functions of quadratic fields*, in: Modular Functions of One Variable VI, Lecture Notes in Math. 627, Springer, 1977, 105–169.

EISENSTEIN CONGRUENCES AND SELMER CLASSES

Prerequisites. Modular forms of level 1, Eisenstein series, Δ and the Hecke operators [SeA, Ch. VII]; Serre writes the weight as $2k$ and numbers the Bernoulli numbers differently. Complete discrete valuation rings and Hensel's lemma. The Chebotarev density theorem. From Chapter 26, *Denominators and the Stickelberger element*: the eigenspaces $A^{(i)}$ of Section 26.2 and Theorem 26.2.2. From Chapter 27, *Odd Tate twists*, with $\ell = p$: the groups $G_{\mathbb{Q},p}$, G_p, $\mathrm{Sha}_p(\mathbb{Q}, e)$, Problems 27.1.4 and 27.2.1, Theorem 27.1.1, and the Euler characteristic formula stated before Problem 27.1.7. From Chapter 29, *Congruence modules*: Problem 29.2.2. Galois representations attached to modular forms are stated in Section 30.3 with references.

Chapter 27 computed the length of $\mathrm{Sha}_p(\mathbb{Q}, e)$ for positive odd e from the theorem of Mazur and Wiles, which was used as a black box. How does one produce classes in Sha, and how does one bound them? Ribet's answer to the first question [Ri] is that a cusp form congruent to an Eisenstein series gives a Galois representation that is reducible modulo p, and a good choice of lattice turns it into an unramified class. The subgroup of $\mathrm{Sha}_p(\mathbb{Q}, k-1)$ killed by p has a deformation-theoretic interpretation as a space of tangent vectors at the reducible Eisenstein representation. We work with level 1, and the example to keep in mind is $k = 12$, $p = 691$. Throughout, p is an odd prime, χ is the p-adic cyclotomic character and ω is its reduction modulo p.

30.1. The congruence

For even $k \geq 4$ let $\sigma_{k-1}(n) := \sum_{d|n} d^{k-1}$, and normalize the Eisenstein series as

$$E_k := 1 - \frac{2k}{B_k} \sum_{n \geq 1} \sigma_{k-1}(n)\, q^n,$$

so that E_k has rational coefficients and constant term 1 [SeA, Ch. VII, §4]. Let $\Delta = q \prod_{n \geq 1} (1-q^n)^{24} = \sum \tau(n) q^n$. Since $B_{12} = -691/2730$, the least common denominator of the coefficients of E_{12} is 691. By Problem 29.2.2 of Chapter 29, $691\,(E_4^3 - E_{12}) = 432000\,\Delta$.

Problem 30.1.1. $\tau(n) \equiv \sigma_{11}(n) \pmod{691}$ for all $n \geq 1$.

The same happens whenever p divides B_k/k.

Problem 30.1.2. Let $k \geq 4$ be even, and let p divide the numerator of B_k/k. There is a cusp form g of weight k and level 1 with coefficients in $\mathbb{Z}_{(p)}$ such that $a_n(g) \equiv \sigma_{k-1}(n) \pmod{p}$ for all $n \geq 1$.

Problem 30.1.3. With g as in Problem 30.1.2, for every prime ℓ and every $n \geq 1$,

$$a_n(T_\ell\, g) \equiv (1 + \ell^{k-1})\, a_n(g) \pmod{p}.$$

Date: November 25, 2026.

The cusp forms with coefficients in $\mathbb{Z}_{(p)}$ form a lattice stable under the Hecke operators. By the lifting lemma of Deligne and Serre [DeS, Lemme 6.11], Problem 30.1.3 gives a normalized eigenform f of weight k and level 1, and a prime $\lambda \mid p$ of the field generated by its coefficients, such that

$$a_\ell(f) \equiv 1 + \ell^{k-1} \pmod{\lambda} \qquad \text{for every prime } \ell. \tag{1}$$

In particular $a_p(f) \equiv 1$: f is *ordinary* at λ. For $k = 12$ we may take $f = \Delta$, and $\tau(691) \equiv 1 \pmod{691}$.

30.2. Lattices

A congruence between f and an Eisenstein series says that a Galois representation is reducible modulo λ. Which reduction one sees depends on a lattice. Let K be a finite extension of $\mathbb{Q}_p$ with ring of integers $\mathcal{O}$, uniformizer π, valuation v with $v(\pi) = 1$, and residue field $\mathbb{F}$. Let G be a profinite group and $\rho\colon G \to \mathrm{GL}(V)$ a continuous irreducible representation on a 2-dimensional K-space. A *lattice* is a free $\mathcal{O}$-submodule of rank 2 that spans V.

Problem 30.2.1. G-stable lattices exist.

Suppose that for one, hence (by the Brauer–Nesbitt theorem [CR, (30.16)]) every, G-stable lattice L, the semisimplification of $L/\pi L$ is $\chi_1 \oplus \chi_2$ with characters $\chi_1 \neq \chi_2\colon G \to \mathbb{F}^\times$.

Problem 30.2.2. Choose $\sigma_0 \in G$ with $\chi_1(\sigma_0) \neq \chi_2(\sigma_0)$. Then $\rho(\sigma_0)$ has eigenvalues $\lambda_1, \lambda_2 \in \mathcal{O}$ with $\lambda_i \equiv \chi_i(\sigma_0) \pmod{\pi}$, and every G-stable lattice L has a basis e_1, e_2 with $\rho(\sigma_0)e_i = \lambda_i e_i$.

Fix such L, e_1, e_2, write $\rho(\sigma) = \left(\begin{smallmatrix} a(\sigma) & b(\sigma) \\ c(\sigma) & d(\sigma) \end{smallmatrix}\right)$ in this basis, and put $m := \min_\sigma v(b(\sigma))$, $n := \min_\sigma v(c(\sigma))$. By irreducibility b and c are not identically zero, so m, n are finite. For $r \in \mathbb{Z}$ let $L_r := \pi^r \mathcal{O} e_1 \oplus \mathcal{O} e_2$.

Problem 30.2.3. L_r is G-stable if and only if $-n \le r \le m$, and every G-stable lattice is homothetic to exactly one L_r: the stable lattices form a segment of length $m + n$ in the tree of $\mathrm{PGL}_2(K)$.

Problem 30.2.4. $m+n \ge 1$. On $L_m/\pi L_m$ the group G acts by $\left(\begin{smallmatrix} \chi_1 & * \\ 0 & \chi_2 \end{smallmatrix}\right)$, a nonsplit extension; on $L_{-n}/\pi L_{-n}$ it acts by a nonsplit $\left(\begin{smallmatrix} \chi_1 & 0 \\ * & \chi_2 \end{smallmatrix}\right)$, with sub χ_2 and quotient χ_1; and for $-n < r < m$ it acts by $\chi_1 \oplus \chi_2$.

Problems 30.2.1–30.2.4 prove the following. It is due to Ribet [Ri, Prop. 2.1].

Theorem 30.2.1 (Ribet's lemma)**.** *There is a G-stable lattice on whose reduction G acts by a nonsplit extension* $\left(\begin{smallmatrix} \chi_1 & * \\ 0 & \chi_2 \end{smallmatrix}\right)$.

30.3. The unramified class

We state three inputs. Let f be a normalized cuspidal Hecke eigenform of weight $k \ge 2$ and level 1, let $\lambda \mid p$ be a prime of the field of its coefficients, and let K be the completion at λ.

- (D) There is a continuous $\rho_f\colon G_{\mathbb{Q},p} \to \mathrm{GL}_2(K)$ with $\operatorname{tr}\rho_f(\mathrm{Frob}_\ell) = a_\ell(f)$ and $\det\rho_f = \chi^{k-1}$, for every prime $\ell \neq p$, where Frob_ℓ denotes arithmetic Frobenius [De].
- (I) ρ_f is irreducible [Ri2, §2].

(O) If $a_p(f)$ is a λ-adic unit, then $\rho_f|_{G_p}$ stabilizes a line on which the inertia group I_p acts by χ^{k-1}, and G_p acts on the quotient by an unramified character [Wi, Thm. 2.1.4].

Chapter 32, *Black box: Galois representations of eigenforms*, states the analogue of (D) as a black box, over CM fields; (I) and (O) are not part of it. Its Section 32.3 shows in the simplest case, the eigenform f of weight 2 and level 11, where ρ_f comes from: it is the rational p-adic Tate module of $J_0(11)$, and the Eichler–Shimura relation gives the analogue of (D).

From now on k is even with $4 \le k \le p-3$, p divides B_k (equivalently, since $k < p$, the numerator of B_k/k), and f, λ are as in (1).

Problem 30.3.1. The semisimplification of ρ_f modulo λ is $1 \oplus \omega^{k-1}$, and $1 \ne \omega^{k-1}$ on G_p, and even on I_p.

Apply Theorem 30.2.1 with $\chi_1 = 1$ and $\chi_2 = \omega^{k-1}$, and let $\bar\rho = \left(\begin{smallmatrix} 1 & \bar b \\ 0 & \omega^{k-1} \end{smallmatrix}\right)$ be the resulting reduction.

Problem 30.3.2. $\kappa(\sigma) := \bar b(\sigma)\,\omega^{1-k}(\sigma)$ is a cocycle on $G_{\mathbb{Q},p}$ with values in $\mathbb{F}(\omega^{1-k})$, and its class is not zero.

Problem 30.3.3. The class of κ vanishes on G_p.

Since $H^1(G_{\mathbb{Q},p}, \mathbb{F}(\omega^{1-k})) = H^1(G_{\mathbb{Q},p}, \mathbb{Z}/p(1-k)) \otimes_{\mathbb{F}_p} \mathbb{F}$, and similarly for G_p, Problems 30.3.1–30.3.3, Problem 27.1.4 and Theorem 27.1.1 prove the following.

Theorem 30.3.1 (Ribet)**.** *Let k be even with $4 \le k \le p-3$, and suppose that $p \mid B_k$. Then $\mathrm{Sha}_p(\mathbb{Q}, k-1) \ne 0$, and $A^{(p-k)} \ne 0$.*

This is the converse to Herbrand's theorem [Ri]; see also [Wa, Thm. 6.18]. For $k = 12$ and $p = 691$ the input is Δ. There is an unramified cyclic extension of $\mathbb{Q}(\zeta_{691})$ of degree 691, Galois over $\mathbb{Q}$, with conjugation action on its relative Galois group through $\omega^{-11} = \omega^{679}$. This proves nonvanishing of $\mathrm{Sha}_{691}(\mathbb{Q}, 11)$. Congruences with Eisenstein series are measured by the Eisenstein ideal of the Hecke algebra, which Mazur introduced in weight 2 and prime level [Ma]. In this range Theorem 27.1.2, a consequence of the main conjecture of Iwasawa theory, proved by Mazur and Wiles [MW], gives $\mathrm{length}_{\mathbb{Z}_p} \mathrm{Sha}_p(\mathbb{Q}, k-1) = v_p(B_k/k)$.

30.4. Tangent vectors at the Eisenstein point

Ribet goes from a modular form to a class. Here a congruence produces a nonzero class. How does a class in $\mathrm{Sha}_p(\mathbb{Q}, k-1)[p]$ give a first-order deformation? Let $\rho_0 := 1 \oplus \omega^{k-1} \colon G_{\mathbb{Q},p} \to \mathrm{GL}_2(\mathbb{F}_p)$, the reduction of the representation $1 \oplus \chi^{k-1}$ of the Eisenstein series E_k; we call it the *Eisenstein point*. Let $\mathbb{F}_p[\varepsilon]$ be the ring with $\varepsilon^2 = 0$. A *lift* of ρ_0 is a continuous homomorphism $\rho_\varepsilon \colon G_{\mathbb{Q},p} \to \mathrm{GL}_2(\mathbb{F}_p[\varepsilon])$ that reduces to ρ_0 modulo ε. Let $\mathrm{ad}\,\rho_0$ be the space $M_2(\mathbb{F}_p)$ with σ acting by conjugation by $\rho_0(\sigma)$. See [Mz, §1] for the general theory.

Problem 30.4.1. Writing $\rho_\varepsilon = (1 + \varepsilon M)\rho_0$ identifies the lifts of ρ_0, up to conjugation by matrices $1 + \varepsilon X$, with $H^1(G_{\mathbb{Q},p}, \mathrm{ad}\,\rho_0)$.

The torus $T = \{\mathrm{diag}(1, t)\}$ commutes with ρ_0, and acts on lifts by conjugation.

Problem 30.4.2. $\mathrm{ad}\,\rho_0 = \mathbb{F}_p E_{11} \oplus \mathbb{F}_p E_{22} \oplus \mathbb{F}_p(\omega^{1-k}) E_{12} \oplus \mathbb{F}_p(\omega^{k-1}) E_{21}$, where E_{ij} are the matrix units, and T acts on these four summands, and on their H^1, with weights 0, 0, -1, $+1$.

A cocycle κ with nonzero class in $H^1(G_{\mathbb{Q},p}, \mathbb{F}_p(\omega^{1-k}))$ gives the nonsplit $\rho_\kappa = \left(\begin{smallmatrix} 1 & \kappa\omega^{k-1} \\ 0 & \omega^{k-1} \end{smallmatrix}\right)$. For $t \in \mathbb{F}_p^\times$, conjugating by $\mathrm{diag}(t,1)$ replaces κ by $t\kappa$, so all the $\rho_{t\kappa}$ are isomorphic; at $t=0$ one reaches ρ_0, and to first order at $t=0$ the family is the lift $(1+\varepsilon\kappa E_{12})\rho_0$, of weight -1. This is the sense in which a class is a tangent vector at the Eisenstein point.

Which lifts are allowed? By (O), ρ_f has a line on which I_p acts by χ^{k-1} with unramified quotient. Call a lift ρ_ε *ordinary* if $\mathbb{F}_p[\varepsilon]^2$ has a G_p-stable direct summand L of rank 1, reducing to $\mathbb{F}_p e_2$, on which I_p acts by ω^{k-1}, with I_p acting trivially on the quotient. Let $t_{\mathrm{ord}} \subseteq H^1(G_{\mathbb{Q},p}, \mathrm{ad}\,\rho_0)$ be the set of classes of ordinary lifts, and $t_{\mathrm{ord}}^{(j)}$ its part of weight j.

Problem 30.4.3. The lift with $M = \left(\begin{smallmatrix} \alpha_1 & \beta \\ \gamma & \alpha_2 \end{smallmatrix}\right)$ is ordinary if and only if α_1 and α_2 vanish on I_p and the class of β vanishes in $H^1(G_p, \mathbb{F}_p(\omega^{1-k}))$. Hence $t_{\mathrm{ord}}^{(0)} = 0$, and $t_{\mathrm{ord}}^{(+1)} = H^1(G_{\mathbb{Q},p}, \mathbb{F}_p(\omega^{k-1}))$.

With Problem 27.1.4 and Theorem 27.1.1, Problems 30.4.1–30.4.3 prove the following.

Theorem 30.4.1. $t_{\mathrm{ord}} = t_{\mathrm{ord}}^{(-1)} \oplus t_{\mathrm{ord}}^{(+1)}$, *and* $t_{\mathrm{ord}}^{(-1)} \cong \mathrm{Sha}_p(\mathbb{Q}, k-1)[p] \cong \mathrm{Hom}(A^{(p-k)}, \mathbb{F}_p)$.

Problem 30.4.4. $\dim t_{\mathrm{ord}}^{(+1)} \geq 1$.

In (D) the Hecke eigenvalues at primes $\ell \neq p$ are traces of arithmetic Frobenius.

Problem 30.4.5. Every ordinary lift of ρ_0 to $\mathbb{F}_p[\varepsilon]$ has trace $1+\omega^{k-1}$.

Return to ρ_f with the basis e_1, e_2 of Problem 30.2.2, with $\chi_1 = 1$ and $\chi_2 = \omega^{k-1}$, and let $I \subseteq \mathcal{O}$ be the ideal generated by the products $b(\sigma)c(\tau)$, $\sigma, \tau \in G_{\mathbb{Q},p}$. Following Bellaïche and Chenevier [BC, Ch. 1], we call it the *reducibility ideal*.

Problem 30.4.6. $I = \pi^{m+n}\mathcal{O}$, and a and d are characters of $G_{\mathbb{Q},p}$ modulo I.

Problem 30.4.7. $a \equiv 1$ and $d \equiv \chi^{k-1}$ modulo I. Hence $v(a_\ell(f) - 1 - \ell^{k-1}) \geq m+n$ for every prime $\ell \neq p$.

Problem 30.4.8. For $f = \Delta$ and $p = 691$, $m+n = 1$: up to homothety ρ_Δ has exactly two stable lattices. Moreover $v_{691}(\tau(\ell) - 1 - \ell^{11}) = 1$ for every prime $\ell \leq 37$.

To seek a lower bound on $m+n$ in terms of the trace congruences, one can compare an integral deformation ring with a Hecke algebra. For modularity theorems under ordinary residually reducible hypotheses over $\mathbb{Q}$, see [SW]. For comparison with Problem 30.4.8, Theorem 27.1.2 gives $\mathrm{length}_{\mathbb{Z}_{691}} \mathrm{Sha}_{691}(\mathbb{Q}, 11) = 1$.

Further reading. Chapter 67, *Twists with few congruences*, treats simultaneous twisting, and Chapter 28, *Odd classes by Gauss sums*, treats the bound for odd classes. The Lean proof [GL] gives the projection denominator bound in `Selmer.denominatorLe_clearingBound`, in `grh/src/New/Congruences/FirstOrder/DenominatorBound.lean` and the simultaneous twisting theorem in `Selmer.exists_mFoldTwist_hasDivisibleSelmerLengthLe`, in `grh/src/New/Congruences/Selmer/TwistingTheorem.lean`; here and below Lean names omit the namespace prefix `New.`

30.5. From the CM field to characters

The two results above use Galois representations over the CM field `Data.E` of Chapter 33, *The data*. This field is abelian over $\mathbb{Q}$ by the cyclotomic embedding `Parameters.toCycloField` [GL]. In this section E denotes an arbitrary abelian number field. We consider the strict Selmer group over E and its character components. Problem 27.2.1 treats the cyclotomic case.

Let E be an abelian number field with $\Gamma := \mathrm{Gal}(E/\mathbb{Q})$ of order prime to p. Let $\mathcal{O} := \mathbb{Z}_p[\mu_{|\Gamma|}]$, let $W := W_e \otimes_{\mathbb{Z}_p} \mathcal{O}$ with $W_e = \mathbb{Q}_p/\mathbb{Z}_p(-e)$ as in Chapter 27, and let $G_E \subseteq G_{\mathbb{Q}}$ be the absolute Galois groups. Let $\mathrm{Sha}_p(E,e)_{\mathcal{O}}$ be the group of classes in $H^1(G_E, W)$ that vanish on the inertia group I_w of every place $w \nmid p$ and on the decomposition group D_w of every $w \mid p$. Since $\mathcal{O}$ is free of finite rank over $\mathbb{Z}_p$, continuous cohomology and the restriction maps commute with $\otimes_{\mathbb{Z}_p}\mathcal{O}$, so $\mathrm{Sha}_p(E,e)_{\mathcal{O}} = \mathrm{Sha}_p(E,e) \otimes_{\mathbb{Z}_p} \mathcal{O}$, with $\mathrm{Sha}_p(E,e)$ as in Chapter 27. For a character $\psi\colon \Gamma \to \mathcal{O}^\times$, let $\mathrm{Sha}_p(\mathbb{Q}, e; \psi)_{\mathcal{O}}$ be defined in the same way from $H^1(G_{\mathbb{Q}}, W \otimes \psi^{-1})$. Let Γ act on $\mathcal{O}[\Gamma]$ by left multiplication, so that $G_{\mathbb{Q}}$ acts on it through Γ, and let $\gamma \in \Gamma$ act on $H^1(G_E, W)$ by $(\gamma c)(h) := \tilde{\gamma}\, c(\tilde{\gamma}^{-1} h \tilde{\gamma})$, for any lift $\tilde{\gamma} \in G_{\mathbb{Q}}$ of γ.

Problem 30.5.1. $H^1(G_E, W) \cong H^1(G_{\mathbb{Q}}, \mathcal{O}[\Gamma] \otimes_{\mathcal{O}} W)$, and $\mathcal{O}[\Gamma] \otimes_{\mathcal{O}} W \cong \bigoplus_{\psi} W \otimes \psi$ as $G_{\mathbb{Q}}$-modules, the sum over all characters ψ of Γ.

Problem 30.5.2. Let v be a prime of $\mathbb{Q}$, and $D = D_v$ or I_v. A class of $H^1(G_E, W)$ vanishes on D_w, respectively on I_w, for every place $w \mid v$ of E if and only if its image under Problem 30.5.1 vanishes on D.

Problem 30.5.3. $\mathrm{Sha}_p(E,e)_{\mathcal{O}} \cong \bigoplus_{\psi} \mathrm{Sha}_p(\mathbb{Q}, e; \psi)_{\mathcal{O}}$. The summand $\mathrm{Sha}_p(\mathbb{Q}, e; \psi)_{\mathcal{O}}$, which comes from the summand $W \otimes \psi^{-1}$ of Problem 30.5.1, is the part on which Γ acts through ψ.

Every class killed by p in the ψ-part of $\mathrm{Sha}_p(E,e)_{\mathcal{O}}$ lifts to $H^1(G_{\mathbb{Q}}, \mathbb{F}(\omega^{-e}\bar{\psi}^{-1}))$, with $\mathbb{F}$ the residue field of $\mathcal{O}$. As in §30.4, a cocycle representing this lift gives an upper-triangular deformation of $1 \oplus \omega^e\bar{\psi}$ over $\mathbb{F}[\varepsilon]$, with $\varepsilon^2 = 0$. The deformation allows ramification at p and at primes dividing the conductor of ψ. When the global and local residual invariants vanish, the coefficient maps are injective there and the strict local condition passes to the lift, as in Problem 27.1.4. For $E = \mathbb{Q}$ and positive odd e, Theorem 27.1.2 gives the length $v_p(\mathrm{num}(B_{e+1}/(e+1)))$. For $E \subseteq \mathbb{Q}(\zeta_p)$, write the reduction of ψ as ω^j after inflation to $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$. If $i \equiv -e - j \not\equiv 0 \pmod{p-1}$, Problem 27.2.2 identifies the subgroup killed by p in this summand with $\mathrm{Hom}(A^{(i)}, \mathbb{F}_p)$. For odd $3 \le i \le p-2$, Theorem 26.2.2 gives the order of $A^{(i)}$ and its criterion for nonvanishing. The case $i = 1$ is discussed after Problem 26.2.5.

Hints

§30.1.

30.1.1: Reduce the identity modulo 691, noting $432000 + 65520 = 720 \cdot 691$.
30.1.2: The forms $E_4^a E_6^b$.
30.1.3: Compare the powers of ℓ dividing the indices in the Hecke coefficient formula.

§30.2.

30.2.1: Consider the orbit of a lattice under the compact group $\rho(G)$ in the discrete space of lattices.

30.2.2: Hensel's lemma for the characteristic polynomial. The projector $(\rho(\sigma_0) - \lambda_2)/(\lambda_1 - \lambda_2)$ has entries in $\mathcal{O}$.

30.2.3: By Problem 30.2.2, a stable lattice is the sum of its intersections with Ke_1 and Ke_2. Write ρ in the basis $\pi^r e_1, e_2$.

30.2.4: The only lines stable under $\bar{\rho}(\sigma_0)$ are $\mathbb{F}e_1$ and $\mathbb{F}e_2$. A representation with semisimplification $\chi_1 \oplus \chi_2$ has a stable line.

§30.3.

30.3.1: Chebotarev, Brauer–Nesbitt, and (1). ω maps I_p onto $\mathbb{F}_p^\times$.

30.3.2: Multiply out $\bar{\rho}(\sigma\tau)$. A coboundary can be removed by conjugating with a unipotent upper triangular matrix.

30.3.3: Reduce the line of (O) inside the lattice of Theorem 30.2.1, and compare it with $\mathbb{F}e_1$ under I_p.

§30.4.

30.4.1: Expand $\rho_\varepsilon(\sigma\tau) = \rho_\varepsilon(\sigma)\rho_\varepsilon(\tau)$.

30.4.2: Conjugate each E_{ij} by $\rho_0(\sigma)$ and by $\mathrm{diag}(1, t)$.

30.4.3: A rank-one summand reducing to $\mathbb{F}_p e_2$ is spanned by $e_2 + \varepsilon x e_1$. For the weight 0 part, $\mathbb{Q}$ has no nontrivial extension unramified at every prime.

30.4.4: The Euler characteristic formula of Chapter 27.

30.4.5: Problem 30.4.3.

30.4.6: The upper left entry of $\rho(\sigma\tau)$.

30.4.7: In the basis of L_m, ρ is upper triangular modulo I. Compare the line $(\mathcal{O}/I)e_1$ with the reduction of the line of (O) under I_p. A character of $G_{\mathbb{Q},p}$ unramified at p is trivial. Then use the determinant.

30.4.8: Problems 30.2.4 and 30.4.7 at $\ell = 2$, where $\tau(2) = -24$. The last statement is a finite computation with the product for Δ.

§30.5.

30.5.1: Shapiro's lemma. The elements $|\Gamma|^{-1} \sum_\gamma \psi(\gamma)^{-1}\gamma$ are orthogonal idempotents.

30.5.2: Mackey's formula. The double cosets $D_v \backslash G_\mathbb{Q} / G_E$ correspond to the places of E above v; for I_v each place w occurs $f(w/v)$ times, its residue degree, through conjugates of I_w.

30.5.3: The decomposition of Problem 30.5.1 is $G_\mathbb{Q}$-stable, hence stable under every D. Under Problem 30.5.1, γ acts on $\mathcal{O}[\Gamma] \otimes_\mathcal{O} W$ by right multiplication by γ^{-1} on $\mathcal{O}[\Gamma]$.

References

[BC] J. Bellaïche and G. Chenevier, *Families of Galois representations and Selmer groups*, Astérisque **324** (2009).

[CR] C. W. Curtis and I. Reiner, *Representation Theory of Finite Groups and Associative Algebras*, Interscience, 1962.

[De] P. Deligne, *Formes modulaires et représentations l-adiques*, Séminaire Bourbaki 1968/69, exp. 355, Lecture Notes in Math. 179, Springer, 1971, 139–172.

[DeS] P. Deligne and J.-P. Serre, *Formes modulaires de poids* 1, Ann. Sci. Éc. Norm. Sup. (4) **7** (1974), 507–530.

[GL] L. Sernau, *GRH for Dirichlet L-functions, in Lean 4*, a shorter rewriting of the Lean proof, text by Claude, `https://github.com/lsernau/grh-lean`, commit `72fead1`, readable edition `grh/`.

[Ma] B. Mazur, *Modular curves and the Eisenstein ideal*, Publ. Math. IHÉS **47** (1977), 33–186.

[MW] B. Mazur and A. Wiles, *Class fields of abelian extensions of* $\mathbf{Q}$, Invent. Math. **76** (1984), 179–330.

[Mz] B. Mazur, *Deforming Galois representations*, in: Galois Groups over $\mathbf{Q}$, Math. Sci. Res. Inst. Publ. 16, Springer, 1989, 385–437.

[Ri] K. A. Ribet, *A modular construction of unramified p-extensions of* $\mathbf{Q}(\mu_p)$, Invent. Math. **34** (1976), 151–162.

[Ri2] K. A. Ribet, *Galois representations attached to eigenforms with Nebentypus*, in: Modular Functions of One Variable V, Lecture Notes in Math. 601, Springer, 1977, 17–52.

[SeA] J.-P. Serre, *A Course in Arithmetic*, Grad. Texts in Math. 7, Springer, 1973.

[SW] C. M. Skinner and A. J. Wiles, *Residually reducible representations and modular forms*, Publ. Math. IHÉS **89** (1999), 5–126.

[Wa] L. C. Washington, *Introduction to Cyclotomic Fields*, 2nd ed., Grad. Texts in Math. 83, Springer, 1997.

[Wi] A. Wiles, *On ordinary λ-adic representations associated to modular forms*, Invent. Math. **94** (1988), 529–573.

PSEUDOCHARACTERS AND THE LENGTH BOUND

Prerequisites. Complete local noetherian rings and Hensel's lemma; the Artin–Rees lemma [AM, Cor. 10.10]; lengths of modules. From Chapter 27, *Odd Tate twists*: the groups $G_{\mathbb{Q},p}$, G_p, $\mathrm{Sha}_p(\mathbb{Q}, e)$, Problem 27.1.1 and Theorem 27.1.2. From Chapter 30, *Eisenstein congruences and Selmer classes*: Problem 30.1.1, the congruence (1), the lattices of Section 30.2 (Problems 30.2.1–30.2.4), the inputs (D), (I), (O) of Section 30.3 with Problems 30.3.1 and 30.3.3, Section 30.4, in particular Problems 30.4.6–30.4.8, and Section 30.5.

Section 30.4 of Chapter 30 observed that the Hecke algebra sees a Galois representation only through its traces. The Hecke algebra on the Eisenstein and cuspidal eigenspaces in Problem 31.1.5 has two components. In general the traces in a Hecke algebra need not be realized by a representation over that algebra. What structure do traces alone carry, and how do they measure Sha? The structure is a pseudocharacter; the ideal of products $b \cdot c$ of Chapter 30 can be read off from the traces; and the quotient by it carries extension classes, which bound the congruence from above by the length of a Selmer group. In the eigenform example, the cocycle obeys every linear relation among the matrices $U(g) - 1$ for the twist $U = \chi^{1-k}\rho_f$ (Problem 31.4.1). Theorem 31.4.1 realizes such cocycles by equivariant maps on submodules of families of matrices. Throughout, p is an odd prime.

31.1. Pseudocharacters of dimension two

Let G be a group and R a commutative ring in which 2 is invertible. A *pseudocharacter of dimension* 2 of G with values in R is a pair (T, D) of a function $T\colon G \to R$ and a homomorphism $D\colon G \to R^\times$ such that $T(1) = 2$ and, for all $g, h \in G$,

$$T(gh) = T(hg), \qquad T(gh) + D(g)\,T(g^{-1}h) = T(g)\,T(h).$$

By [Ch, Lemma 1.9] such pairs are the same as Chenevier's determinants of dimension 2. The function T is then a pseudocharacter of dimension 2 in the sense of Taylor [Ta, §1] and Rouquier [Ro], and conversely every such T arises in this way [Ch, Prop. 1.29]; see also [BC, §1.2]. The notion is due to Wiles in dimension two and to Taylor in general [BC, §1.1].

Problem 31.1.1. For every homomorphism $\rho\colon G \to \mathrm{GL}_2(R)$, $(\operatorname{tr}\rho, \det\rho)$ is a pseudocharacter. In particular, so is $(\psi_1+\psi_2, \psi_1\psi_2)$ for any two characters $\psi_1, \psi_2\colon G \to R^\times$.

Problem 31.1.2. If (T, D) is a pseudocharacter, then $D(g) = \frac{1}{2}\big(T(g)^2 - T(g^2)\big)$ and $T(g^{-1}) = D(g)^{-1}T(g)$ for all $g \in G$.

So D is determined by T, and we often write T for the pair.

Problem 31.1.3. Let $R \subseteq R_1 \times R_2$ be a subring in which 2 is invertible, and let (T_i, D_i) be pseudocharacters with values in R_i. If $(T_1(g), T_2(g)) \in R$ for every g, then $((T_1, T_2), (D_1, D_2))$ is a pseudocharacter with values in R.

Date: November 25, 2026.

The first example of a pseudocharacter that is not visibly a trace is the one carried by a Hecke algebra with one Eisenstein and one cuspidal point. Let G be profinite, let $\chi\colon G \to \mathbb{Z}_p^\times$ be a continuous character whose reduction $\bar\chi$ is not trivial, and let $\rho\colon G \to \mathrm{GL}_2(\mathbb{Q}_p)$ be a continuous representation with $\operatorname{tr}\rho(G) \subseteq \mathbb{Z}_p$, $\operatorname{tr}\rho \equiv 1+\chi \pmod p$ and $\operatorname{tr}\rho \neq 1+\chi$. Put

$$e := \min_{g\in G} v_p\big(\operatorname{tr}\rho(g) - 1 - \chi(g)\big), \qquad \mathcal{T}(g) := \big(1+\chi(g), \operatorname{tr}\rho(g)\big) \in \mathbb{Z}_p \times \mathbb{Z}_p.$$

Problem 31.1.4. The $\mathbb{Z}_p$-subalgebra of $\mathbb{Z}_p \times \mathbb{Z}_p$ generated by the $\mathcal{T}(g)$ is $\mathbf{T}_e := \{(u,v) : u \equiv v \pmod{p^e}\}$, and $x \mapsto (0,p^e)$ induces $\mathbb{Z}_p[x]/(x(x-p^e)) \cong \mathbf{T}_e$. The function $\mathcal{T}$ is a pseudocharacter with values in $\mathbf{T}_e$.

The ring $\mathbf{T}_e$ is the *toy Hecke algebra*: $x=0$ is the Eisenstein point, $x=p^e$ the cuspidal point, and e measures how close they are. It occurs in nature.

Problem 31.1.5. The $\mathbb{Z}_{691}$-subalgebra of $\mathrm{End}(M_{12}(\mathbb{Q}) \otimes \mathbb{Q}_{691})$ generated by the Hecke operators T_n, $n \geq 1$, on modular forms of weight 12 and level 1 is isomorphic to $\mathbb{Z}_{691}[x]/(x(x-691))$.

31.2. The reducibility ideal

Let R be a complete local noetherian ring with maximal ideal $\mathfrak{m}$ and residue field $\mathbb{F}$ of characteristic $\neq 2$ (so $2 \in R^\times$), and let (T,D) be a pseudocharacter of G with values in R such that $T \equiv \chi_1 + \chi_2 \pmod{\mathfrak{m}}$ for two distinct characters $\chi_1, \chi_2\colon G \to \mathbb{F}^\times$. Fix $\sigma_0 \in G$ with $\chi_1(\sigma_0) \neq \chi_2(\sigma_0)$.

Problem 31.2.1. The polynomial $X^2 - T(\sigma_0)X + D(\sigma_0)$ has roots $\lambda_1, \lambda_2 \in R$ with $\lambda_i \equiv \chi_i(\sigma_0) \pmod{\mathfrak{m}}$, and $\lambda_1 - \lambda_2 \in R^\times$.

Define $a, d\colon G \to R$ by

$$a(g) := \frac{T(\sigma_0 g) - \lambda_2 T(g)}{\lambda_1 - \lambda_2}, \qquad d(g) := T(g) - a(g).$$

Problem 31.2.2. Suppose that $T = \operatorname{tr}\rho$ for $\rho\colon G \to \mathrm{GL}_2(R)$ with $\rho(\sigma_0) = \mathrm{diag}(\lambda_1,\lambda_2)$, and write $\rho = \left(\begin{smallmatrix} a' & b \\ c & d' \end{smallmatrix}\right)$. Then $a = a'$, $d = d'$, and $a(gh) - a(g)a(h) = b(g)c(h)$.

So a and d are the diagonal entries of a representation that need not exist, and the defect of a from being multiplicative stands in for the products $b(g)c(h)$.

Problem 31.2.3. $a \equiv \chi_1$ and $d \equiv \chi_2 \pmod{\mathfrak{m}}$. In particular $a(g) \in R^\times$.

Problem 31.2.4. $D(g) = a(g)T(g) - a(g^2)$ for every $g \in G$.

The *reducibility ideal* $I \subseteq R$ is the ideal generated by the elements $a(gh) - a(g)a(h)$, $g,h \in G$.

Problem 31.2.5. Modulo I, a and d are characters $G \to (R/I)^\times$, $T \equiv a + d$ and $D \equiv ad$.

Problem 31.2.6. Let $J \subsetneq R$ be an ideal, and let $\psi_1, \psi_2\colon G \to (R/J)^\times$ be characters with $\psi_i \equiv \chi_i \pmod{\mathfrak{m}}$ and $T \equiv \psi_1 + \psi_2 \pmod J$. Then $\psi_1 \equiv a$ and $\psi_2 \equiv d \pmod J$, and $I \subseteq J$.

Problems 31.2.5 and 31.2.6 prove the following; in particular I does not depend on σ_0. Over a henselian local ring in which $d!$ is invertible, Bellaïche and Chenevier give the corresponding reducibility ideal for each partition of the pairwise distinct, absolutely irreducible residual constituents of a d-dimensional pseudocharacter [BC, Prop. 1.5.1].

Theorem 31.2.1. *I is the smallest ideal J of R such that T is congruent modulo J to a sum of two characters lifting χ_1 and χ_2.*

For a representation ρ over a discrete valuation ring as in Section 30.2, Problems 31.2.2 and 30.4.6 give $I = \pi^{m+n}\mathcal{O}$, where $m+n$ is the length of the segment of stable lattices. Return to the toy Hecke algebra.

Problem 31.2.7. In Problem 31.1.4, suppose that ρ is irreducible, and let $m+n$ be the length of its segment of stable lattices (Problem 30.2.3, with $\chi_1 = 1$, $\chi_2 = \bar{\chi}$). Then $m+n \geq e$, and the reducibility ideal of $\mathcal{T}$ is $\{0\} \times p^{m+n}\mathbb{Z}_p = p^{m+n-e}\, x\mathbf{T}_e$.

The *Eisenstein ideal* of a pseudocharacter T with respect to two given characters $\psi_1, \psi_2 \colon G \to R^\times$ is the ideal I_{Eis} generated by the $T(g) - \psi_1(g) - \psi_2(g)$. By Theorem 31.2.1, $I \subseteq I_{\mathrm{Eis}}$ whenever the ψ_i lift the χ_i. In the setting of Chapter 30 the two ideals coincide.

Problem 31.2.8. Let k, p, f, λ be as in Section 30.3, and let $m+n$ be the length of the segment of stable lattices of ρ_f. Then

$$m+n = \min_{\ell \neq p} v\big(a_\ell(f) - 1 - \ell^{k-1}\big),$$

the minimum over primes $\ell \neq p$. So the reducibility ideal of $\operatorname{tr}\rho_f$ equals its Eisenstein ideal for $(1, \chi^{k-1})$.

For Δ and $p = 691$ both sides are 1 (Problem 30.4.8). When $K = \mathbb{Q}_p$, in the toy Hecke algebra built from $\rho = \rho_f$ and χ^{k-1} we get $e = m+n$, and the reducibility ideal is $x\mathbf{T}_e$: the Eisenstein component $\mathbf{T}_e/x\mathbf{T}_e = \mathbb{Z}_p$ is the largest quotient on which $\mathcal{T}$ is reducible.

31.3. The quotient by the reducibility ideal and Ext^1

Ribet's lemma produced a class modulo π. The reducibility ideal produces a class modulo I, which generates a copy of $\mathcal{O}/I$. Keep the notation of Section 30.2, with $\chi_1 \neq \chi_2$, and write ρ in the basis $\pi^m e_1, e_2$ of L_m as $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$. Then the values of b generate $\mathcal{O}$, the values of c generate $I = \pi^{m+n}\mathcal{O}$, and by Problem 31.2.5 the reductions ψ_1, ψ_2 of a, d modulo I are characters. Put $\psi := \psi_1\psi_2^{-1}$.

Problem 31.3.1. $\kappa(g) := b(g)\, d(g)^{-1} \bmod I$ is a cocycle on G with values in $(\mathcal{O}/I)(\psi)$.

Problem 31.3.2. The $\mathcal{O}$-submodule of $H^1(G, (\mathcal{O}/I)(\psi))$ generated by the class of κ is isomorphic to $\mathcal{O}/I$.

Thus the quotient $\mathcal{O}/I$ embeds in a group of extensions of ψ_2 by ψ_1. For two distinct residual characters over a henselian local ring R, Bellaïche and Chenevier construct an injection from $\mathrm{Hom}_R(B, R/I)$ to the algebraic extension group of ψ_2 by ψ_1, where B is the upper right module of a chosen Cayley–Hamilton quotient [BC, Thm. 1.5.5]; for the continuous extension group under additional hypotheses, see [BC, Prop. 1.5.10(ii)]. Now take $G = G_{\mathbb{Q},p}$, and f, λ, $\mathcal{O}$ as in Problem 31.2.8,

so that $\psi \equiv \chi^{1-k} \pmod I$. As in Section 30.5, $\mathrm{Sha}_p(\mathbb{Q}, k-1) \otimes_{\mathbb{Z}_p} \mathcal{O}$ is the group of classes in $H^1(G_{\mathbb{Q},p}, (K/\mathcal{O})(1-k))$ that vanish on G_p. Use the coefficient embedding $(\mathcal{O}/I)(1-k) \hookrightarrow (K/\mathcal{O})(1-k)$, $\bar{a} \mapsto a/\pi^{m+n} + \mathcal{O}$.

Problem 31.3.3. The class of κ vanishes on G_p, and its image in $H^1(G_{\mathbb{Q},p}, (K/\mathcal{O})(1-k))$ generates a submodule isomorphic to $\mathcal{O}/I$. Hence $\mathrm{length}_{\mathcal{O}}\big(\mathrm{Sha}_p(\mathbb{Q}, k-1) \otimes \mathcal{O}\big) \geq m+n$.

This is the direction of Ribet and of Mazur and Wiles [MW], for one eigenform: a congruence of exponent $m+n$ produces a cyclic piece of Sha of that length. For Δ it gives length $\mathrm{Sha}_{691}(\mathbb{Q}, 11) \geq 1$, and Theorem 27.1.2 gives equality. Read the other way, Problem 31.3.3 bounds a congruence by a Selmer group: $m+n \leq \mathrm{length}_{\mathcal{O}}\big(\mathrm{Sha}_p(\mathbb{Q}, k-1) \otimes \mathcal{O}\big)$. In the proof, a Selmer length contributes, in this direction, to the upper bound for the cost of clearing a projection; this is the step of Chapter 65, *Denominators of projections to lifts*, that this chapter serves. In Problem 31.3.3 the class already lies in the kernel of restriction to G_p, so its full length contributes to the lower bound for Sha.

31.4. Cocycles that obey the relations

The proof works with cocycles obeying the simultaneous relations below, and Problem 31.4.1 gives an example. Let Λ be a commutative ring, G a group, X a finite set, and, for $i \in X$, let $U_i \colon G \to M_q(\Lambda)$ be homomorphisms of monoids; let $\varrho \colon G \to M_s(\Lambda)$ be another, and $\alpha \in \Lambda$. Put $\mathcal{N} := M_q(\Lambda)^X$, on which g acts by $(m_i)_i \mapsto (U_i(g)m_i)_i$, and $U(g) - 1 := (U_i(g) - 1)_i \in \mathcal{N}$. A map $\gamma \colon G \to (\Lambda/\alpha)^s$ is a *cocycle for* ϱ if $\gamma(gh) = \gamma(g) + \varrho(g)\gamma(h)$. It *obeys the relations among the* $U(g) - 1$ if, for every finitely supported $\theta \colon G \to \Lambda$,

$$\sum_g \theta(g)\,\big(U(g) - 1\big) = 0 \quad \Longrightarrow \quad \sum_g \theta(g)\,\gamma(g) = 0.$$

If all U_i are trivial, only $\gamma = 0$ obeys them.

Problem 31.4.1. In the setting of Problem 31.3.3, put $\Lambda := \mathcal{O}$, $\alpha := \pi^{m+n}$, $U := \chi^{1-k}\rho_f$ in the basis $\pi^m e_1, e_2$ of L_m (one representation, $q = 2$) and $\varrho := \chi^{1-k}$ ($s = 1$). Then $\kappa(g) = \chi(g)^{1-k} b(g) \bmod I$, and κ is a cocycle for ϱ that obeys the relations among the $U(g) - 1$.

From now on let γ be a cocycle for ϱ that obeys the relations among the $U(g) - 1$, and let $\mathcal{M} \subseteq \mathcal{N}$ be the Λ-span of the $U(g) - 1$, $g \in G$.

Problem 31.4.2. There is a unique Λ-linear map $\phi \colon \mathcal{M} \to (\Lambda/\alpha)^s$ with $\phi(U(g) - 1) = \gamma(g)$ for all g. The module $\mathcal{M}$ is stable under G, and $\phi(gy) = \varrho(g)\phi(y)$ for $y \in \mathcal{M}$.

So the graph of ϕ is a G-stable submodule of $\mathcal{N} \times (\Lambda/\alpha)^s$, with g acting on the second factor through ϱ, on which the first projection is injective. It is usually too small: even over $\mathbb{Z}_p$, $\mathcal{M}$ need not contain $p^j\mathcal{N}$ for any $j \geq 0$. Let Λ be noetherian. By the Artin–Rees lemma [AM, Cor. 10.10], applied to the submodule $\mathcal{M}$ of the finitely generated module $\mathcal{N}$, there is $\nu \geq 1$ with $\mathcal{M} \cap \alpha^\nu \mathcal{N} \subseteq \alpha\mathcal{M}$.

Problem 31.4.3. Let $\mathcal{M} \cap \alpha^\nu \mathcal{N} \subseteq \alpha\mathcal{M}$. Then

$$Y := \big\{ \big(y + \alpha^\nu v,\ \phi(y)\big) : y \in \mathcal{M},\ v \in \mathcal{N} \big\}$$

is a G-stable submodule of $\mathcal{N} \times (\Lambda/\alpha)^s$, the first projection is injective on Y, and $\big(U(g) - 1 + \alpha^\nu v, \gamma(g)\big) \in Y$ for all $g \in G$ and $v \in \mathcal{N}$.

Problem 31.4.4. Let $\Lambda = \mathbb{Z}_p$, $\alpha = p$, $G = \mathbb{Z}$, X a point, $U(j) = \left(\begin{smallmatrix} 1 & jp \\ 0 & 1 \end{smallmatrix}\right)$, $\varrho = 1$ and $\gamma(j) = j \bmod p$. Then γ obeys the relations among the $U(j) - 1$, and the least ν with $\mathcal{M} \cap p^\nu M_2(\mathbb{Z}_p) \subseteq p\mathcal{M}$ is $\nu = 2$. For $\nu = 1$ the set Y of Problem 31.4.3 contains $(0, 0)$ and $(0, 1)$.

Problems 31.4.2 and 31.4.3 prove the following theorem, which is stated as in the proof.

Theorem 31.4.1. *Let Λ be a commutative noetherian ring, $\alpha \in \Lambda$, G a group, X a finite set, and $U_i \colon G \to M_q(\Lambda)$, $i \in X$, and $\varrho \colon G \to M_s(\Lambda)$ homomorphisms of monoids. Let $\gamma \colon G \to (\Lambda/\alpha)^s$ be a cocycle for ϱ that obeys the relations among the $U(g) - 1$. Then there are $\nu \geq 0$ and a G-stable Λ-submodule Y of $M_q(\Lambda)^X \times (\Lambda/\alpha)^s$, with g acting by $\big((m_i)_i, w\big) \mapsto \big((U_i(g)m_i)_i, \varrho(g)w\big)$, such that the first projection is injective on Y and $\big((U_i(g) - 1)_i + \alpha^\nu v, \gamma(g)\big) \in Y$ for all $g \in G$ and all $v \in M_q(\Lambda)^X$.*

If Λ is a discrete valuation ring and $\alpha \neq 0$, the first projection identifies Y with a lattice in $M_q(\Lambda)^X$: its image contains $\alpha^\nu M_q(\Lambda)^X$.
In the Lean formalization. In the Lean proof [GL], Theorem 31.4.1 is `ribetCocycles.exists_graph_subreprese` and the cocycles that obey the relations form `ribetCocycles`, both in `New/Congruences/LocalLoss/Basic.lean` of the readable edition.

Hints

§31.1.

31.1.1: Cayley–Hamilton: $\rho(g) + \det \rho(g)\, \rho(g)^{-1} = \operatorname{tr} \rho(g)$.
31.1.2: Take $h = g$, then $h = 1$.
31.1.3: Problem 31.1.2.
31.1.4: Subtract the scalar $1 + \chi(g)$ from $\mathcal{T}(g)$. Then Problems 31.1.2, 31.1.1 and 31.1.3.
31.1.5: Use the eigenbasis E_{12}, Δ, Problem 30.1.1, and $\tau(2) = -24$.

§31.2.

31.2.1: Hensel's lemma.
31.2.2: Compute $\operatorname{tr}(\rho(\sigma_0)\rho(g))$.
31.2.3: Reduce modulo $\mathfrak{m}$ and use $T(\sigma_0 g) \equiv \chi_1(\sigma_0 g) + \chi_2(\sigma_0 g)$.
31.2.4: Express $T(\sigma_0 g^2)$ by the defining identity with $(g, g\sigma_0)$, and $T(g^2)$ by Problem 31.1.2.
31.2.5: Problems 31.2.3 and 31.2.4.
31.2.6: Problem 31.1.2, and the polynomial of Problem 31.2.1 modulo J.
31.2.7: First, the reduction of a stable lattice has semisimplification $1 \oplus \bar{\chi}$: its trace is $1 + \bar{\chi}$, its determinant is $\bar{\chi}$ by Problem 31.1.2, and Brauer–Nesbitt applies. The roots of Problem 31.2.1 and the function a may be computed in each factor. Use Problem 31.2.2 in the second factor, and note that $\mathbf{T}_e$ projects onto the second factor.
31.2.8: One inequality is Problem 30.4.7. For the other, apply Problem 31.2.6 with J the ideal generated by the $a_\ell(f) - 1 - \ell^{k-1}$, and Chebotarev.

§31.3.

31.3.1: Modulo I the matrix is upper triangular; multiply two of them.

31.3.2: Evaluate at σ_0.

31.3.3: Run Problem 30.3.3 modulo I, as in Problem 30.4.7; $(\mathcal{O}/I)(1-k)$ has no invariants under I_p. Then Problem 27.1.1.

§31.4.

31.4.1: Problem 30.4.7, and the upper right entry of $U(g)$.

31.4.2: Expand $U(gh)-1$ by the cocycle rule.

31.4.3: For injectivity, α kills $(\Lambda/\alpha)^s$.

31.4.4: Compute $\mathcal{M}$ first.

References

[AM] M. F. Atiyah and I. G. Macdonald, *Introduction to Commutative Algebra*, Addison-Wesley, 1969.

[BC] J. Bellaïche and G. Chenevier, *Families of Galois representations and Selmer groups*, Astérisque **324** (2009).

[Ch] G. Chenevier, *The p-adic analytic space of pseudocharacters of a profinite group and pseudorepresentations over arbitrary rings*, in: Automorphic Forms and Galois Representations, Vol. 1, London Math. Soc. Lecture Note Ser. 414, Cambridge Univ. Press, 2014, 221–285; `https://arxiv.org/abs/0809.0415`.

[GL] L. Sernau, *GRH for Dirichlet L-functions, in Lean 4*, a shorter rewriting of the Lean proof, text by Claude, `https://github.com/lsernau/grh-lean`, commit `72fead1`, readable edition `grh/`.

[MW] B. Mazur and A. Wiles, *Class fields of abelian extensions of* $\mathbf{Q}$, Invent. Math. **76** (1984), 179–330.

[Ro] R. Rouquier, *Caractérisation des caractères et pseudo-caractères*, J. Algebra **180** (1996), 571–586.

[Ta] R. Taylor, *Galois representations associated to Siegel modular forms of low weight*, Duke Math. J. **63** (1991), 281–332.

BLACK BOX: GALOIS REPRESENTATIONS OF EIGENFORMS

Prerequisites. Local and global class field theory, including ray class groups and the Chebotarev density theorem [Ne, Ch. V–VI, §VII.13]. Elliptic curves at the level of [Si1, Ch. III, V, §§VII.3–VII.4], and the statement of Tate's uniformization [Si2, Ch. V]; the curve $y^2 = x^3 - x$ as in Chapter 13, *Complex multiplication and reduction at an inert prime*. Modular forms of weight 2 and Hecke operators [DS, Ch. 1–6]. Lattices over a discrete valuation ring. The exercises use the cyclotomic character to illustrate Hodge–Tate weights; crystallinity and potential semistability enter only through the stated theorems. The cited theorems are black boxes for this chapter. Section 32.4 states a theorem of the proof and gives the definitions needed to read it.

32.1. Galois representations over CM fields

What Galois representation does an automorphic representation determine, and at which places can the two be compared?

In this chapter F is any CM field (not the field E of Chapter 33), with maximal totally real subfield F^+ and complex conjugation $x \mapsto \bar{x}$; ℓ is a prime and $\iota\colon \mathbb{C} \cong \overline{\mathbb{Q}}_\ell$ a ring isomorphism ([BLGGT] use its inverse). Let ϵ_ℓ be the ℓ-adic cyclotomic character. A cuspidal automorphic representation π of $\mathrm{GL}_a(\mathbb{A}_F)$ is *polarizable* if $\pi^c \cong \pi^\vee \otimes (\chi \circ N_{F/F^+} \circ \det)$ for a continuous character $\chi\colon \mathbb{A}_{F^+}^\times/(F^+)^\times \to \mathbb{C}^\times$ with $\chi_v(-1) = (-1)^a$ at every real place v, and *regular algebraic* if π_∞ has the infinitesimal character of an irreducible algebraic representation of $\mathrm{Res}_{F/\mathbb{Q}}\mathrm{GL}_a$; see [BLGGT, §2.1]; the pair (π, χ) is then called polarized. For a finite place w with residue field of order q_w and uniformizer ϖ_w, an irreducible representation π_w of $\mathrm{GL}_a(F_w)$ is *unramified* if it has a nonzero vector fixed by $\mathrm{GL}_a(\mathcal{O}_{F_w})$; it is then a subquotient of the normalized induction of the character $b \mapsto \prod_{i=1}^a \chi_i(b_{ii})$ of the upper triangular Borel subgroup, where the χ_i are unramified characters of $F_w^\times$, and its *Satake parameters* are $\chi_1(\varpi_w), \dots, \chi_a(\varpi_w)$.

Theorem 32.1.1. *Let (π, χ) be a regular algebraic polarized cuspidal pair as above. There is a continuous semisimple $r = r_{\ell,\iota}(\pi)\colon G_F \to \mathrm{GL}_a(\overline{\mathbb{Q}}_\ell)$ such that:* (i) $r^c \cong r^\vee \otimes \epsilon_\ell^{1-a} r_{\ell,\iota}(\chi)|_{G_F}$; (ii) *at every finite place $w \nmid \ell$ at which π_w is unramified, r is unramified, and for a geometric Frobenius* Frob_w *the eigenvalues of $r(\mathrm{Frob}_w)$ are $\iota(q_w^{(a-1)/2}\alpha_1), \dots, \iota(q_w^{(a-1)/2}\alpha_a)$, where $\alpha_1, \dots, \alpha_a$ are the Satake parameters of π_w;* (iii) *for every $w \mid \ell$, $r|_{G_{F_w}}$ is potentially semistable, crystalline if π_w is unramified, with Hodge–Tate weights determined by π_∞.*

The construction uses the cohomology of unitary Shimura varieties and, in the generality treated by Chenevier and Harris, also p-adic families [Cl, HT, Shi, CH]. At the ramified places $w \nmid \ell$ the published theorem gives more: the Frobenius-semisimplified Weil–Deligne representation of $r|_{G_{F_w}}$ corresponds, after applying ι^{-1}, to $\pi_w \otimes |\det|_w^{(1-a)/2}$ under the local Langlands correspondence; in this generality this is [BLGGT, Thm. 2.1.1], incorporating results of Taylor–Yoshida and

Date: November 26, 2026.

Caraiani [TY, Car1]. For part (iii) see also [BLGGT, Thm. 2.1.1] and the work cited there, including [Car2]. Section 32.4 states the theorem on Galois representations of eigenforms that the proof establishes for definite unitary groups.

The smallest case is $a = 1$ over an imaginary quadratic field K, where the unitary group is $U(1) := \ker(N\colon \mathrm{Res}_{K/\mathbb{Q}}\mathbb{G}_m \to \mathbb{G}_m)$.

Problem 32.1.1. $U(1)(\mathbb{R})$ is the unit circle. $U(1)(\mathbb{Q}_p) \cong \mathbb{Q}_p^\times$ if p splits in K, and $U(1)(\mathbb{Q}_p)$ is compact otherwise.

Problem 32.1.2. Let ϕ be a character of $\mathbb{A}_K^\times/K^\times$ that is trivial on $\mathbb{A}_\mathbb{Q}^\times$. Then $\phi^c = \phi^{-1}$, and there is exactly one character μ of $U(1)(\mathbb{A})/U(1)(\mathbb{Q})$ such that $\phi(x) = \mu(x/x^c)$ for every $x \in \mathbb{A}_K^\times$. Conversely each such μ gives such a ϕ.

Problem 32.1.3. Let ϕ be a character of $\mathbb{A}_K^\times/K^\times$. If $\phi^c = \phi^{-1}$, then $\phi|_{\mathbb{A}_\mathbb{Q}^\times}$ is either trivial or the quadratic character $\omega_{K/\mathbb{Q}}$.

So the characters with $\phi^c = \phi^{-1}$ fall into two classes, and by Problem 32.1.2 only the first comes from $U(1)$.

32.2. The Hecke character of $\mathbb{Q}(\mathrm{i})$

What is the representation of Theorem 32.1.1 when $a = 1$, and how does it compare with the curve $E\colon y^2 = x^3 - x$? Let $K = \mathbb{Q}(\mathrm{i})$, $\mathcal{O} = \mathbb{Z}[\mathrm{i}]$ and $\mathfrak{f} = (2 + 2\mathrm{i})$.

Problem 32.2.1. Every ideal $\mathfrak{a}$ of $\mathcal{O}$ prime to $1 + \mathrm{i}$ has exactly one generator $\alpha \equiv 1 \pmod{\mathfrak{f}}$. Let $\psi(\mathfrak{a}) := \alpha$. Then ψ is multiplicative, $\psi(\mathfrak{a}^c) = \overline{\psi(\mathfrak{a})}$, and $\psi(\mathfrak{a})\psi(\mathfrak{a}^c) = N\mathfrak{a}$.

For $p \equiv 1 \pmod 4$ and $\mathfrak{p} \mid p$, one has $p + 1 - \#E(\mathbb{F}_p) = \psi(\mathfrak{p}) + \psi(\mathfrak{p}^c)$ [IR, Ch. 18, §4].

Problem 32.2.2. $\psi((1 + 2\mathrm{i})) = -1 - 2\mathrm{i}$ and $\psi((3 + 2\mathrm{i})) = 3 + 2\mathrm{i}$, and $\#E(\mathbb{F}_5) = \#E(\mathbb{F}_{13}) = 8$.

Problem 32.2.3. Let $n \geq 1$. If ideals $\mathfrak{a}, \mathfrak{b}$ prime to 2ℓ have the same class in the ray class group modulo $\mathfrak{f}\ell^n$, then $\psi(\mathfrak{a}) \equiv \psi(\mathfrak{b}) \pmod{\ell^n\mathcal{O}}$.

Combining Problem 32.2.3 with Artin reciprocity for the ray class fields modulo $\mathfrak{f}\ell^n$ gives the following.

Theorem 32.2.1. *There is a continuous character $\psi_\ell\colon G_K \to (\mathcal{O} \otimes \mathbb{Z}_\ell)^\times$, unramified outside 2ℓ, with $\psi_\ell(\mathrm{Frob}_\mathfrak{p}) = \psi(\mathfrak{p})$ for every prime $\mathfrak{p} \nmid 2\ell$, where $\mathrm{Frob}_\mathfrak{p}$ is an arithmetic Frobenius.*

By Problem 32.2.1, $\psi\psi^c$ is the norm. For a $\mathbb{Z}_\ell$-algebra map $\tau\colon \mathcal{O} \otimes \mathbb{Z}_\ell \to \overline{\mathbb{Q}}_\ell$, the character $\tau \circ \psi_\ell$ takes a geometric Frobenius at $\mathfrak{p} \nmid 2\ell$ to $\tau(\psi(\mathfrak{p}))^{-1}$; in Theorem 32.1.1(ii) the corresponding unramified local character takes $\varpi_\mathfrak{p}$ to $\iota^{-1}(\tau(\psi(\mathfrak{p}))^{-1})$. At the places not above ℓ the theorem is then class field theory; the next problem looks at the places above ℓ.

Problem 32.2.4. Let $\ell \equiv 1 \pmod 4$, $\ell = \lambda\bar{\lambda}$, and let $\psi_\lambda\colon G_K \to \mathbb{Z}_\ell^\times$ be ψ_ℓ followed by $\mathcal{O} \otimes \mathbb{Z}_\ell \to \mathcal{O}_\lambda = \mathbb{Z}_\ell$. Then $\psi_\lambda = \epsilon_\ell$ on a subgroup containing a neighborhood of the identity in the inertia group at λ, and ψ_λ has finite image on the inertia group at $\bar{\lambda}$.

So ψ_λ has Hodge–Tate weights 1 and 0 at the two places above ℓ (in the convention where ϵ_ℓ has weight 1), and the polarization appears as $\mathrm{HT}_{\tau c} = 1 - \mathrm{HT}_\tau$.

The automorphism $[\mathrm{i}](x, y) = (-x, \mathrm{i}y)$ of E is defined over K, so $V_\ell(E) := T_\ell(E) \otimes \mathbb{Q}$ is free of rank one over $K \otimes \mathbb{Q}_\ell$, and G_K acts on it through a character $G_K \to (K \otimes \mathbb{Q}_\ell)^\times$.

Since E has good reduction at $\mathfrak{p} \nmid 2$, $V_\ell(E)$ is unramified at $\mathfrak{p} \nmid 2\ell$ [Si1, §VII.4], and an element $\beta \in \mathcal{O}$ acts on $V_\ell(E)$ through $[\beta]$.

Problem 32.2.5. Let $\mathfrak{p} \nmid 2\ell$, and let $\mathrm{Frob}_\mathfrak{p}$ denote an arithmetic Frobenius. If $N\mathfrak{p} = p \equiv 1 \pmod 4$, then $\mathrm{Frob}_\mathfrak{p}$ acts on $V_\ell(E)$ as $\psi(\mathfrak{p})$. If $\mathfrak{p} = (p)$ with $p \equiv 3 \pmod 4$, it acts as $-p = \psi((p))$.

By the Chebotarev density theorem, Problem 32.2.5 proves the following; it is due to Deuring, see [Si2, Ch. II, §10].

Theorem 32.2.2. *The character of G_K on $V_\ell(E)$ is ψ_ℓ.*

Problem 32.2.6. Let $\psi_1, \psi_2 \colon G_K \to \overline{\mathbb{Q}}_\ell^\times$ be ψ_ℓ followed by the two $\mathbb{Z}_\ell$-algebra homomorphisms $\mathcal{O} \otimes \mathbb{Z}_\ell \to \overline{\mathbb{Q}}_\ell$. Then $\psi_2 = \psi_1^c$, $V_\ell(E) \otimes_{\mathbb{Q}_\ell} \overline{\mathbb{Q}}_\ell \cong \mathrm{Ind}_{G_K}^{G_\mathbb{Q}} \psi_1$, and $\mathrm{tr}(\mathrm{Frob}_p \mid V_\ell(E)) = 0$ for $p \equiv 3 \pmod 4$, $p \neq \ell$.

Over $\overline{\mathbb{Q}}_\ell$, the restriction of $V_\ell(E) \otimes_{\mathbb{Q}_\ell} \overline{\mathbb{Q}}_\ell$ to G_K is $\psi_1 \oplus \psi_1^c$, which is reducible. So the weight-two form of E, base changed to K, is not cuspidal, and it enters Theorem 32.1.1 only through ψ, with $a = 1$. For a cuspidal example with $a = 2$ one needs a curve without complex multiplication by K. We take $X_0(11)$ and stay over $\mathbb{Q}$; its form has no complex multiplication, hence no quadratic self-twist, so its base change to K is cuspidal [AC, Ch. 3], and the local questions are the same.

32.3. Eichler–Shimura for $X_0(11)$

How does one get Frobenius eigenvalues out of the cohomology of a Shimura variety, and what does each method give? Let

$$f = q \prod_{n \geq 1} (1 - q^n)^2 (1 - q^{11n})^2 = \sum_{n \geq 1} a_n q^n,$$

the normalized eigenform spanning $S_2(\Gamma_0(11))$ [DS]. The curve $X_0(11)$ has genus one and the model $E \colon y^2 + y = x^3 - x^2 - 10x - 20$ over $\mathbb{Q}$, with good reduction away from 11 (LMFDB, curve 11.a2, `https://www.lmfdb.org/EllipticCurve/Q/11/a/2`). For $p \neq 11$, the Hecke operator T_p acts on $E = J_0(11)$ as $[a_p]$, and by the Eichler–Shimura relation [DS, Thm. 8.7.2], [Sh, Thm. 7.9], the reduction of T_p modulo p is $F + V$, where F is the Frobenius endomorphism and $FV = VF = p$.

Problem 32.3.1. $a_2 = -2$, $a_3 = -1$, $a_5 = 1$, $a_7 = -2$, $a_{11} = 1$, $a_{13} = 4$.

Problem 32.3.2. For $p \notin \{11, \ell\}$, the arithmetic Frobenius at p on $V_\ell(E)$ satisfies $\mathrm{Frob}_p^2 - a_p \mathrm{Frob}_p + p = 0$.

For $p \notin \{11, \ell\}$, the arithmetic Frobenius at p has determinant p on $V_\ell(E)$, by the Weil pairing [Si1, §III.8], and $\#E(\mathbb{F}_{p^k}) = p^k + 1 - \mathrm{tr}(\mathrm{Frob}_p^k \mid V_\ell(E))$ for $k \geq 1$ [Si1, §V.2].

Problem 32.3.3. Let $\Phi \in \mathrm{GL}_2(\overline{\mathbb{Q}}_\ell)$ satisfy $\Phi^2 - a\Phi + p = 0$ with $a \in \mathbb{Z}$, and let $\det \Phi = p$. Then the characteristic polynomial of Φ is $X^2 - aX + p$. Hence, taking $\ell \neq p$, $\#E(\mathbb{F}_p) = p + 1 - a_p$ for $p \neq 11$.

The relation of Problem 32.3.2 kills Frobenius; it does not give the multiplicities of its roots. In dimension two the determinant supplies them. In dimension three, $\mathrm{diag}(\alpha,\alpha,\beta)$ and $\mathrm{diag}(\alpha,\beta,\beta)$ are killed by the same quadratic polynomial. In the cohomological construction, counts of points give traces of powers of Frobenius, following Langlands and Kottwitz [Ko]. The simplest instance is the trace formula for $\#E(\mathbb{F}_{p^k})$ stated before Problem 32.3.3.

Problem 32.3.4. $\#E(\mathbb{F}_p) = p + 1 - a_p$ for $p = 2, 3, 5, 7, 13$ by direct count. For $p \notin \{11, \ell\}$, the numbers $\#E(\mathbb{F}_p)$ and $\#E(\mathbb{F}_{p^2})$ determine the characteristic polynomial of the arithmetic Frobenius on $V_\ell(E)$; for $p = 2$ both equal 5.

At 11 the curve has split multiplicative reduction. By Tate's uniformization [Si2, Ch. V], E is uniformized over $\mathbb{Q}_{11}$ by $\mathbb{G}_m/q^{\mathbb{Z}}$ for some nonzero $q \in 11\mathbb{Z}_{11}$, and the exact sequence $0 \to \mathbb{Z}_\ell(1) \to T_\ell(E) \to \mathbb{Z}_\ell \to 0$ has extension class given by the Kummer class of q.

Problem 32.3.5. For $\ell \neq 11$, the inertia group at 11 acts on $V_\ell(E)$ through a nontrivial group of unipotent matrices; in particular $V_\ell(E)$ is ramified at 11.

So the place 11 is not of the kind covered by Theorem 32.1.1(ii); the finer compatibility there, through the Weil–Deligne representation, is due to Carayol [Ca]. The next section asks what survives if one compares only at unramified places.

32.4. Hecke polynomials on a definite unitary group

The input to Theorem 32.1.1 is a representation of $\mathrm{GL}_a(\mathbb{A}_F)$. Theorem 32.4.1 starts with forms on the unitary group of the standard definite hermitian space. What does an eigenform there determine at a split place, and in what sense is it compared with Frobenius?

Let F be a CM field, $n \geq 1$, and

$$G_f := \{g \in \mathrm{GL}_n(\mathbb{A}_{F,f}) : \bar{g}^T g = 1\}, \qquad \mathcal{K}_0 := G_f \cap \mathrm{GL}_n(\widehat{\mathcal{O}}_F).$$

For a finite place w of F, let q_w be the order of its residue field, ϖ_w a uniformizer of F_w, and $\mathcal{K}_w$ the group of $k \in \mathcal{K}_0$ whose components at all places other than $w, \bar{w}$ are 1. Let w be *split*, $\bar{w} \neq w$. For $a \in \mathrm{GL}_n(F_w)$ let $b_w(a) \in G_f$ have component a at w, $(\bar{a}^T)^{-1}$ at $\bar{w}$ and 1 elsewhere. For $j \geq 0$ let

$$D_j := \{a \in \mathrm{GL}_n(F_w) : a \text{ and } \varpi_w a^{-1} \text{ have entries in } \mathcal{O}_w,\ \mathrm{ord}_w \det a = j\}.$$

For a function ϕ on G_f fixed by $\mathcal{K}_w$ under right translation, the Hecke operator is $(T_{w,j}\phi)(g) := \sum_a \phi(g\, b_w(a))$, the sum over a in a set of representatives of $D_j/\mathrm{GL}_n(\mathcal{O}_w)$. For $q, N \in \mathbb{N}$ and $t\colon \mathbb{N} \to \mathbb{C}$ put

$$H(q, N, t) := \sum_{j=0}^{N} (-1)^j q^{\binom{j}{2}}\, t(j)\, X^{N-j}.$$

A function ϕ on G_f with values in a finite-dimensional complex vector space *has Hecke polynomial* $Q \in \mathbb{C}[X]$ at the split place w if ϕ is fixed by $\mathcal{K}_w$ and there is $t\colon \mathbb{N} \to \mathbb{C}$ with $Q = H(q_w, n, t)$ and $T_{w,j}\phi = t(j)\phi$ for every $j \in \mathbb{N}$.

Problem 32.4.1. The map $a \mapsto a\mathcal{O}_w^n/\varpi_w\mathcal{O}_w^n$ is a bijection from $D_j/\mathrm{GL}_n(\mathcal{O}_w)$ onto the subspaces of codimension j of $\mathbb{F}_{q_w}^n$. Hence $D_j = \emptyset$ for $j > n$, $D_n = \varpi_w \mathrm{GL}_n(\mathcal{O}_w)$, and D_1 is the union of $q_w + 1$ cosets when $n = 2$.

Problem 32.4.2. Let $n = 1$. Then $T_{w,0}\phi = \phi$, $(T_{w,1}\phi)(g) = \phi(g\, b_w(\varpi_w))$ and $T_{w,j}\phi = 0$ for $j \geq 2$. A nonzero ϕ fixed by $\mathcal{K}_w$ has a Hecke polynomial at w if and only if $\phi(g\, b_w(\varpi_w)) = t_1\phi(g)$ for a constant t_1 and all g, and then the polynomial is $X - t_1$.

Problem 32.4.3. $H(q, 2, t) = t(0)X^2 - t(1)X + q\, t(2)$. If $q \geq 1$, $\beta_1, \ldots, \beta_N \in \mathbb{C}$, and $t(j) = q^{-\binom{j}{2}} e_j(\beta_1, \ldots, \beta_N)$ for $0 \leq j \leq N$, with e_j the elementary symmetric polynomials, then $H(q, N, t) = \prod_{i=1}^{N}(X - \beta_i)$.

Away from ℓ, the split-place clause of Theorem 32.4.1 below evaluates the local polynomial on a *geometric* Frobenius, whose inverse acts on the residue field by $x \mapsto x^{q_w}$. For $E = X_0(11)$ and $p \notin \{11, \ell\}$, taking $t = (1, a_p, 1, 0, 0, \ldots)$ gives $H(p, 2, t) = X^2 - a_p X + p$, which kills the arithmetic Frobenius on $V_\ell(E)$ by Problem 32.3.2.

Problem 32.4.4. Let $\Phi \in \mathrm{GL}(V)$ satisfy $\Phi^2 - a\Phi + p = 0$, and let $\mathrm{GL}(V)$ act on the dual $V^\vee$ by $g \mapsto (g^{-1})^T$. Then Φ^{-1} acts on $V^\vee$ by a matrix that satisfies the same equation. So for $p \notin \{11, \ell\}$, $X^2 - a_p X + p$ kills the geometric Frobenius at p on $V_\ell(E)^\vee$.

In rank one the forms of trivial weight are the complex-valued functions on $G_f = \{x \in \mathbb{A}_{F,f}^\times : x\bar{x} = 1\}$ that are invariant under $U(1)(F^+) := \{\gamma \in F^\times : \gamma\bar{\gamma} = 1\}$, embedded diagonally, and whose stabilizer under right translation contains a neighborhood of the identity.

Problem 32.4.5. Let $n = 1$ and let μ be a character of G_f, trivial on $U(1)(F^+)$, whose kernel contains a neighborhood of the identity. Then μ is a form of trivial weight, and at every split w with $\mu(b_w(\mathcal{O}_w^\times)) = 1$ it has Hecke polynomial $X - \mu(b_w(\varpi_w))$. Here $b_w(x)$ has components x at w and $\bar{x}^{-1}$ at $\bar{w}$.

For an eigenform, all but finitely many places of prime norm must be split and admit the prescribed Hecke polynomial.

Problem 32.4.6. In $\mathbb{Q}(\mathrm{i})$ the place $(1+\mathrm{i})$ has norm 2 and is fixed by conjugation. If a CM field F contains a root of unity of exact order 5040, then every finite place v of F with q_v prime is split.

A homomorphism r from a group Γ to $\mathrm{GL}_n(k)$, k a field, is *trace-nondegenerate* if every z in the k-span of $r(\Gamma)$ with $\mathrm{tr}(z\, r(h)) = 0$ for all $h \in \Gamma$ is 0.

Problem 32.4.7. Every character $\Gamma \to k^\times$ is trace-nondegenerate. The homomorphism $r\colon \mathbb{Z} \to \mathrm{GL}_2(k)$, $m \mapsto \left(\begin{smallmatrix} 1 & m \\ 0 & 1 \end{smallmatrix}\right)$, is not trace-nondegenerate.

The statement used in the proof. Fix ℓ and ι as in Section 32.1, an algebraic closure $\overline{\mathbb{Q}}$, and a CM field F with an embedding $F \to \overline{\mathbb{Q}}$ and a CM type $\Phi = (\Phi_v)_{v|\infty}$, an embedding $\Phi_v\colon F \to \mathbb{C}$ inducing each infinite place v. Let $G_F = \mathrm{Gal}(\overline{\mathbb{Q}}/F)$. Assume F contains a root of unity of exact order 5040. *Weil data* on such a field consist of an element $\jmath \in F$ with $\bar{\jmath} = -\jmath$, $\mathrm{Im}\,\Phi_v(\jmath) > 0$ for every $v \mid \infty$, and $(1 - \jmath^{-1})/2$ integral; a finite idele α with $\mathrm{ord}_w(\jmath\alpha\bar{\alpha}) = -\mathrm{ord}_w(\mathfrak{D}_{F/\mathbb{Q}})$ at every finite w, $\mathfrak{D}_{F/\mathbb{Q}}$ the different; and a continuous character υ of $\mathbb{A}_F^\times/F^\times$ with values of absolute value 1, such that $\upsilon(x) = \prod_{v|\infty} x_v/|x_v|$ whenever the finite part of x lies in $\widehat{\mathcal{O}}_F^\times$ (with $x_v \in \mathbb{C}^\times$ through Φ_v), $\upsilon(\bar{x}) = \upsilon(x)^{-1}$ for all x, and $\upsilon(\varpi_w) = -1$ at every w with $\bar{w} = w$ (ϖ_w placed at w, 1 elsewhere).

In this chapter a *weight* $\kappa = (c, e)$ is the weight of a form (not the weight of a place of Chapter 33): functions $c_v \colon \mathbb{N} \to \mathbb{N}$ and integers e_v, for $v \mid \infty$. Let W_κ be the tensor product over v of the representations of $\mathrm{GL}_n(\mathbb{C})$ with $c_v(h)$ columns of height h, $0 \le h < n$, twisted by $\det^{e_v}$, written in coordinates through Schur matrices in chosen bases of tableaux, and let $U(F^+) := \{\gamma \in \mathrm{GL}_n(F) : \bar{\gamma}^T \gamma = 1\}$ act on it through the complex conjugates of the $\Phi_v(\gamma)$. A *form of weight* κ is a function $f \colon G_f \to W_\kappa$ whose stabilizer under right translation contains a neighborhood of the identity and which satisfies $f(\gamma g) = \gamma \cdot f(g)$ for $\gamma \in U(F^+)$, embedded diagonally, and $g \in G_f$. For a family $P = (P_v)$ of polynomials in $\mathbb{C}[X]$ indexed by the finite places of F, f is an *eigenform for* P if $f \neq 0$ and, for all but finitely many finite places v, if q_v is prime then v is split and f has Hecke polynomial P_v at v.

A *Frobenius datum* (v, A, s) is a finite place v of F with q_v prime, a valuation ring A of $\overline{\mathbb{Q}}$ lying over v (an $x \in \mathcal{O}_F$ is in the maximal ideal of A exactly when $x \in v$), and $s \in G_F$ such that s^{-1} stabilizes A and induces $x \mapsto x^{q_v}$ on its residue field. A set Y of Frobenius data contains *most Frobenius data* if each nonempty member $\mathcal{U}$ of the topology of G_F contains a nonempty member $\mathcal{U}'$ of that topology such that, for all but finitely many v, Y contains every datum (v, A, s) with $s \in \mathcal{U}'$. A homomorphism $r \colon G_F \to \mathrm{GL}_n(\overline{\mathbb{Q}}_\ell)$ is *attached to* P if it is continuous and trace-nondegenerate, and for every real $\eta > 0$ the set of Frobenius data (v, A, s) for which every coefficient of $\det(X - r(s)) - \iota P_v$ has ℓ-adic absolute value at most η contains most Frobenius data; here ιP_v is P_v with ι applied to its coefficients.

Theorem 32.4.1. *Let F have Weil data, let $n \ge 1$, and let w be a finite place of F with $w \nmid \ell$. For every family P, every weight κ and every form f of weight κ that is an eigenform for P:*

(a) *some $r \colon G_F \to \mathrm{GL}_n(\overline{\mathbb{Q}}_\ell)$ is attached to P;*
(b) *for every r attached to P, if f is fixed by $\mathcal{K}_w$, then for every valuation ring A of $\overline{\mathbb{Q}}$ over w:*
  (i) *r is trivial on the inertia group of A;*
  (ii) *if w is split, then for every $Q \in \mathbb{C}[X]$ such that f has Hecke polynomial Q at w, and every $s \in G_F$ such that s^{-1} stabilizes A and induces $x \mapsto x^{q_w}$ on its residue field, $(\iota Q)(r(s)) = 0$.*

The full theorem gives (a) for every finite place w. At $w \mid \ell$, if f is fixed by $\mathcal{K}_w$, it gives crystallinity and the Hodge–Tate jumps determined by κ for each attached r at each A over w. At a split such w, a local Hecke polynomial also gives a condition on a crystalline Frobenius. We omit the precise statements at $w \mid \ell$. In (b)(ii), ιQ kills $r(s)$. This alone does not determine the multiplicities in the characteristic polynomial (compare $\mathrm{diag}(\alpha, \alpha, \beta)$ in Section 32.3).

In the Lean formalization. Theorem 32.4.1 is the case $w \nmid \ell$ of `GaloisRep.sphericalCompat_std` of the Lean proof [GL] (names omit the namespace `New`), with conclusion `GaloisRep.SphericalCompat`; its local conclusion at each A over w is `GaloisRep.IsCompatibleAt`, which at $w \nmid \ell$ reduces to (i) and (ii). The Lean proof obtains the theorem by lifting f along two characters to rank $2n + 1$, attaching a representation to each lift, twisting each, and cancelling the $n + 1$ extra characters on each side.

Problem 32.4.8. Let $n = 1$, $\kappa = (0, 0)$ (that is, $c_v = 0$ and $e_v = 0$ for all v, so $W_\kappa = \mathbb{C}$), and let F contain a root of unity of exact order 5040. The constant function $f = 1$ is a form of weight κ and an eigenform for $P_v = X - 1$ (all v), and

the trivial homomorphism $r = 1$ is attached to P. At every split $w \nmid \ell$ and for every s as in Theorem 32.4.1(b)(ii), $(\iota Q)(r(s)) = 0$ for $Q = X - 1$.

Problem 32.4.9. Let F have Weil data, let f be a form that is an eigenform for P, and let r be attached to P. Then the set of Frobenius data (v, A, s) with $(\iota P_v)(r(s)) = 0$ contains most Frobenius data.

Thus $(\iota P_v)(r(s)) = 0$ for most Frobenius data (v, A, s): the Hecke polynomial kills Frobenius. This is the step that the last part, from Chapter 33 on, takes from this chapter.

Hints

§32.1.

32.1.1: $K \otimes \mathbb{Q}_p$ is $\mathbb{Q}_p \times \mathbb{Q}_p$ or a field.

32.1.2: Hilbert's Theorem 90 for K and for each $K \otimes \mathbb{Q}_v$, and for the units at the unramified places.

32.1.3: ϕ is trivial on $\mathbb{Q}^\times$ and on the norms xx^c; use $\mathbb{A}_{\mathbb{Q}}^\times/\mathbb{Q}^\times N(\mathbb{A}_K^\times) \cong \mathbb{Z}/2$.

§32.2.

32.2.1: The units $\pm 1, \pm \mathrm{i}$ map bijectively onto $(\mathcal{O}/\mathfrak{f})^\times$, which has order 4; and $\mathfrak{f}^c = \mathfrak{f}$.

32.2.3: Write $\mathfrak{a} = \mathfrak{b}(\beta)$ with $\beta \equiv 1 \pmod{{}^\times \mathfrak{f}\ell^n}$; compare $\beta\,\psi(\mathfrak{b})$ with the primary generator of $\mathfrak{a}$.

32.2.4: Approximate $u \in 1 + \ell^m\mathbb{Z}_\ell$ at λ by Gaussian integers $\equiv 1$ at $\bar{\lambda}$ and modulo a high power of $1 + \mathrm{i}$; local reciprocity, normalized as in Theorem 32.2.1.

32.2.5: In the split case use the action on the invariant differential to distinguish the two primes over p, and the trace to distinguish unit multiples. In the inert case compare Frobenius over $\mathbb{F}_{p^2}$ with Frobenius over $\mathbb{F}_p$.

32.2.6: Complex conjugation acts on $V_\ell(E)$ and anticommutes with [i].

§32.3.

32.3.1: Expand the product to order q^{13}.

32.3.2: Multiply $T_p = F + V$ by F, and use that Frob_p acts on T_ℓ of the reduction as F.

32.3.3: Cayley–Hamilton.

32.3.4: In $\mathbb{F}_4$, the equation becomes $y^2 + y = x^3 + x^2$. Use $\alpha^2 + \beta^2 = (\alpha + \beta)^2 - 2\alpha\beta$.

32.3.5: Kummer theory for the extensions $\mathbb{Q}_{11}^{\mathrm{ur}}(q^{1/\ell^n})$; $v_{11}(q) \neq 0$.

§32.4.

32.4.1: The lattice $a\mathcal{O}_w^n$ determines the coset $a\mathrm{GL}_n(\mathcal{O}_w)$; it lies between $\varpi_w\mathcal{O}_w^n$ and $\mathcal{O}_w^n$, with index q_w^j in $\mathcal{O}_w^n$.

32.4.2: Problem 32.4.1 with $n = 1$.

32.4.3: Expand the product and compare coefficients.

32.4.4: Transpose the equation for Φ.

32.4.5: $\mathcal{K}_w = b_w(\mathcal{O}_w^\times)$, and μ is multiplicative.

32.4.6: If $\bar{v} = v$, conjugation induces an automorphism of the residue field $\mathbb{F}_p$; take a root ζ of order 5040 and consider $\zeta^2 - 1$; $1 - \zeta^2$ is a unit because 2520 is not a prime power.

32.4.7: For a character the span is k. For the second assertion, consider $r(1) - r(0)$.

32.4.8: Problems 32.4.2, 32.4.6 and 32.4.7.

32.4.9: Theorem 32.4.1(b)(ii) at $w = v$, $Q = P_v$, away from finitely many places.

References

[AC] J. Arthur and L. Clozel, *Simple Algebras, Base Change, and the Advanced Theory of the Trace Formula*, Ann. of Math. Stud. 120, Princeton Univ. Press, 1989.

[BLGGT] T. Barnet-Lamb, T. Gee, D. Geraghty and R. Taylor, *Potential automorphy and change of weight*, Ann. of Math. (2) **179** (2014), 501–609.

[Ca] H. Carayol, *Sur les représentations ℓ-adiques associées aux formes modulaires de Hilbert*, Ann. Sci. Éc. Norm. Sup. (4) **19** (1986), 409–468.

[Car1] A. Caraiani, *Local–global compatibility and the action of monodromy on nearby cycles*, Duke Math. J. **161** (2012), 2311–2413.

[Car2] A. Caraiani, *Monodromy and local–global compatibility for $l = p$*, Algebra Number Theory **8** (2014), 1597–1646.

[CH] G. Chenevier and M. Harris, *Construction of automorphic Galois representations, II*, Camb. J. Math. **1** (2013), 53–73.

[Cl] L. Clozel, *Représentations galoisiennes associées aux représentations automorphes autoduales de* GL(n), Publ. Math. IHÉS **73** (1991), 97–145.

[DS] F. Diamond and J. Shurman, *A First Course in Modular Forms*, Grad. Texts in Math. 228, Springer, 2005.

[GL] L. Sernau, *GRH for Dirichlet L-functions, in Lean 4*, a shorter rewriting of the Lean proof, text by Claude, `https://github.com/lsernau/grh-lean`, commit `72fead1`, readable edition `grh/`.

[HT] M. Harris and R. Taylor, *The Geometry and Cohomology of Some Simple Shimura Varieties*, Ann. of Math. Stud. 151, Princeton Univ. Press, 2001.

[IR] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, 2nd ed., Grad. Texts in Math. 84, Springer, 1990.

[Ko] R. E. Kottwitz, *Points on some Shimura varieties over finite fields*, J. Amer. Math. Soc. **5** (1992), 373–444.

[Ne] J. Neukirch, *Algebraic Number Theory*, Grundlehren Math. Wiss. 322, Springer, 1999.

[Sh] G. Shimura, *Introduction to the Arithmetic Theory of Automorphic Functions*, Princeton Univ. Press, 1971.

[Shi] S. W. Shin, *Galois representations arising from some compact Shimura varieties*, Ann. of Math. (2) **173** (2011), 1645–1741.

[Si1] J. H. Silverman, *The Arithmetic of Elliptic Curves*, 2nd ed., Grad. Texts in Math. 106, Springer, 2009.

[Si2] J. H. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*, Grad. Texts in Math. 151, Springer, 1994.

[TY] R. Taylor and T. Yoshida, *Compatibility of local and global Langlands correspondences*, J. Amer. Math. Soc. **20** (2007), 467–493.

THE DATA

Prerequisites. Cyclotomic fields: the degree of $\mathbb{Q}(\zeta_n)$, the splitting of primes in it, and the conductor–discriminant formula [Wa, Ch. 2–3]. The discriminant in a tower [Ne, Ch. III, §2]; finiteness of the class group [Ne, Ch. I, §6]. Quadratic reciprocity [IR, Ch. 5]. Chebyshev's function satisfies $\psi(u) \le 2u$ for $u \ge 1$ [RS, Thm. 12]. From the earlier chapters: the character χ_K and the weight $1 - \chi_K$ (Chapter 2), the infinite places of the CM field of Chapter 3 and the prime sums over them, sparse sets of places (Chapter 4), and the chain of $m \approx \sqrt{x}$ steps (Chapter 8).

Every later chapter of this part works with one collection of objects: two integers q_0 and d, a CM field E obtained by adjoining a root of unity to $\mathbb{Q}(\sqrt{-d})$, three scales $x < x_1 < b$, the number m of lifts, the ranks r and k and the step size t, a set of places of E with weights, and three large primes. This chapter lists them, checks that their sizes fit together, defines the direction amount, the main amount and the total remainder used in the later bounds, and states that such data exist for every large integer x. The spaces, forms and twists that the later chapters attach to the data are fixed in Chapter 34, *Spaces, forms and twists*. We write log for the natural logarithm.

33.1. The modulus and the prime d

How must d be chosen so that every prime dividing q_0 splits in $K = \mathbb{Q}(\sqrt{-d})$?

Definition 33.1.1. *Parameters* are natural numbers q_0 and d with $18480 \mid q_0$, d prime, $q_0 \mid 2(d+1)$ and $q_0 \nmid d+1$.

Let $K := \mathbb{Q}(\sqrt{-d}) \subset \mathbb{C}$, and let $\chi_K(n) := \left(\frac{n}{d}\right)$ be the Legendre symbol.

Problem 33.1.1. $18480 = 2^4 \cdot 3 \cdot 5 \cdot 7 \cdot 11$. Parameters satisfy $q_0 \ne 0$, $d \equiv q_0/2 - 1 \pmod{q_0}$ and $d \equiv 7 \pmod 8$. For $q_0 = 18480$ the least admissible d is 9239, and $\varphi(18480) = 3840$.

Problem 33.1.2. Let c, s be nonnegative integers. (i) Every prime $p \mid 3^c 2^s q_0$ divides $(d+1)/4$, and $\chi_K(p) = 1$. (ii) A prime p with $\chi_K(p) \ne 1$ satisfies $p \ge 13$.

Since $d \equiv 3 \pmod 4$, χ_K is the character of K (Problem 2.1.1), so the primes of Problem 33.1.2(i) split in K. For $d = 9239$ the least prime p with $\chi_K(p) = -1$ is 19.

33.2. The field and its places

For a nonnegative integer s let $\lfloor \log_3 s \rfloor$ be the floor logarithm (zero for $s = 0$), and

$$l_0(s) := 3^{\lfloor \log_3 s \rfloor + 4}, \qquad T(s) := 3^{\lfloor \log_3 s \rfloor + 5}\, 2^s, \qquad q_1 := q_0 T(s), \qquad q_2 := (q_0 d)^{s+6}.$$

Let $E = E_s := K(\zeta_{q_1})$, with ζ_{q_1} a primitive q_1-th root of unity, let Φ be the set of infinite places of E, $f := \#\Phi$, and let $\mathrm{rd}_E := |\mathrm{disc}\, E|^{1/[E:\mathbb{Q}]}$ be the root discriminant.

Date: November 26, 2026.

Fix an embedding $E \to \mathbb{C}$ over K. Composing it with the elements of $\mathrm{Gal}(E/K)$ gives a bijection between $\mathrm{Gal}(E/K)$ and Φ, through which Φ becomes a group; sending g to the unit u with $g(\zeta_{q_1}) = \zeta_{q_1}^u$ identifies it with $(\mathbb{Z}/q_1)^\times$. For $\nu \in \mathbb{Z}$ let $[\nu] \in \Phi$ be the place of $\nu \bmod q_1$ if $\gcd(\nu, q_1) = 1$, and the identity otherwise. The *class* of $\tau \in \Phi$ modulo $n \mid q_1$ is its image in $(\mathbb{Z}/n)^\times$. Let Φ_a be the set of places of class 1 modulo q_0.

Problem 33.2.1. $T(s) = 3l_0(s)2^s$, and $27s < l_0(s)$; if $s \geq 1$, then $l_0(s) \leq 81s$.

Problem 33.2.2. $\varphi(q_1) = T(s)\varphi(q_0)$, and $[E : K] = \varphi(q_1)$. Hence $f = T(s)\varphi(q_0)$, and exactly $T(s)$ places have class 1 modulo q_0, and exactly $T(s)$ have class -1.

Problem 33.2.3. $E \subset \mathbb{Q}(\zeta_{q_1 d})$, $q_1 d \mid q_2$, and $1 \leq \mathrm{rd}_E \leq q_1 d$. A prime $p \equiv 1 \pmod{q_1 d}$ splits completely in E.

Problem 33.2.4. For $s \geq 1$, $\mathrm{rd}_E \geq \mathrm{rd}_{\mathbb{Q}(\zeta_{2^s})} = 2^{s-1}$.

33.3. Scales, ranks and signs

Let γ be Euler's constant, $\mathrm{CS}(d) := \gamma - L'(1, \chi_K)/L(1, \chi_K)$, and

$$C := v_0 + (2d + 6) + q_0 + |\mathrm{CS}(d)| + \sum_w \big|\log|\Phi'_{q_0}(w)|\big|,$$

the sum over the primitive q_0-th roots of unity $w \in \mathbb{C}$, with Φ_{q_0} the cyclotomic polynomial, and $v_0 \geq 0$ the integer, depending only on q_0 and d, that the proof fixes for the integral vacuum (Chapter 34, Section 34.8). For a finite set $\mathcal{F} \subset \Phi$ and a nonnegative integer ℓ_0, call $\mathcal{F}$ *sparse up to* ℓ_0 if for every prime $\ell \leq \ell_0$ and all integers $0 < i < j < l_0(s)$ there are no $\sigma, \tau, \rho \in \mathcal{F}$, distinct or not, with $\tau/\sigma \equiv \pm\ell^i$ and $\rho/\sigma \equiv \pm\ell^j$ (the two signs independent) modulo the largest divisor of q_1 prime to ℓ. For $\kappa\colon \Phi \to \mathbb{Z}_{\geq 0}$, integers $m \geq 0$ and $M \geq 0$, and real L, let

$$L_-(\kappa, m, M, L) := \frac{m}{f} \sum_{\tau \in \Phi} \log \kappa(\tau) + (m - 1) \log \frac{M \mathrm{rd}_E}{2\pi} - \frac{15}{2} L,$$

with $\log 0 := 0$. It depends on s through Φ, f and rd_E.

Definition 33.3.1. *Data* for parameters (q_0, d) consist of the following.

1. Integers $x, x_1, b \geq 1$ with $10^{12}C \leq \log\log b$, $(\log b)^{100} \leq x$, $x^{10^6} \leq x_1$, $x_1^{10^6} \leq b$, and $(\log x_1)^6 \leq \log b$.
2. Integers $m, r, s \geq 0$ with $\sqrt{x} \leq m \leq 2\sqrt{x}$, $x^5 \leq r \leq 3x^5$, $m = 2^e$ and $s = 22e$ for some integer $e \geq 1$, $r = 3^{e'}$ for some integer $e' \geq 1$, $s \leq 32 \log x$, and $q_1 x_1 \mid b$, where $q_1 = q_0 T(s)$. The field is $E = E_s$.
3. A set $\Phi_b \subset \Phi$ of places of class -1 modulo q_0, with $T(s) \leq \#\Phi_b \log b$, sparse up to $(r + 1 - m) \cdot 5r$.
4. The weight $\kappa\colon \Phi \to \mathbb{Z}_{\geq 0}$: $\kappa(\tau) = b$ for $\tau \in \Phi_b$, and $\kappa(\tau) = \lfloor xb/x_1 \rfloor$ otherwise.
5. Distinct primes $p_0, p_1 \equiv 1 \pmod{q_2^2}$ in $[b^{10}, b^{11}]$, and $\alpha \in \mathcal{O}_K$ with $\alpha\bar{\alpha} = p_0 p_1$; let $\pi_M := \overline{\iota(\alpha)} \in \mathcal{O}_E$, where $\iota\colon \mathcal{O}_K \hookrightarrow \mathcal{O}_E$ is the inclusion.
6. A prime $N \equiv 1 \pmod{q_2^2}$ with $L_- \leq \log N \leq L_- + \sqrt{\log b}$, where $L_- := L_-(\kappa, m, p_0 p_1, \log b)$, and $\pi_N \in \mathcal{O}_E$ with $\pi_N \bar{\pi}_N = N$.

Write $a := xb$, $M := p_0 p_1$, $k := r + 1 - m$, $t := 5r$, and $n_j := k + j(t + 1)$ for nonnegative integers j. We call m the number of lifts, k the rank of the source and r the rank of the target, M the principal level and N the level.

Problem 33.3.1. $\log\log b \ge 10^{12}\cdot 18480$, and $\log b < x < x_1 < b$.

Problem 33.3.2. $m \ge 10000$, $2m \le r$, and $r/2 \le k \le r$; in particular $r+1 = k+m$ with $k \ge 1$.

Problem 33.3.3. $x^{11} \le T(s) \le x^{11}(\log b)^{1/5}$, and $x^{11}\varphi(q_0) \le f$.

The hermitian spaces $Y_0,\dots,Y_m$ form a chain over E. Section 34.3 specifies their adelic frames. For $0 \le j < m$ the Gram matrix of Y_j, in suitable coordinates, is the orthogonal sum of the identity matrix of size n_j and the matrix Σ_j of size $m-1-j$ with rows and columns indexed by $0,\dots,m-2-j$, whose (u,v) entry is 0 unless $u+v = m-2-j$, is 1 if $u+v = m-2-j$ and $u \ne v$, and is $-N$ if $u = v = (m-2-j)/2$. The space Y_m is the standard positive definite space of rank $n_m - 1$.

Problem 33.3.4. For $0 \le j \le m$, Y_j has rank $r + jt$ and exactly $\lfloor (m-j)/2 \rfloor$ negative eigenvalues at each infinite place. Y_0 is the orthogonal sum of the identity of size k, $m/2-1$ hyperbolic planes and $\langle -N\rangle$. Formally, for matrices defined in the same way with $m = 4$ (no data have $m = 4$), the numbers of negative eigenvalues of $Y_0,\dots,Y_4$ are $2,1,1,0,0$.

Write $\varrho := m/2 - 1$ for the number of hyperbolic planes displayed in the block Σ_0. Then $m = 2\varrho + 2$.

33.4. The weights and the two amounts

Let $\Lambda_K(\nu) := \Lambda(\nu)(1-\chi_K(\nu))$. For real y, $\sigma \in \Phi$ and integers $j \ge 0$ let

$$s_{\mathrm{fin}}(y,\sigma) := \sum_{\nu=1}^{a} \Lambda_K(\nu)\Big(\frac{y}{\nu} - \kappa([-\nu]\sigma)\Big)_+, \qquad s_\infty(j) := \log j! + j\log\frac{M}{\Omega},$$

where $\Omega := e^{\mathrm{CS}(d)}\,2\pi/\mathrm{rd}_E$ and $[-\nu]\sigma$ is the product in the group Φ. We call $s_\infty(j)$ the size of a derivative of order j, and use $s_{\mathrm{fin}}(\kappa(\sigma),\sigma)$ to measure its guaranteed divisibility when $j = \kappa(\sigma)$. The *direction amount* and the *main amount* are

$$h_{\mathrm{dir}} := \sum_{\sigma\in\Phi}\big(s_\infty(\kappa(\sigma)) - s_{\mathrm{fin}}(\kappa(\sigma),\sigma)\big), \qquad h_{\mathrm{main}} := mk\,h_{\mathrm{dir}}.$$

The *unit of error* is $U := fa\log^3 b$.

Definition 33.4.1. The *denominator budget* is $B := U/(mk) = fa\log^3 b/(mk)$.

With $c_1 := -1 - \mathrm{CS}(d)$, the *main prime sum* and the *total remainder* are

$$s_{\mathrm{main}} := a\Big(\log a - \frac{1}{f}\sum_{\tau\in\Phi}\log\kappa(\tau) + c_1\Big), \qquad \mathrm{rem} := \sum_{\tau\in\Phi_a}\big(s_{\mathrm{fin}}(a,\tau) - s_{\mathrm{main}}\big).$$

Chapter 3 expresses rem through remainders of prime sums in progressions.

Problem 33.4.1. $x_1 \mid a$, and $a/x_1 \le \kappa(\tau) \le b$ for every $\tau \in \Phi$.

Problem 33.4.2. Let $0 \le y \le a$. The term of $s_{\mathrm{fin}}(y,\sigma)$ at ν vanishes unless $\nu < x_1$, and $0 \le s_{\mathrm{fin}}(y,\sigma) \le 2y\sum_{\nu\le x_1}\Lambda(\nu)/\nu \le 2y(\log x_1 + 2) \le y\log b$.

Problem 33.4.3. $\Omega \le 1$, and $20\log b \le \log(M/\Omega) \le 23\log b$.

Problem 33.4.4. For integers $0 \le y \le a$, $20y\log b \le s_\infty(y) \le 25y\log b$. For every integer $y \ge 1$ there is a real λ_y such that

$$s_\infty(y) = y\log\frac{yM}{e\Omega} + \tfrac{1}{2}\log(2\pi y) + \frac{\lambda_y}{12y}, \qquad 0 < \lambda_y < 1.$$

Problem 33.4.5. For every $\tau \in \Phi$, $\kappa(\tau)\log b \le s_\infty(\kappa(\tau)) - s_{\mathrm{fin}}(\kappa(\tau),\tau) \le 25\kappa(\tau)\log b$. Hence $b\,\#\Phi_a \le h_{\mathrm{dir}} \le 25fb\log b$.

Problem 33.4.6. $h_{\mathrm{main}} \ge x^4 fa$.

Problem 33.4.7. With $\delta_b := \#\Phi_b/f$, $s_{\mathrm{main}} = a\big(\log x_1 - \delta_b\log(x_1/x) + c_1\big)$, and $1/(\varphi(q_0)\log b) \le \delta_b \le 1/\varphi(q_0)$.

33.5. The level primes

Problem 33.5.1. Let h be the class number of K, and let $p'_0,\dots,p'_h$ be distinct primes that split in K. Then there are $i \ne j$ and $\alpha \in \mathcal{O}_K$ with $\alpha\bar\alpha = p'_i p'_j$.

Problem 33.5.2. $\sqrt{-1} \in E$. For every prime $p \equiv 1 \pmod 4$ there exist $u, v \in \mathbb{Z}$ with $u^2 + v^2 = p$. The element $\pi := u + \sqrt{-1}\,v \in \mathcal{O}_E$ satisfies $\pi\bar\pi = p$.

Problem 33.5.3. Let $m \ge 2$, $L \ge 7$, $1 \le \kappa(\tau) \le e^L$ for all $\tau \in \Phi$, $e^{20L} \le M \le e^{22L}$ and $q_1 d \le e^L$. Then $mL \le L_-(\kappa, m, M, L) \le 24mL$.

Problem 33.5.4. For data, $b^{20} \le M \le b^{22}$, $m\log b \le \log N \le 30m\log b$, and $b < M < N$.

33.6. Existence

How should the scales be chosen, as functions of x, so that Definition 33.3.1(1)–(2) hold?

Problem 33.6.1. Let $x > 1$, let m be the least power of 2 with $m \ge \sqrt{x}$, and r the least power of 3 with $r \ge x^5$. Then $2 \le m < 2\sqrt{x}$ and $3 \le r < 3x^5$. If $c \ge 0$ and b is the least multiple of an integer $n \ge 1$ with $b > c$, then $b \le c + n$.

Problem 33.6.2. Fix parameters and $0 < \varepsilon < 1/100$, and for each x let $x_1 = \lfloor\exp(x^{\varepsilon/6})\rfloor$ and let b be an integer with $x^\varepsilon \le \log b \le x^\varepsilon + 1$. Then the five inequalities of Definition 33.3.1(1) hold for all large x. If instead $x_1 = \lfloor\exp(x^\beta)\rfloor$ with $\beta > \varepsilon/6$, then $(\log x_1)^6 > \log b$ for all large x. If instead $\varepsilon > 1/100$ and $x^\varepsilon \le \log b \le x^\varepsilon + 1$, then $(\log b)^{100} > x$ for all large x.

The other choices need more. The proof uses the following window theorem. Fix integers $n_0 \ge 1$ and $A \ge 0$ with $4 \mid n_0$. For every sufficiently large real w_0, every integer $v > 1$ with $n_0^v \le w_0^A$, and every real $u_0 \in [w_0, w_0^A]$, there is a prime $p \equiv 1 \pmod{n_0^v}$ with $u_0 \le \log p \le u_0 + w_0$. Taking $n_0 = q_0 d$ and $v = 2(s+6)$ gives the modulus q_2^2 for p_0, p_1, N. The proof combines these windows with the norm constructions of Problems 33.5.1 and 33.5.2. It obtains the sparse set Φ_b from Behrend's construction (Chapter 4). Its existence theorem is as follows.

Theorem 33.6.1. *Let (q_0, d) be parameters and $0 < \varepsilon < 1/100$. For every sufficiently large integer x there are data for (q_0, d) whose first scale is x, such that (1) $x_1 = \lfloor\exp(x^{\varepsilon/6})\rfloor$; (2) b is the least natural number that is divisible by $q_1 x_1$ and exceeds $\exp(x^\varepsilon)$; (3) m is the least power of 2 with $\sqrt{x} \le m$, and r is the least power of 3 with $x^5 \le r$; (4) $x^{\varepsilon/6} - 1 \le \log x_1$ and $x^\varepsilon \le \log b \le x^\varepsilon + 1$.*

"Sufficiently large" depends on (q_0, d) and ε; the statement gives no explicit threshold. In its proof m, r, s and b are taken as above; the digits of the exponents defining Φ_b form vectors on a common sphere (Chapter 4); and the windows used to choose the primes have length $x^{\varepsilon/6}$ in $\log p$.

Problem 33.6.3. For the data of Theorem 33.6.1 and all large x: $\log b \le 2x^{\varepsilon}$ and $\log x_1 \ge x^{\varepsilon/12}$.

In the Lean formalization. In the Lean proof [GL] (`grh/src/`, with the namespace `New.` omitted below), Definition 33.1.1 is `Parameters` and Definition 33.3.1 is `Data`, with fields including `natX`, $\texttt{natX}_1$, `natB`, `m`, `r`, `towerExp`, `bPlaces`, `weight`, `levelPrime`, `piMBar`, `N`, `piN` (`New/Reduction/Data/FieldsAndPlaces.lean`, `New/Reduction/Data/AdmissibleData.lean`); h_{dir}, h_{main}, rem are `Data.directionAmount`, `Data.mainAmount`, `Data.totalRemainder`; U and B are `Data.errorUnit` and `Data.denominatorBudget`; the spaces Y_j are `Data.spaceY`, with Gram matrices for $j < m$ given by `Data.spaceY_gram_eq` and standard endpoint Y_m by `Data.isStd_spaceY_last`; ϱ is `Data.`ϱ, the number of hyperbolic planes of the shape `Data.shape` of Y_0; and Theorem 33.6.1 is `eventually_exists_data` (`New/Reduction/Data/Existence.lean`). The prime window is `exists_prime_modEq_one_log_mem` (`Lib/Analytic/Primes.lean`); the proof of existence uses `exists_three_term_free`, `Parameters.exists_prime_pair_norm` and `Parameters.exists_mul_star_eq_prime`. The constant v_0 is `Parameters.vacuumBoundConst`. Problems 33.1.1, 33.2.3, 33.2.4, 33.3.1, 33.4.7, 33.5.1, 33.6.1, 33.6.2 and 33.6.3 are derived here.

Hints

§33.1.

33.1.1: $d + 1 > 0$; $q_0/2$ divides $d + 1$ with odd quotient, and $8 \mid q_0/2$.

33.1.2: (i) Show $d \equiv -1 \pmod{4p}$ and apply quadratic reciprocity; for $p = 2$ use $d \equiv 7 \pmod 8$. (ii) Use (i) with $18480 \mid q_0$.

§33.2.

33.2.1: For $s \ge 1$, $3^{\lfloor \log_3 s \rfloor} \le s < 3^{\lfloor \log_3 s \rfloor + 1}$; treat $s = 0$ directly.

33.2.2: The primes $2, 3$ divide q_0; K is ramified only at d, and $d \nmid q_1$. Count the fibres of $(\mathbb{Z}/q_1)^{\times} \to (\mathbb{Z}/q_0)^{\times}$.

33.2.3: $K \subset \mathbb{Q}(\zeta_d)$ since $d \equiv 3 \pmod 4$. The conductor–discriminant formula.

33.2.4: $|\mathrm{disc}\, L| = |\mathrm{disc}\, F|^{[L:F]}\, N_{F/\mathbb{Q}}(\mathfrak{d}_{L/F})$ for $F \subset L$, with $\mathfrak{d}_{L/F}$ the relative discriminant ideal.

§33.3.

33.3.1: $C \ge q_0$.

33.3.2: $\sqrt{x} \ge (\log b)^{50}$.

33.3.3: Problem 33.2.1 and $s \le 32 \log x$ bound the power of 3; $\log b \ge (\log x_1)^6 \ge (10^6 \log x)^6$, and $\log x \ge 100 \log\log b$ is large.

33.3.4: Σ_j is a sum of hyperbolic planes and, when $m - 1 - j$ is odd, the middle entry.

§33.4.

33.4.1: $q_1 x_1 \mid b$, and $x \le x_1$.

33.4.2: $0 \le \Lambda_K \le 2\Lambda$ and Problem 33.4.1. For an integer $u \ge 1$, $\log u! = \sum_{n \le u} \Lambda(n) \lfloor u/n \rfloor$, and Chebyshev's bound $\psi(u) \le 2u$.

33.4.3: Problems 33.2.3 and 33.2.4, $|\mathrm{CS}(d)| \le C$, $2^s = m^{22}$, and $q_1 x_1 \mid b$.

33.4.4: $y! \le y^y$ and $a \le b^2$. Stirling's formula with Robbins' remainder [Rob].

33.4.5: Problems 33.4.2 and 33.4.4; on Φ_b the weight is b; Definition 33.3.1(3) and Problem 33.2.2.

33.4.6: Problems 33.3.2, 33.2.2 and 33.4.5, and $\varphi(q_0) \le C$.

33.4.7: Write $\log \kappa$ through $\log a$, $\log x$ and $\log x_1$; Problem 33.2.2.

§33.5.

33.5.1: Pigeonhole on the classes of primes $\mathfrak{p}_i \mid p_i'$.

33.5.2: $4 \mid q_1$. Fermat's two-squares theorem.

33.5.3: The mean of $\log \kappa$ lies in $[0, L]$, and $19L \le \log(M \mathrm{rd}_E / 2\pi) \le 23L$ by Problem 33.2.3 and $L \ge 7 > \log 2\pi$.

33.5.4: Problem 33.5.3 with $L = \log b$, using Problems 33.4.1 and 33.3.2, and $q_1 d \le b$ from $q_1 x_1 \mid b$ and $d \le C < x_1$.

§33.6.

33.6.2: Take logarithms to compare the five conditions; keep track of the floor in x_1.

33.6.3: $x^\varepsilon + 1 \le 2x^\varepsilon$; $\lfloor e^u \rfloor \ge e^{u/2}$ for $u \ge 2$.

References

[GL] L. Sernau, *GRH for Dirichlet L-functions, in Lean 4*, a shorter rewriting of the Lean proof, text by Claude, `https://github.com/lsernau/grh-lean`, commit `72fead1`, readable edition `grh/`.

[IR] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, 2nd ed., Grad. Texts in Math. 84, Springer, 1990.

[Ne] J. Neukirch, *Algebraic Number Theory*, Grundlehren Math. Wiss. 322, Springer, 1999.

[RS] J. B. Rosser and L. Schoenfeld, *Approximate formulas for some functions of prime numbers*, Illinois J. Math. **6** (1962), 64–94.

[Rob] H. Robbins, *A remark on Stirling's formula*, Amer. Math. Monthly **62** (1955), 26–29.

[Wa] L. C. Washington, *Introduction to Cyclotomic Fields*, 2nd ed., Grad. Texts in Math. 83, Springer, 1997.

SPACES, FORMS AND TWISTS

Prerequisites. Chapter 33, *The data*: the parameters, the field E and its places, the scales, ranks and signs, and the level primes. From Chapter 5 the isomorphisms $\iota \mid \ell$ and the rings $\mathcal{O}_\iota$; from Chapter 6 twisted lattices (Section 6.1), their index and covolume (Section 6.2). Finite groups GL_r over finite fields and their irreducible characters, at the level of Green's parametrization; unitary groups over CM fields and their adelic points; theta lifts, at the level of definitions.

Which spaces, forms and characters does the proof attach to the data? This chapter fixes them, following [GL]; the later chapters use this notation. The Poincaré map is defined in Chapter 36, the composite lift and the data of each lift of the chain in Chapter 43, and gains and exceptional primes in Chapter 48. Critical pairs and the target lattice are defined at the end of this chapter.

For a prime p and a ring homomorphism $\eta\colon \mathbb{C} \to \mathbb{C}_p$, val is the valuation of $\mathbb{C}_p$ normalized by $\mathrm{val}(p) = 1$, with $\mathrm{val}(0) = \infty$, read after η; after an isomorphism $\iota\colon \mathbb{C} \to \overline{\mathbb{Q}}_\ell$ it is read through ι and the inclusion $\overline{\mathbb{Q}}_\ell \subset \mathbb{C}_\ell$. Put $\mathrm{val}_+ := \max(\mathrm{val}, 0)$. Let $\mathcal{O}_\eta$ be the ring of $z \in \mathbb{C}$ with $\mathrm{val}(\eta z) \geq 0$. For a positive integer q, let $\mathcal{O}^{[q]}$ be the ring of numbers *integral away from* q: the $z \in \mathbb{C}$ with $\mathrm{val}(\eta z) \geq 0$ for every prime $\ell \nmid q$ and every ring homomorphism $\eta\colon \mathbb{C} \to \mathbb{C}_\ell$.

34.1. Chosen places, the group $\bar{G}$ and the idempotent e_0

A finite place w of E is *chosen* if it divides π_M; let $\mathcal{M}$ be the set of chosen places and $\mathcal{M}_i$ those above p_i $(i = 0, 1)$. For $w \in \mathcal{M}$ let k_w be the residue field, and put $\bar{G} := \prod_{w\in\mathcal{M}} \mathrm{GL}_r(k_w) = \bar{G}_0 \times \bar{G}_1$, with $\bar{G}_i := \prod_{w\in\mathcal{M}_i} \mathrm{GL}_r(k_w)$. A *label* of degree r over k_w is a monic squarefree polynomial of degree r with nonzero constant term; after fixing an injective character $\overline{k_w}^\times \to \mathbb{C}^\times$ for each residue field, Green's construction associates to the label an irreducible character Ξ_c of $\mathrm{GL}_r(k_w)$ and the central idempotent $e_c := (\Xi_c(1)/\#\mathrm{GL}_r(k_w)) \sum_g \overline{\Xi_c(g)}\, g$. A family of labels $(c_w)_{w\in\mathcal{M}}$ is *good* if, for $i = 0, 1$, no c_w with $w \in \mathcal{M}_i$ has a root $z \in k_w$ with $z^{q_2} = 1$, and at least one c_w with $w \in \mathcal{M}_i$ is irreducible with a root in $\overline{k_w}$ of order $(\#k_w)^r - 1$. Let $e_0 \in \mathbb{C}[\bar{G}]$ be the sum, over the good families, of the tensor products $\bigotimes_w e_{c_w}$; it is a central idempotent.

The larger finite group $\prod_{w\in\mathcal{M}} \mathrm{GL}_{rt}(k_w)$, with matrices of size $rt = 5r^2$, has order $\mathcal{N} := \prod_{w\in\mathcal{M}} \#\mathrm{GL}_{rt}(k_w)$.

Problem 34.1.1. For $i = 0, 1$ there are exactly f chosen places above p_i, and $\#k_w = p_i$ for $w \in \mathcal{M}_i$. Moreover $\log \mathcal{N} \leq (rt)^2 f \log M \leq x^{32}$.

34.2. The gap and the weights of the lifts

The *gap* is $\Delta := 2r^8$. For $j \geq 0$ and $\tau \in \Phi$ the *weight of lift* j is $\kappa_j(\tau) := \kappa(\tau) + (j + \frac{1}{2})\Delta$. The rank-$r$ target uses the following initial segment ς_τ of the

Date: November 26, 2026.

target parameter at τ:

$$\varsigma_\tau := \Big(\tfrac{k}{2}-1,\ \tfrac{k}{2}-2,\ \ldots,\ 1-\tfrac{k}{2};\ \ -\kappa(\tau)-\Delta,\ -\kappa(\tau)-2\Delta,\ \ldots,\ -\kappa(\tau)-m\Delta\Big),$$

with $k-1$ entries before the semicolon and m after it (k is even). The full sequence continues with $-\kappa(\tau)-(m+1)\Delta, -\kappa(\tau)-(m+2)\Delta, \ldots$.

Problem 34.2.1. The entries of ς_τ are strictly decreasing; its j-th entry after the semicolon is $\Delta/2-\kappa_j(\tau)$.

Definition 34.2.1. The *diagram* of the data assigns to $\tau \in \Phi$ and an integer $h \geq 1$ the number $\beta(\tau,h) \geq 0$ of its columns of height h at τ:

- $\beta(\tau,1) := a$ if $\tau \in \Phi_a$, and $\beta(\tau,1) := 0$ otherwise;
- $\beta(\tau,k) := \kappa_1(\tau) - \lfloor (k+t+1)/2 \rfloor$;
- $\beta(\tau,h) := \Delta-(t+1)$ if $h > k$ and $t+1$ divides $h-k$;
- $\beta(\tau,h) := 0$ for every other h.

The first two cases are disjoint since $k \geq 2$ (Problem 33.3.2). Both differences are positive for the data of Chapter 33. The forms on X_j have, at τ, the highest weight read from β at the heights below n_j: its entry p, numbered from 0 for $0 \leq p < n_j$, is $\sum_{p<h<n_j} \beta(\tau,h)$ plus the last entry, which is 0 for $j=0$ and $\lfloor n_{j-1}/2 \rfloor - \kappa_j(\tau)$ for $j \geq 1$.

Problem 34.2.2. At $\tau \in \Phi_a$ the columns of height below k are precisely the a columns of height one, and at $\tau \notin \Phi_a$ there are no columns of height below k. The corresponding highest weights on X_0 are $(a,0,\ldots,0)$ and 0, respectively, and their Weyl modules are the modules A_τ of Section 34.5. Formally, for $k=4$, $t=5$, $\Delta=8$, $a=3$ and $\kappa_j(\tau) = 12+8j$ at a place $\tau \in \Phi_a$ (values that no data have), the weight on X_1 at τ is $(0,-3,-3,-3)$ followed by six entries -18, and that on X_2 is $(-3,-6,-6,-6)$ followed by six entries -21 and six entries -23.

34.3. The spaces

Each space has a Gram matrix J over E and an adelic frame, chosen in the proof, in which J becomes the specified diagonal sign matrix at infinity and the identity at the finite places; this frame is used for the rational subgroup and for all lattice and reduction conditions. The *standard lattice stabilizer* $K^\circ(V)$ of such a framed space V of rank n is the group of finite adelic unitary matrices of V that are integral at every finite place, the stabilizer of the standard lattice of integral finite adelic vectors of length n. For $j \geq 0$, X_j is the standard positive definite space of rank n_j. The spaces Y_j, $0 \leq j \leq m$, are those of Section 33.3; for $j < m$ the identity block of Y_j is X_j, and Y_m is identified, through a chosen bijection of bases, with the orthogonal complement in X_m of its last basis vector. For $1 \leq j \leq m$, number the r basis vectors of W_j from 0 to $r-1$; its Gram matrix is diagonal, with sign $+1$ at index $i < k+j-1$ and -1 at the other indices; and V_j is the standard positive definite space of rank $r+t$.

Problem 34.3.1. W_j has exactly $m-j$ negative signs for $1 \leq j \leq m$. Formally, for $r=9$, $m=4$, $j=1$, the negative basis vectors are the last three.

34.4. Principal forms, good forms and the target

Let V be such a framed space of rank r, with numbered signs, such as Y_0 or W_j; for Y_0 the sign paired with entry i, numbered from 0, is $(-1)^{\max(i+1-k,0)}$. A *principal form* on V is a bounded continuous complex function on its adelic unitary group, invariant on the left under the rational points and on the right under the *principal level* of integral finite adelic unitary matrices that reduce to the identity at every $w \in \mathcal{M}$, such that, if the product e over τ of the discrete-series kernels with doubled parameter $2\varsigma_\tau$ and the numbered signs of V is integrable, right convolution by e fixes the form. They form a space $H(V)$, on which $\bar{G}$ acts by right translation through integral lifts. The *good forms* are $H_g(V) := e_0 H(V)$. The *target forms* and their dimension are $T := H_g(Y_0)$ and $d_T := \dim_{\mathbb{C}} T$.

34.5. Source forms

The *source forms* S are the algebraic modular forms on the unitary group of X_0 with values in $\bigotimes_{\tau\in\Phi} A_\tau$, where A_τ is the Weyl module of highest weight $(a, 0, \dots, 0)$ for $\tau \in \Phi_a$ and $A_\tau = \mathbb{C}$ otherwise. A form is evaluated on the finite adelic unitary group, and a rational element acts on its values through the entrywise conjugates of its archimedean components. The level consists of the integral finite adelic unitary matrices reducing to the identity at every $w \in \mathcal{M}$ and having last row congruent to $(0, \dots, 0, 1)$ modulo π_N. Put $D_X := \dim_{\mathbb{C}} S$. For each prime $w \mid \pi_N$ of E fix an integral finite idele z_w of norm one, equal to 1 outside w and $\bar{w}$, whose reduction at w has order $N-1$; right translation by the scalar z_w is an operator T_w on S. A source form φ is *ramified* if $\sum_{i=0}^{N-2} T_w^i \varphi = 0$ for every $w \mid \pi_N$; the ramified forms are a subspace S_{ram}. Write $S_{\mathrm{ram}}^{\mathrm{int}}$ for the ramified forms whose gauge of Chapter 48 is at most 1 at every finite adelic argument, for every prime ℓ and every field isomorphism $\iota\colon \mathbb{C} \to \overline{\mathbb{Q}}_\ell$, composed with the inclusion into $\mathbb{C}_\ell$.

34.6. Tame characters and twists

A *tame character* ξ consists of a continuous unitary character of the norm-one ideles of E, trivial on the norm-one elements of $E^\times$, a finite set Q_ξ of finite places of E, and characters ψ_w of $k_w^\times$ for all finite places w, such that: ξ has weight 0 and tame part (ψ_w), that is, $\xi(u) = \prod_w \psi_w(u_w \bmod w)$ for every norm-one idele u with integral finite part; $\psi_w = 1$ for $w \notin Q_\xi$; $\bar{w} \notin Q_\xi$ for $w \in Q_\xi$; and $\operatorname{Nm} Q_\xi := \prod_{w\in Q_\xi} \#k_w$ is prime to MN. A *twist* ϑ is a tame character with $\psi_w \neq 1$ for every $w \in Q_\vartheta$; it is *m-fold* if $\psi_w^n \neq 1$ for every $w \in Q_\vartheta$ and $1 \le n \le m$. The trivial twist 1 has $Q = \varnothing$. For a nonnegative integer n, the power ξ^n as a tame character has the same set Q_ξ and tame part (ψ_w^n).

Problem 34.6.1. A character ψ of $k_w^\times$ has $\psi^n \neq 1$ for $1 \le n \le m$ if and only if its order exceeds m. For $k_w = \mathbb{F}_{13}$, exactly 8 of the 12 characters have order exceeding 3.

34.7. The characters of the lifts

The proof fixes two characters of the norm-one ideles, trivial on the rational points: $\mu^\flat$, of weight $-\kappa_0$ with trivial tame part, and χ_M, of weight 0, whose tame part (ω_w) is trivial off $\mathcal{M}$ and has order q_2 at each $w \in \mathcal{M}$. With υ the splitting character of the Weil representation restricted to the norm-one ideles (weight 1,

trivial tame part), the *character of lift* j is $\mu_j^0 := \mu^\flat\,(\upsilon^{-\Delta}\chi_M)^j$, of weight $-\kappa_j$ and tame part (ω_w^j).

34.8. The integral vacuum

For each s the proof fixes $c_{\mathrm{vac}} \in \mathbb{C}^\times$ such that c_{vac} times the vacuum of the standard rank-one space over E_s has values integral under every ring map $\mathbb{C} \to \mathbb{C}_p$, for every prime p, at all finite arguments, and all conjugates over K of these values have absolute value at most $\exp(v_0 q_1^2)$, with v_0 as in Section 33.3. The *integral vacuum* of a space of rank n is c_{vac}^n times its vacuum.

34.9. The chain and the single lifts

The weight on Y_m at τ has the same last entry as the weight on X_m. Put $\beta^\circ(h) := \Delta/2 - \lfloor (t+1)/2 \rfloor$ if $h \geq k$ and $t+1$ divides $h-k$, and $\beta^\circ(h) := 0$ otherwise; for $1 \leq h < n_m - 1$ the weight on Y_m has $\beta_Y(\tau, h) := \beta^\circ(h) + \beta(\tau, h+1) - \beta^\circ(h+1)$ columns of height h, that is, its entry p, numbered from 0 for $0 \leq p < n_m - 1$, is $\sum_{p<h<n_m-1} \beta_Y(\tau, h)$ plus the last entry.

For a tame character ξ, the *lower chain* Θ_ξ is a linear map from $H(Y_0)$ to algebraic forms of this weight on Y_m: the composite of m normalized theta lifts $Y_{j-1} \to Y_j$, $1 \leq j \leq m$, whose j-th step is built from the character $\mu_j^0 \xi^j$, followed by the passage to algebraic forms on Y_m. For an m-fold twist ϑ, Θ_ϑ also denotes its restriction to T, with target the subspace of this weight on which the final level acts by the character prescribed by ϑ, and $Z(\vartheta) := \det(\Theta_\vartheta^* \Theta_\vartheta)$. For $1 \leq j \leq m$, the *single lift on principal forms* $\hat{u}_{\xi,j}$ is the theta lift from $H(W_j)$ to the algebraic level forms on V_j of the weight, level and character of the descent pair for (ξ, j), built from $\mu_j^0 \xi$, and the *single lift* $u_{\xi,j}$ is its restriction to $H_g(W_j)$; for an m-fold twist ϑ, $Z_j(\vartheta) := \det(u^* u)$ with $u := u_{\vartheta^j,j}$. Chapter 43 describes the datum, characters and scalar in each step of the lower chain; the final level and its character are named in the remark below. Both determinants use the Petersson inner product on the source and the class-sum inner product on the algebraic level forms in the target.

34.10. Critical pairs

For a continuous unitary character μ of the norm-one ideles of E, trivial on the norm-one elements of $E^\times$, and a finite set S of finite places of E, write $\bar{S}$ for the set of conjugate places.

Definition 34.10.1. The *partial Hecke value* $L^S(z, \mu)$, for real $z > 1$, is the Euler product over the finite places $v \notin S \cup \bar{S}$ of $(1 - c_v(\#k_v)^{-z})^{-1}$, where c_v is the value of the Hecke character $x \mapsto \mu(x/\bar{x})$ of E at a chosen uniformizer at v. At $z = 1$ it is the limit from the right, where this limit exists and is finite. For $z > 1$, if $S \cup \bar{S}$ contains the places where this Hecke character ramifies, the product is its L-function without the Euler factors at $S \cup \bar{S}$.

A *critical pair* $P = (\nu, z)$ consists of such a character ν, of weight $-\mathrm{wt}_P$ with $\mathrm{wt}_P \colon \Phi \to \mathbb{Z}_{\geq 0}$ (the *negative weight* of P), residue characters ψ_w that give its tame part and are trivial off $\mathcal{M}$, and an integer z with $1 \leq z \leq t$ and $z \leq \mathrm{wt}_P(\sigma) \leq 4b$ for all $\sigma \in \Phi$. It is *ramified* if $\psi_w \neq 1$ exactly for $w \in \mathcal{M}$. For a tame character ξ and $\epsilon = \pm 1$ its *ratio* is

$$R_P(\xi, \epsilon) := \frac{|L^{\mathcal{M} \cup Q_\xi}(z, (\nu \xi^\epsilon)^{-1})|}{|L^{\mathcal{M}}(z, \nu^{-1})|}, \qquad R_P(\xi) := R_P(\xi, 1).$$

Problem 34.10.1. For $1 \le j \le m$, a critical pair with tame part (ω_w^j), the j-th power of the tame part of χ_M, is ramified. Formally, if a family of residue characters is trivial off the nonempty set $\mathcal{M}$ and has order 6 at every place of $\mathcal{M}$, then for exactly 9 of the integers $1 \le j \le 10$ its j-th power is nontrivial at every place of $\mathcal{M}$.

34.11. The target lattice

Recall the isomorphisms $\iota \mid \ell$ of Chapter 5. For an m-fold twist ϑ, the target of Θ_ϑ is the space of algebraic forms on Y_m of the weight specified in Section 34.9 on which the final level acts by the character prescribed by ϑ, with the class-sum inner product. A form F in it is *integral at* ι if its values have gauge (Chapter 48) at most 1 at every finite adelic argument, for the composite of ι with the inclusion $\overline{\mathbb{Q}}_\ell \subset \mathbb{C}_\ell$.

Definition 34.11.1. The *target lattice* is the following twisted lattice on T, in the sense of Chapter 6, Section 6.1. Its twists are the m-fold twists, with the trivial twist 1; its maps are the lower chains Θ_ϑ on T; for every $n \in \mathbb{N}$, the twist ϑ is *allowed* at n if $\gcd(n, \operatorname{Nm} Q_\vartheta) = 1$; and $\mathfrak{L}_{\vartheta,\iota}$ is the $\mathcal{O}_\iota$-module of forms in the target of Θ_ϑ that are integral at ι. The coordinates of a form F in the target of Θ_1 are the coordinates, in the standard basis of the Weyl module, of its values $F(g_c)$ at fixed representatives g_c of the classes at its level; their rational Gram matrix is block diagonal, with one copy of the Gram matrix of the Weyl module for each class. For $v \in T$ and $\sigma \in \operatorname{Aut}(\mathbb{C})$, $\|v\|_\sigma^2$ is the squared length, for this Gram matrix, of the coordinate vector of $\Theta_1 v$ with σ applied to each coordinate. A vector $v \in T$ is *integral at* $\iota \mid \ell$ if $\Theta_\vartheta v \in \mathfrak{L}_{\vartheta,\iota}$ for every ϑ allowed at ℓ. A family $y_1, \dots, y_n$ in T has *covolume* at most c if for every $\sigma \in \operatorname{Aut}(\mathbb{C})$ the determinant of the products of the coordinate vectors of the $\Theta_1 y_i$, with σ applied, taken by the same Gram matrix, has absolute value at most e^c. It has *index* at most δ if there is a function $e\colon \mathbb{N} \to \mathbb{R}_{\ge 0}$ satisfying both conditions below. For every finite set U of primes, $\sum_{\ell \in U} e(\ell) \log \ell \le \delta$. For every prime ℓ and every $\iota \mid \ell$, there is a matrix $u \in M_n(\mathcal{O}_\iota)$ with $|\det u|_\iota \ge \ell^{-e(\ell)}$ such that $\sum_k u_{ik} y_k$ is integral at ι for every i.

These are the index and covolume of Section 6.2 for this twisted lattice. The proof shows that these data satisfy the pairing condition of a twisted lattice and that the maps Θ_ϑ are injective on T (Problem 59.4.3); by definition its volume at ϑ is $Z(\vartheta)$. The stabilizers of the classes at the levels of the targets are trivial, so $\|v\|_\sigma^2$ is also the weighted sum of Chapter 42, Section 42.3, for the form $\Theta_1 v$.

In the Lean formalization. In the Lean proof [GL] (`grh/src/`, with the namespace `New.` omitted below): The objects of this chapter are `Data.IsChosen`, `Data.chosenGL`, `Data.e`$_0$, `Data.gap`, `Data.liftWeight`, `Data.targetParameter`, `Data.spaceY`, `Data.spaceW`, `Data.descentPair`, `Data.principalForms`, `Data.goodForms`, `Data.targetForms`, `Data.SourceForm`, `Data.ramifiedSourceForms`, `Data.integralRamified`, `Data.TameChar`, `Data.Twist`, `Data.MFoldTwist`, `Data.untwistedLiftChar`, `Parameters.vacuumScale`, `Parameters.intVacuum`, `Data.lowerChain`, `Data.`Θ, `Data.goodLift`, `Data.chainDeterminant` and `Data.liftDeterminant`; step j of the normalized chain is `Data.liftY` at index $j-1$. For a tame character, `Data.lowerChainAtLevel` gives `Data.lowerChain` its codomain of forms of the prescribed level and character, given by `Data.lastLevel` and the pullback of

`Data.lastLevelChar` under reduction to `Data.lastResidueLevel`; the weight on Y_m is `Data.weightY`, with columns `Data.columnsY`, given by `Data.weightY_eq`. The definitions of W_j, of the descent pair (with the same standard target space V_j at every j), of both single lifts and of $Z_j(\vartheta)$ accept every nonnegative integer j; both single lifts are zero outside $1 \le j \le m$. For an m-fold twist, `Data.`Θ restricts `Data.lowerChainAtLevel` to T. The single lift on principal forms is `Data.singleLift`, and its restriction to good forms is `Data.goodLift`. The constant v_0 of Chapter 33 is `Parameters.vacuumBoundConst`; the characters $\mu^\flat$, χ_M, (ω_w) are `Data.chiZero`, `Data.chiM`, `Data.chiMLocal`. The properties of e_0, of these characters, of μ_j^0 and of c_{vac} stated in Sections 34.1, 34.7 and 34.8 are `Data.isCentralProj_e`$_0$, `Data.chiZero_hasWeight`, `Data.chiM_hasWeight`, `Data.orderOf_chiMLocal`, `Data.chiMLocal_eq_one_of_not_isChosen`, `Data.untwistedLiftChar_hasWeight` and `Parameters.isVacuumScale_vacuumScale`; the restricted splitting character υ is `WeilData.upsilonU1`, of weight 1 and trivial tame part by `WeilData.upsilonU1_hasWeight`. Problem 34.2.1 is `Data.targetParameter_eq` and `Data.targetParameter_strictAnti`. The truncated valuation val_+ on $\overline{\mathbb{Q}}_\ell$ is `ellVal`, and $\mathcal{O}^{[q]}$ is `Seesaw.integralAway` q, which enters the clause on the coefficients of `Data.IsChainDatum`. The group $\bar{G}$ is `Data.chosenGL`, a product over the pairs (i,w) with $w \in \mathcal{M}_i$, so $\bar{G}_i$ is its factor at i; $\mathcal{N}$ is `Data.chosenGroupOrder`. The place count in Problem 34.1.1 is `Data.card_chosenPlace`, and the residue-field size is the restriction of `Data.q_eq_levelPrime` to chosen places. The endpoint of the bound is `Data.log_chosenGroupOrder_le`; its proof gives the intermediate bound as well. Definition 34.2.1 is `Data.columnCount`; the last entry is `Data.lastEntry`, and the weight on X_j is `Data.weightX`, given through the diagram by `Data.weightX_eq`. $K^\circ(V)$ is `stdLevel`. Definition 34.10.1 is `AutChar.L`, `Data.CriticalPair` (with wt_P its field `negWeight`), `Data.CriticalPair.IsRamified` and `Data.CriticalPair.ratio`; at $z = 1$, `AutChar.L` takes the value of `extendFrom` from $(1,\infty)$. The first assertion of Problem 34.10.1 uses `Data.chiMLocal_zpow_ne_one_iff_isChosen`, stated for all integers $n \neq 0$ with $|n| \le 8m$. The count for order 6 is a formal example. Definition 34.11.1 is `Data.targetLattice` (in `New/Reduction/IntegralTargetForms.lean`), a `TwistedLattice`, with `integralVectors`, `IndexLe`, `CovolumeLe` and `normSqAt`; its volume and injectivity are `Data.volume_targetLattice` and `Data.injective_lift_targetLattice`; the pairing condition is its field `norm_inner_le_one`; triviality of the stabilizers is `Data.classAut_lastResidueLevel_eq_bot`, and `Data.normSqAt_targetLattice` compares the two norms.

Hints

§34.1.

34.1.1: $p_i \equiv 1 \pmod{q_1 d}$ splits completely in E (Problem 33.2.3), and the ideal (π_M) of $\mathcal{O}_K$ is the product of one prime above p_0 and one above p_1; $[E:K] = f$. Use $\#\mathrm{GL}_n(\mathbb{F}_q) < q^{n^2}$ for $n \ge 1$, $r \le 3x^5$, Problems 33.2.2, 33.3.3 and 33.5.4, $\varphi(q_0) \le C$ and $(\log b)^{100} \le x$.

§34.2.

34.2.1: $\kappa(\tau) + \Delta > k/2$.

34.2.2: $n_0 = k$. Below $n_1 = 10$ the nonzero columns have heights 1 and 4; below $n_2 = 16$ also 10.

§34.3.

34.3.1: $r - (k + j - 1)$.

§34.6.

34.6.1: $\mathbb{F}_{13}^{\times}$ is cyclic of order 12.

§34.10.

34.10.1: ω_w has order q_2 at $w \in \mathcal{M}$ and is trivial off $\mathcal{M}$; $q_2 \geq 2^s > m$ by Definition 33.3.1(2).

References

[GL] L. Sernau, *GRH for Dirichlet L-functions, in Lean 4*, a shorter rewriting of the Lean proof, text by Claude, `https://github.com/lsernau/grh-lean`, commit `72fead1`, readable edition `grh/`.

THE MAIN INEQUALITY

Prerequisites. Hadamard's inequality for positive definite Hermitian matrices [HJ, §7.8]. Dirichlet L-functions: $L(1,\chi) \neq 0$ for χ nonprincipal, induced and primitive characters, and the functional equation [Dav, Ch. 4, Ch. 5, Ch. 8, Ch. 9]. From Chapter 1 the remainder $R_{d,q}$, written R_q here for fixed d, the one-sided criterion and the prime number theorem in progressions; from Chapter 3 the identity for the total remainder; from Chapter 33 the data and Problem 33.6.3; from Chapter 34 the objects and the target lattice (Definition 34.11.1); and the statements of Theorems A, B and C (Chapters 42, 36 and 54). The problems in Section 35.1 use no earlier chapter.

Theorems A and B supply many independent target forms, with upper bounds for the lengths of their untwisted lifts and for the index of the family; Theorem C bounds the covolume plus twice the index of such a family from below by the main amount, times the dimension, less a small error. How do the three statements give the theorem? Comparing the two bounds gives the main inequality for the total remainder rem. The identity of Theorem 3.2.1 then gives an upper bound for the prime-sum remainder $R_{q_0}(x)$. We first do the comparison in a lattice, then state the main inequality, and finally pass to the one-sided bound and to the theorem. Parts VII, VIII and IX state and deduce Theorems B, A and C.

35.1. The comparison in a lattice

Let $N \geq 1$ be an integer, and give $\mathbb{C}^d$ the Hermitian form $\langle v, w\rangle := N\,\bar{v}^{\mathsf{T}} w$. For $y_1, \dots, y_n \in \mathbb{Q}^d$ write $\mathrm{Gram}(y) := \det(\langle y_i, y_j\rangle)_{i,j\leq n}$, and let $H := \log N$.

Problem 35.1.1. If $\langle y_i, y_i\rangle \leq e^u$ for $i = 1, \dots, n$, then $\mathrm{Gram}(y) \leq e^{nu}$; if the y_i are linearly independent, $\log \mathrm{Gram}(y) \leq nu$.

The comparison itself is an inequality between real numbers. Suppose that a family of n vectors in a space of dimension $d \geq 1$ satisfies a lower bound and two upper bounds,

$$d(H - 3F) \leq c + 2\delta, \qquad c \leq n(H - \rho + F), \qquad \delta \leq dI,$$

for real numbers H, F, I, ρ, c, δ. The upper exponent per vector is $H - \rho + F$, including the error F.

Problem 35.1.2. If moreover $H + F \geq 0$ and $d/2 \leq n \leq d$, then $n\rho \leq d(4F + 2I)$, and $\rho \leq 2(4F + 2I)$ when $4F + 2I \geq 0$.

Problem 35.1.3. In the comparison of real numbers above, after dropping the hypothesis $H + F \geq 0$ one can satisfy all three bounds and $d/2 \leq n \leq d$ while $n\rho > d(4F + 2I)$. (Here H is any real number, not necessarily $\log N$.)

In this lattice the main amount sits in the metric. In Chapter 54 it enters through the height of the family $\iota \mapsto Z(1)/Z(\theta_\iota)$, where the twist θ_ι is chosen for each pair (ℓ, ι) (Problem 54.2.4).

Date: November 26, 2026.

35.2. The main inequality

Let rem be the total remainder of Chapter 33, $U = fa\log^3 b$ the unit of the errors and $F := U\log b$. Theorems A and B (Chapters 42 and 36) concern the ramified source forms S_{ram}, the integral ones $S^{\mathrm{int}}_{\mathrm{ram}}$, the finite group $\bar G$, and the normalized translates $A_s\colon S_{\mathrm{ram}} \to T$ of the Poincaré map, $s \in \bar G$. For $v \in T$ and $\sigma \in \mathrm{Aut}(\mathbb{C})$, $\|v\|^2_\sigma$ is the squared length of Definition 34.11.1, computed from the σ-conjugate coordinates of the untwisted lift $\Theta_1 v$. Theorems A, B and C are proved in Parts VIII, VII and IX (Chapters 42, 36 and 54); here we use only their statements, in the following form.

(A1) (Theorem 42.3.2(a), which writes $\|\Theta_1 A_s\varphi\|_\sigma$ for the length used here and $fa\log^4 b$ for F.) S_{ram} is spanned by the set S_{short} of $\varphi \in S^{\mathrm{int}}_{\mathrm{ram}}$ with $\|A_s\varphi\|^2_\sigma \le \exp(h_{\mathrm{main}} - m\,\mathrm{rem} + F)$ for every $s \in \bar G$ and every σ.

(A2) (Theorem 42.3.2(b), which writes $2fa\log^3 b$ for $2U$.) If $J \subseteq \bar G$ is finite and every y_i lies in $A_s(S^{\mathrm{int}}_{\mathrm{ram}})$ for some $s \in J$, then $y_1, \dots, y_n$ has index at most $2\,\#J \dim S_{\mathrm{ram}} \cdot U$.

(B) (Consequence of Theorem 36.4.2: there the maps $e_0\rho(s)\mathcal{P}$ on S_{ram} have the same ranges as the A_s.) $d_T > 0$, and there is a finite $J \subseteq \bar G$ with $\#J \dim S_{\mathrm{ram}} \le 5d_T \log(1+2b^2)$ and $\dim \sum_{s\in J} A_s(S_{\mathrm{ram}}) \ge (1 - 4/b^2)d_T$.

Theorem C (Theorem 54.2.1), in full, is the lower bound: if $y_1, \dots, y_n$ are linearly independent target forms with $(1-4/b^2)d_T \le n$, of index at most δ and covolume at most c, then

$$d_T(h_{\mathrm{main}} - 3fa\log^4 b) \le c + 2\delta;$$

index and covolume are those of the target lattice (Definition 34.11.1).

The upper bound for the covolume is Hadamard's inequality: if $\|z_i\|^2_\sigma \le e^u$ for $i = 1, \dots, n$ and every σ, then $z_1, \dots, z_n$ has covolume at most nu.

Problem 35.2.1. For J as in (B), the span of $\bigcup_{s\in J} A_s(S_{\mathrm{short}})$ is $\sum_{s\in J} A_s(S_{\mathrm{ram}})$. Hence that space has a basis $y_1, \dots, y_n$ with each $y_i \in A_s(S_{\mathrm{short}})$ for some $s \in J$, and $(1-4/b^2)d_T \le n \le d_T$.

Problem 35.2.2. This family has covolume at most $n(h_{\mathrm{main}} - m\,\mathrm{rem} + F)$ and index at most $d_T \cdot 10\log(1+2b^2)\,U$.

Problem 35.2.3. $n\,m\,\mathrm{rem} \le d_T\big(4F + 20\log(1+2b^2)\,U\big)$.

Problem 35.2.4. $n \ge d_T/2$, and $8F + 40\log(1+2b^2)\,U \le fa\log^5 b$. Hence $m\,\mathrm{rem} \le fa\log^5 b$.

Theorem 35.2.1 (Main inequality)**.** $m\,\mathrm{rem} \le fa\log^5 b$.

The errors per dimension are: F from the size in Theorem A, $20\log(1+2b^2)\,U$ from the index in Theorems A and B (counted twice, as it enters as 2δ), and $3F$ from Theorem C.

35.3. From the main inequality to the theorem

Let $q_0 \ge 1$ and d be the parameters of the data, so that $18480 \mid q_0$ and d is a prime with $d \equiv q_0/2 - 1 \pmod{q_0}$; then d is odd and prime to q_0. Recall that, for $q \ge 1$ prime to d, $R_q(y) = \sum_{n\le y} \lambda(n)(1/n - 1/y) - \log y/\varphi(q) - c_q$, with $\lambda(n) = \Lambda(n)(1 - (n/d))$ for $n \equiv 1 \pmod q$ and $\lambda(n) = 0$ otherwise, where (n/d) is the Legendre symbol and c_q is the constant for which $R_q(y) \to 0$; these are $R_{d,q}$

and $c_{d,q}$ of Chapter 1. When d varies we write $R_q^{(d)} = R_{d,q}$. We use the identity of Theorem 3.2.1,

$$\text{rem} = a\big(\#\Phi_b\,(R_{q_0}(x) - R_{q_0}(x_1)) + \#\Phi_a\,R_1(x_1)\big)$$

for the sets Φ_a and Φ_b of a-places and b-places, together with $f = \#\Phi_a\,\varphi(q_0)$ and $0 < \#\Phi_a \le \#\Phi_b \log b$ (Chapter 33).

Problem 35.3.1. $R_{q_0}(x) \le \varphi(q_0)\log^6 b/m + |R_{q_0}(x_1)| + \log b\,|R_1(x_1)|$.

Two further inputs. By the prime number theorem in progressions, for every prime $d \ne 2$, every $q \ge 1$ prime to d and every integer $B \ge 0$, one has $|R_q(y)| \le (\log y)^{-B}$ for all large y (Chapter 1). And for $0 < \varepsilon < 1/100$ and every large integer x there are data with this x, with $\log b \le 2x^{\varepsilon}$, $m \ge \sqrt{x}$ and $\log x_1 \ge x^{\varepsilon/12}$ (Problem 33.6.3).

Problem 35.3.2. Let $\varepsilon > 0$. For all large integers x and every real y with $\log y \ge x^{\varepsilon/12}$, one has $|R_{q_0}(y)| \le x^{-2}$ and $|R_1(y)| \le x^{-2}$.

Problem 35.3.3. Let $0 < \varepsilon < 1/100$. For all large integers x, $R_{q_0}(x) \le (64\varphi(q_0) + 3)\,x^{-1/2+6\varepsilon}$.

Problem 35.3.4. For $q \ge 1$ prime to d and real $y \ge 2$, $R_q(y) - R_q(\lfloor y\rfloor) \le 3/y$. For $-1 \le u \le 0$, $\lfloor y\rfloor^u \le 2y^u$.

Problem 35.3.5. Let $\varepsilon > 0$. For all large real y, $R_{q_0}(y) \le y^{-1/2+\varepsilon}$.

Theorem 35.3.1 (One-sided bound)**.** *Let $q_0 \ge 1$ be a multiple of* 18480*, let $d \equiv q_0/2 - 1 \pmod{q_0}$ be a prime, and let $\varepsilon > 0$. Then $R_{q_0}(y) \le y^{-1/2+\varepsilon}$ for all large real y.*

The criterion of Chapter 1 reads: let $q_0 \ge 1$ be a multiple of 8, let $d_0 \ge 0$ be an integer with $d_0 \equiv 7 \pmod 8$ and prime to q_0, and let $\beta > \frac12$; if for every prime $d \equiv d_0 \pmod{q_0}$ one has $R_{q_0}^{(d)}(y) \le y^{\beta-1}$ for all large y, then $L(\rho,\psi) \ne 0$ for every character ψ modulo q_0 and every $\rho \ne 1$ with $\operatorname{Re}\rho > \beta$.

Problem 35.3.6. For $q \ge 1$, $q_0 := 18480q$ and $d_0 := 9240q - 1$: $d_0 \equiv 7 \pmod 8$, $\gcd(d_0, q_0) = 1$, and $d_0 = q_0/2 - 1$.

Problem 35.3.7. Let $q \ge 1$, let χ be a character modulo q, and let χ' be the character modulo $q_0 = 18480q$ that it induces. If χ is nonprincipal or $s \ne 1$, then $L(s,\chi') = L(s,\chi)\prod_{p\mid q_0}(1 - \chi(p)p^{-s})$, so $L(s,\chi') \ne 0$ implies $L(s,\chi) \ne 0$.

Problems 35.3.6 and 35.3.7, Theorem 35.3.1, the criterion and $L(1,\chi) \ne 0$ for χ nonprincipal prove the following.

Theorem 35.3.2. *Let $q \ge 1$, let χ be a Dirichlet character modulo q, and let $s \in \mathbb{C}$ with $\operatorname{Re} s > \frac12$, where $s \ne 1$ if χ is principal. Then $L(s,\chi) \ne 0$.*

Problem 35.3.8. Every zero s of a Dirichlet L-function with $0 < \operatorname{Re} s < 1$ has $\operatorname{Re} s = \frac12$.

Theorem 35.3.2 is the half-plane form of the generalized Riemann hypothesis for Dirichlet L-functions. Thus Theorems A, B and C give the main inequality, from which the one-sided bound and the criterion of Chapter 1 yield Theorem 35.3.2.

In the Lean formalization. In the Lean proof [GL], Theorem 35.2.1 is `New.star_inequality`, in `grh/src/New/Reduction/MainInequality.lean`; Problem 35.3.1, Theorem 35.3.1 and Theorem 35.3.2 are `New.Data.primeRemainder_le`, `New.eventually_primeRemainder_le_rpow` and `New.grh`, in `grh/src/New/Reduction/OneSidedBound.lean`. Hadamard's inequality for the covolume is `New.TwistedLattice.covolumeLe_of_normSqAt_le`, and Problems 35.2.1–35.2.4 follow the proof of `New.star_inequality`. Problems 35.3.2 and 35.3.3 are `New.eventually_abs_primeRemainder_exp_le` and `New.eventually_primeRemainder_natCast_le`. For the first bound of Problem 35.3.4 the proof uses `New.primeRemainder_sub_primeRemainder_floor_le`, which gives $26/y$ in place of $3/y$, for every prime d and every $q \geq 1$; the sharper bound is an exercise here. The second bound is `New.natFloor_rpow_le_two_mul_rpow`. Problem 35.3.8 is `New.zeros_on_line`, in `grh/src/New/Main.lean`, applied to `New.grh`.

Hints

§35.1.

35.1.1: Apply Hadamard's inequality to the Gram matrix.

35.1.2: Insert the upper bounds into the lower bound; then use $n(H+F) \leq d(H+F)$.

35.1.3: Take $d = 2$, $n = 1$, $F = I = \delta = 0$ and $H = -1$.

§35.2.

35.2.1: Images of a spanning set span the image.

35.2.2: Hadamard's inequality with $u = h_{\mathrm{main}} - m\,\mathrm{rem} + F$; (A2) and the bound for $\#J \dim S_{\mathrm{ram}}$ in (B).

35.2.3: Compare the two bounds for $c + 2\delta$, using $n \leq d_T$ and $h_{\mathrm{main}} + F \geq 0$.

35.2.4: $\log(1 + 2b^2) \leq 3 \log b$, and $\log b \geq 128$.

§35.3.

35.3.1: Solve the identity for $R_{q_0}(x)$, and divide Theorem 35.2.1 by $ma\#\Phi_b$.

35.3.2: Take $B \geq 24/\varepsilon$; d is odd and prime to q_0.

35.3.3: Use Problem 35.3.1 for the data at x and Problem 35.3.2 with $y = x_1$.

35.3.4: The two sums differ by $(1/\lfloor y \rfloor - 1/y) \sum_{n \leq y} \lambda(n)$; use $0 \leq \lambda \leq 2\Lambda$ and $\psi(\lfloor y \rfloor) < 1.04 \lfloor y \rfloor$ [RS, Thm. 12].

35.3.5: Problem 35.3.3 with $\min(\varepsilon/7, 1/200)$ in place of ε, and Problem 35.3.4.

35.3.7: Compare Euler products for $\mathrm{Re}\, s > 1$, then continue analytically.

35.3.8: Reduce to a primitive character; then the functional equation and Theorem 35.3.2.

References

[Dav] H. Davenport, *Multiplicative Number Theory*, 3rd ed., Grad. Texts in Math. 74, Springer, 2000.

[GL] L. Sernau, *GRH for Dirichlet L-functions, in Lean 4*, a shorter rewriting of the Lean proof, text by Claude, `https://github.com/lsernau/grh-lean`, commit `72fead1`, readable edition `grh/`.

[HJ] R. A. Horn and C. R. Johnson, *Matrix Analysis*, 2nd ed., Cambridge Univ. Press, 2013.

[RS] J. B. Rosser and L. Schoenfeld, *Approximate formulas for some functions of prime numbers*, Illinois J. Math. **6** (1962), 64–94.

THEOREM B: ENOUGH FORMS

Prerequisites. From Chapter 10: Poincaré series on $\mathrm{SL}_2(\mathbb{Z})$, the unfolding of Problem 10.1.1, Problem 10.1.3, and the main term of the dimension (Section 10.4). From Chapter 21: class sets, the groups Γ_L, forms and their norm (Section 21.3), Problems 21.1.2, 21.1.4, 21.3.2 and 21.3.5, and the mass of rank two, written here $\mathrm{mass}_2 = 1/32$. From Chapter 23: the period of Section 23.4. From Chapter 9: Hilbert–Schmidt norms, Problems 9.2.2, 9.2.5 and 9.3.1, near isometries, and Theorems 9.3.1 and 9.4.1. From Chapter 33: the data, and the spaces and forms of Chapter 34 (Y_0, X_0, the chosen places $\mathcal{M}$, the group $\bar{G}$, the idempotent e_0, the forms $H(Y_0)$, the target T of dimension d_T, the source $S \supseteq S_{\mathrm{ram}}$ of dimension D_X, and the operators T_w). The Bessel periods of Gan, Gross and Prasad [GGP, §§12, 23], at the level of the definition. Norms of linear maps are Hilbert–Schmidt norms, $\|L\|^2 = \mathrm{Tr}(L^*L)$, and log is the natural logarithm.

In Chapter 10 a Fourier coefficient of a cusp form is, up to an explicit factor, its inner product with a Poincaré series, and Petersson's formula expands the inner products of two Poincaré series. In the proof, a Poincaré map represents Bessel periods on a unitary group, and the Gram operators between it and its translates by a finite group have an expansion in integrals indexed by rational points. After projection to the good forms and restriction to the ramified source, a finite set of translates spans almost all of the target (Theorem 36.4.2). The estimates behind this are developed in Chapters 37, 38 and 41. How does the Gram operator group into double cosets in a finite example, and what does a second moment over translates give? Hermitian forms h and inner products are linear in the first variable; Chapter 9 uses the other convention, and the statements recalled from it do not depend on the choice.

36.1. The Bessel subgroup

Let E/F be a CM extension, ψ_F a nontrivial character of $F\backslash\mathbb{A}_F$, and let V be a hermitian space over E of rank r with a decomposition

$$V = Ev_1 \oplus \cdots \oplus Ev_\varrho \oplus X \oplus Ez \oplus Ev_1' \oplus \cdots \oplus Ev_\varrho',$$

where $h(v_a, v_c) = h(v_a', v_c') = 0$, $h(v_a, v_c') = \delta_{ac}$, the space X of rank k is orthogonal to the v_a, v_a' and z, and z is orthogonal to every v_a and v_a', with $h(z,z) = -N$ for a prime N. So $r = 2\varrho + k + 1$. This is the shape of Y_0 in Chapter 33, with $\varrho = m/2 - 1$, $X = X_0$, and N the prime of the data.

Let $\mathcal{U}$ be the group of $n \in U(V)$ such that $(n-1)v_a$ lies in the span of $v_1, \dots, v_{a-1}$ for every a, and $(n-1)y$ lies in the span of $v_1, \dots, v_\varrho$ for every y orthogonal to all v_a. It is the unipotent radical of the stabilizer of the isotropic flag $Ev_1 \subset Ev_1 + Ev_2 \subset \cdots$. Embed $U(X)$ in $U(V)$ as the pointwise stabilizer of the v_a, the v_a' and z. Put

Date: November 26, 2026.

$v_{\varrho+1} := z$ and, for $n \in \mathcal{U}$,

$$\lambda(n) := \sum_{a=1}^{\varrho} h(nv_{a+1}, v'_a), \qquad \psi_{\mathcal{U}}(n) := \psi_F\big(\mathrm{Tr}_{E/F}\,\lambda(n)\big).$$

The *Bessel subgroup* is $R := \mathcal{U} \rtimes U(X)$. For scalar-valued automorphic forms y on $U(V)$ and ϕ on $U(X)$ for which the integral converges absolutely, the Bessel period integrates y against $\overline{\psi_{\mathcal{U}}}$ over $\mathcal{U}(F)\backslash\mathcal{U}(\mathbb{A}_F)$, and the result against $\bar{\phi}$ over $U(X)(F)\backslash U(X)(\mathbb{A}_F)$ [GGP, §§12, 23]. For $\varrho = 0$ the group $\mathcal{U}$ is trivial, and the Bessel period is the restriction period along $U(X) \subset U(X \perp Ez)$.

Problem 36.1.1. For $n \in \mathcal{U}$, $\lambda(n)$ is the sum over $a \le \varrho$ of the coefficient of v_a in nv_{a+1}. The map $\lambda\colon \mathcal{U} \to E$ is a homomorphism, and $\lambda(gng^{-1}) = \lambda(n)$ for $g \in U(X)$. Hence $\psi_{\mathcal{U}}$ is a character of $\mathcal{U}(\mathbb{A}_F)$, trivial on $\mathcal{U}(F)$ and fixed by $U(X)$.

Problem 36.1.2. $U(X)$ normalizes $\mathcal{U}$, and $U(X) \cap \mathcal{U} = \{1\}$.

Problem 36.1.3. As an algebraic group over F, $\mathcal{U}$ has dimension $\varrho(r+k) = 2\varrho(r-2\varrho) + \varrho^2 + \varrho(\varrho-1)$. For $(\varrho, k) = (1, 0)$ it is the three-dimensional unipotent radical of a Borel subgroup of $U(V)$, V of rank 3.

36.2. Poincaré series

The Poincaré series of the proof plays the role of that of Chapter 10: the Bessel subgroup replaces Γ_∞ in the period, and a Bessel function replaces $e(mz)$. Take $V = Y_0$, $X = X_0$ and $G := U(Y_0)$, with the forms $H(Y_0)$, a finite-dimensional space with the Petersson inner product, and the source forms S, as in Chapter 34. On the Bessel subgroup of the data the proof fixes a generic character $\psi_{\mathcal{U}}$ and a quotient measure; no comparison with the character of Section 36.1 is made here.

Definition 36.2.1 (Poincaré maps)**.** Let λ be a linear form on the values of the source forms and g a point of the archimedean unitary group of Y_0. (From here on λ is such a linear form; the homomorphism $\lambda\colon \mathcal{U} \to E$ of Section 36.1 enters only through $\psi_{\mathcal{U}}$.) For $\varphi \in S$, the *Bessel function of φ formed with λ* is $\mathcal{W}_{\lambda,\varphi}(nh) := \psi_{\mathcal{U}}(n)\,\lambda\big(h_\infty^{-1}\varphi(h_f)\big)$ for $n \in \mathcal{U}(\mathbb{A}_F)$ and $h \in U(X_0)(\mathbb{A}_F)$, where h_∞^{-1} acts on the values. By the Riesz representation theorem there is a unique $\mathcal{P}_{g,\lambda}\varphi \in H(Y_0)$ with

$$\langle \mathcal{P}_{g,\lambda}\varphi, y\rangle = \int_{R(F)\backslash R(\mathbb{A}_F)} \mathcal{W}_{\lambda,\varphi}(x)\,\overline{y(xg)}\,dx \qquad (y \in H(Y_0)).$$

The linear map $\mathcal{P}_{g,\lambda}\colon S \to H(Y_0)$ is the *Poincaré map* of (g, λ): it represents a Bessel period of φ, linear in φ and conjugate-linear in y. The proof fixes one pair (g, λ); $\mathcal{P}$ without subscripts is the Poincaré map of this pair.

For the fixed pair, $\mathcal{P}\varphi$ is a Poincaré series for every φ: the sum over $\gamma \in G(F)$ of the translates of a seed made of each coordinate of the archimedean Bessel function, multiplied by a cutoff at the infinite places and by the indicator of a translate of the level at the finite places, one for each class; the coefficients are the Bessel coordinates of the values of a central translate of φ at class representatives.

At a fixed level on a definite group with one class, the forms are the vectors invariant under a finite group, and the series becomes a finite sum. Let Γ be a finite group acting unitarily on a space V_π, and let the forms on G be the vectors V_π^Γ, with $\|\psi\|^2 := |\Gamma|^{-1}\|\psi\|_{V_\pi}^2$, as in Chapter 21 for one class. Let $\Gamma_X \subset \Gamma$ be a subgroup, W a unitary representation of Γ_X, and $\jmath\colon W \to V_\pi$ a Γ_X-equivariant

linear map with $\|\jmath\xi\|^2_{V_\pi} = c_0\|\xi\|^2_W$ for a constant $c_0 > 0$. The forms on X are W^{Γ_X}, with $\|\xi\|^2 := |\Gamma_X|^{-1}\|\xi\|^2_W$. For $\psi \in V_\pi^\Gamma$ and $\xi \in W^{\Gamma_X}$ put

$$\mathrm{Per}(\psi,\xi) := |\Gamma_X|^{-1}\langle\psi, \jmath\xi\rangle_{V_\pi}, \qquad P\xi := \sum_{\gamma\in\Gamma/\Gamma_X} \gamma\,\jmath\xi.$$

Problem 36.2.1. $P\xi$ is well defined and lies in V_π^Γ, and $\langle\psi, P\xi\rangle = \mathrm{Per}(\psi,\xi)$ for every $\psi \in V_\pi^\Gamma$, where the left side is the inner product of forms.

Problem 36.2.2. The adjoint of $P\colon W^{\Gamma_X} \to V_\pi^\Gamma$ for the two norms of forms is $P^*\psi = \jmath^*\psi$, where $\jmath^*$ is the adjoint for the inner products of W and V_π. In particular $P \neq 0$ if and only if $\mathrm{Per}(\psi,\xi) \neq 0$ for some ψ and ξ.

Problem 36.2.3. Let $(W', \jmath')$ be a second pair as above, with Poincaré map P'. For $\xi \in W^{\Gamma_X}$ and $\xi' \in W'^{\Gamma_X}$,

$$\langle P\xi, P'\xi'\rangle = \sum_{\delta\in\Gamma_X\backslash\Gamma/\Gamma_X} \frac{\langle\delta\,\jmath\xi, \jmath'\xi'\rangle_{V_\pi}}{|\Gamma_X \cap \delta\Gamma_X\delta^{-1}|},$$

and if $(W', \jmath') = (W, \jmath)$ the term of $\delta = 1$ is $c_0\langle\xi,\xi'\rangle$, the inner product of forms.

So $\mathcal{K} := c_0^{-1}P^*P$ is the identity plus a sum over the nontrivial double cosets. This is the finite form of Petersson's formula, Theorem 10.2.1, where the double cosets $\Gamma_\infty\backslash\Gamma/\Gamma_\infty$ give the Kloosterman terms.

36.3. The smallest case

Take $\mathcal{O} = \mathbb{Z}[\mathrm{i}]$, $\Gamma := \Gamma_{I_2}$, of order 32 by Problem 21.1.2, and $\mathrm{Cl}_2 = \{I_2\}$ by Problem 21.1.4. Let $\mathbf{e}_1, \mathbf{e}_2$ be the standard basis of $\mathbb{C}^2$, $z := \mathbf{e}_2$ and $X := \mathcal{O}\mathbf{e}_1$; here $h(z,z) = 1$, since everything is definite. The stabilizer of z is $\Gamma_X = \{\mathrm{diag}(u,1) : u \in \mu_4\}$. In this section, as in Chapter 21, $a \geq 0$ is the degree of a symmetric power (not the scale of Chapter 33), and $0 \leq j, j' \leq a$ are integers. Let $V_\pi := \mathrm{Sym}^a(\mathbb{C}^2)$, $W := \mathrm{Sym}^j(\mathbb{C}\mathbf{e}_1)$ and $\jmath(\xi) := \xi\,\mathbf{e}_2^{a-j}$. When $4 \mid j$ and $4 \mid a-j$, Per is the period $P(\psi,\xi)$ of Section 23.4, and Problem 36.2.1 says that it is the inner product with $P\xi$. For $4 \mid j$ let $\xi_j \in W^{\Gamma_X}$ be the form with value $\mathbf{e}_1^j$.

Problem 36.3.1. $\Gamma_X\backslash\Gamma/\Gamma_X$ has five elements: the classes of $\mathrm{diag}(1,u)$, $u \in \mu_4$, with four elements each, and the class of the sixteen antidiagonal matrices.

Problem 36.3.2. Let $4 \mid j$. Then $P\xi_j = 4\big(\mathbf{e}_1^j\mathbf{e}_2^{a-j} + \mathbf{e}_1^{a-j}\mathbf{e}_2^j\big)$ if $4 \mid a$, and $P\xi_j = 0$ otherwise. For $a = 8$: $P\xi_0 = 4(\mathbf{e}_1^8 + \mathbf{e}_2^8)$ and $P\xi_4 = 8\mathbf{e}_1^4\mathbf{e}_2^4$.

Problem 36.3.3. Here $c_0 = \binom{a}{j}^{-1}$. Let $4 \mid a$ and $4 \mid j, j'$, and put $\mathcal{K}_{jj'} := \big(c_0(j)c_0(j')\big)^{-1/2}\langle P\xi_j, P\xi_{j'}\rangle/(\|\xi_j\|\|\xi_{j'}\|)$. Then

$$\mathcal{K}_{jj'} = 4\big(\delta_{jj'} + \delta_{j',a-j}\big).$$

In the expansion of Problem 36.2.3 the identity class contributes $\delta_{jj'}$ to $\mathcal{K}_{jj'}$, the three classes $\mathrm{diag}(1,u)$ with $u \neq 1$ together contribute $3\delta_{jj'}$, and the antidiagonal class contributes $4\delta_{j',a-j}$.

Problem 36.3.4. Let $4 \mid a$. The forms $P\xi_j$ with $4 \mid j$ and $2j \leq a$ are an orthogonal basis of $\mathcal{A}_{(a)}(2)$, their number is $\lfloor a/8\rfloor + 1$, and $P\xi_{a-j} = P\xi_j$.

Here different indices can give the same series; in Problem 10.1.3 two Poincaré series are proportional.

Problem 36.3.5. Let $4 \mid a$ and $D^* := 4\,\mathrm{mass}_2 \dim \mathrm{Sym}^a(\mathbb{C}^2)$. Then $D^* = (a+1)/8$, and $0 < \dim \mathcal{A}_{(a)}(2) - D^* \le 7/8$.

So for $4 \mid a$ the series $P\xi_j$ with $4 \mid j$ and $0 \le 2j < a$ are orthogonal and span a subspace of codimension at most one, and $\dim \mathcal{A}_{(a)}(2)$ is D^* up to a bounded error, as $\dim S_k$ is $(k-1)/12$ up to a bounded error for even $k \ge 4$ in Problem 10.4.2. But their diagonal Gram entries are 4, not 1: the elements $\mathrm{diag}(1,u)$ with $u \ne 1$, which preserve the line Ez without fixing z, each contribute as much as the identity. The toy has nothing to average over. (Problems 37.1.7 and 37.1.6 make this precise.) In the proof a finite level group acts on the forms of principal level and translates one Poincaré map.

36.4. Translates of one Poincaré map

The proof gives three estimates for the scaled Poincaré map of the data: a second moment over the finite group (Theorem 40.3.1), the near isometry of its projection to the good forms (Theorem 41.2.2), and an upper bound for the dimension of the target (Theorem 41.3.1). We apply the two translate theorems of Chapter 9 to obtain Theorem 36.4.1 and, using also the dimension bound for S_{ram}, Theorem 36.4.2. How small can the second moment of the Gram operators between a Poincaré map and its translates be, and how does its upper bound combine with near isometry of the projected map to give a spanning estimate?

Let ρ be a unitary representation of a finite group $\bar{G}$ on a finite-dimensional space $\mathcal{Y}$, let $\mathcal{X}$ be a finite-dimensional inner product space, and let $\mathcal{P}^\circ \colon \mathcal{X} \to \mathcal{Y}$ be linear. Put $\mathcal{K}_s := \mathcal{P}^{\circ *}\rho(s)\mathcal{P}^\circ \in \mathrm{End}\,\mathcal{X}$ for $s \in \bar{G}$; it is the *Gram operator* between $\mathcal{P}^\circ$ and its translate $\rho(s)\mathcal{P}^\circ$. Recall two facts from Chapter 9. By Problem 9.2.2, $\mathrm{Tr}\big((\rho(s)\mathcal{P}^\circ\mathcal{P}^{\circ *}\rho(s)^{-1})(\rho(t)\mathcal{P}^\circ\mathcal{P}^{\circ *}\rho(t)^{-1})\big) = \|\mathcal{K}_{s^{-1}t}\|^2$, so $s \mapsto \|\mathcal{K}_s\|^2$ is of *positive type*: there are vectors u_s, $s \in \bar{G}$, of an inner product space with $\langle u_s, u_t\rangle = \|\mathcal{K}_{s^{-1}t}\|^2$. By Problem 9.2.5, if p is the orthogonal projection onto a $\bar{G}$-stable subspace $\mathcal{Y}_0$ and $p\mathcal{P}^\circ$ is an isometry, then $\dim \mathcal{Y}_0 \sum_{s\in\bar{G}} \|\mathcal{K}_s\|^2 \ge \#\bar{G}\,(\dim \mathcal{X})^2$. Chapter 37 computes the Gram operators of a Poincaré map on a finite group: there the lower bound is attained when the weight is irreducible (Problems 37.1.4 and 37.2.1), and the translates by a subgroup act on the source through a representation, as $\bar{R}_0$ does below.

Definition 36.4.1 (the scaled Poincaré map)**.** We use $\mathcal{M} = \mathcal{M}_0 \cup \mathcal{M}_1$, $\bar{G} = \bar{G}_0 \times \bar{G}_1$, ρ on $H(Y_0)$, e_0, $T = e_0H(Y_0)$, d_T, $S \supseteq S_{\mathrm{ram}}$ and $D_X = \dim S$ as in Chapter 34; for the data, $b \ge 1000$. A finite adelic element of $U(Y_0)$ is *integral* if its matrix in the lattice basis of the proof, to which the vectors v_a, z, v_a' of Section 36.1 belong, is integral at every finite place; its *reduction* is then the family of its residues at the places $w \in \mathcal{M}$, an element of $\bar{G}$. The integral elements with reduction 1 form the principal level K_M. The *classes* c are the double cosets of the finite adelic points of $U(X_0)$ by the rational points and the level of the source forms; each has a representative h_c, viewed in $U(Y_0)$. A *Bessel coordinate* $i = (i_\tau)_\tau$ is a tuple of coordinates of the archimedean Bessel functions, one at each infinite place. The *coordinate space* has an orthonormal basis $e_{c,i}$ indexed by the pairs of a class and a Bessel coordinate. Let C be the coefficient isomorphism of the Poincaré series of Section 36.2, from S to the coordinate space: it translates a source form by a fixed central element and evaluates it at the class representatives in Bessel coordinates. Give S the inner product transported by C. Let $\nu > 0$ be the

covolume, for the product of the local Bessel Haar measures on the real unipotent group, of the lattice of $n \in \mathcal{U}(F)$ with $h_c^{-1} n_f h_c \in K_M$; it is the same for every class. (In this Part the letter ν has no other meaning.) The *scaled Poincaré map* and its *Gram operators* are

$$\mathcal{P}^\circ := (\mathrm{vol}(K_M)\,\nu)^{-1/2}\,\mathcal{P} \circ C^{-1}, \qquad \mathcal{K}_s := \mathcal{P}^{\circ *}\rho(s)\mathcal{P}^\circ \quad (s \in \bar{G}),$$

a map from the coordinate space to $H(Y_0)$ and operators on the coordinate space. Further, G_∞ is the product over the infinite places of the real groups of Y_0, in the rescaled bases of the proof, and dy its product measure; γ_∞ and γ_f are the components of a rational $\gamma \in U(Y_0)(F)$ in G_∞ and in the finite adelic group; deg is the product over the infinite places of the degree constants of the Bessel systems (formal degrees), and mass_r is the mass $\sum 1/\#\mathrm{Aut}$ of the genus of the standard lattice of rank r.

Definition 36.4.2 (the Bessel representation)**.** Let $\bar{R}_0 \subseteq \bar{G}$ be the group of reductions of the integral points of the finite adelic Bessel subgroup. For $s \in \bar{G}$, $\rho_{\mathrm{Bes}}(s)$ is the operator on the coordinate space whose $((c,i),(c',i'))$ entry is the complex conjugate of ν^{-1} times the sum, over the $\gamma \in R(F)$ with $h_c^{-1}\gamma_f h_{c'}$ integral of reduction s, of the integrals

$$\int_{G_\infty} u_c(y)\, u_{c'}(\gamma_\infty^{-1} y)\, W_i(y)\, \overline{W_{i'}(\gamma_\infty^{-1} y)}\, dy.$$

Here u_c is the class cutoff and W the full Bessel function; both are made precise in Chapter 37 (Theorem 37.3.1 and Definition 37.3.1), in whose notation the entry is the complex conjugate of $\nu^{-1}\mathrm{Amp}(R(F); c, s, c')_{ii'}$. The proof shows that $\rho_{\mathrm{Bes}}(s) = 0$ for $s \notin \bar{R}_0$ and that ρ_{Bes} is a unitary representation of $\bar{R}_0$ on the coordinate space.

The same sums taken over all $\gamma \in U(Y_0)(F)$ give the entries of $\mathcal{K}_s$: this is the block identity, Theorem 37.3.2, the analogue of Problem 36.2.3. It implies $\rho(t)\mathcal{P}^\circ = \mathcal{P}^\circ \rho_{\mathrm{Bes}}(t)$ for $t \in \bar{R}_0$ (Problem 37.4.1).

Fillings. The proof establishes the estimates of this Part not only for the data. A *filling* consists of a CM field E with a CM type, the integers ϱ and k of Section 36.1, a prime N, two further primes p_0, p_1 with, for each, a set of f chosen places of norm p_i (f the number of infinite places of E; no chosen place is conjugate to a chosen place), a real $b \geq 1000$, a level in $U(X_0)$ whose classes have trivial stabilizers, and a Bessel system at each infinite place, subject to size conditions in powers of b. It is *admissible* if it satisfies the further standing hypotheses of the proof; the data give an admissible filling. For a filling, $\bar{G}$, the classes, the coordinate space, ν, $\bar{R}_0$, ρ_{Bes}, deg and mass_r are defined as above, D_X is the dimension of the coordinate space, and a linear map from the coordinate space to a representation ρ of $\bar{G}$ *satisfies the block identity* if the identity of Theorem 37.3.2 holds with this map in place of $\mathcal{P}^\circ$. The field has *Weil data* if it contains a primitive 5040-th root of unity and carries the further choices, a splitting character among them, with which the proof forms theta lifts; the field of the data has them. The two properties of ρ_{Bes} in Definition 36.4.2 hold for every admissible filling over a field containing a primitive 5040-th root of unity. Chapters 38, 39, 40 and 41 say for which fillings each estimate is proved; the reader may take the data throughout.

The second moment over the whole group is Theorem 40.3.1: with $D_{\text{main}} = D_X^2/(\deg \cdot \text{mass}_r)$ (Definition 37.3.2),

$$\sum_{s\in\bar G} \|\mathcal{K}_s\|^2 \le (1+9b^{-4})\, D_{\text{main}}.$$

Chapter 40 proves it from the estimates of Chapters 38 and 39, which rest on statements read from the proof. Two of them, which Chapter 38 derives, concern the reductions near the Bessel subgroup: for $j = 0, 1$, the sum of $\|\mathcal{K}_s - \rho_{\text{Bes}}(s)\|^2$ over the $s \in \bar G$ whose component in $\bar G_j$ equals that of an element of $\bar R_0$ is at most $b^{-12}\, \#\bar R_0\, D_X$ (Theorem 38.3.3); hence $\|\mathcal{P}^{\circ *}\mathcal{P}^\circ - 1\|^2 \le b^{-12} D_X$ and $\|\mathcal{K}_1\|^2 \le 2D_X$ (Problem 38.3.9). In the toy of Section 36.3 the second estimate fails (Problem 37.1.7); Problem 37.1.6 shows how a level repairs it.

The second moment is to be compared with the target. By Theorem 41.3.1,

$$d_T \le \#\bar G \cdot \deg \cdot \text{mass}_r.$$

Its proof compares the good forms on Y_0 with those on the definite space W_m; there the principal level is free, and the forms of the chosen weight have dimension exactly $\#\bar G \cdot \text{mass}_r \cdot \deg$. Problem 36.3.5 shows the correction at a level with stabilizers. With Theorem 40.3.1 this gives (Problem 41.3.6)

$$d_T \sum_{s\in\bar G} \|\mathcal{K}_s\|^2 \le \#\bar G\, (1+9b^{-4})\, D_X^2,$$

$1 + 9b^{-4}$ times the lower bound of Problem 9.2.5 for an exactly isometric projected map, with $\mathcal{Y}_0 = T$.

Good forms. Recall from Chapter 9 that $L\colon \mathcal{X} \to \mathcal{Y}$ is a near isometry with error ε if $\dim Z - \varepsilon \dim \mathcal{X} \le \|L \operatorname{pr}_Z\|^2$ for every subspace $Z \subset \mathcal{X}$, where pr_Z is the orthogonal projection onto Z, and that by Problem 9.3.1 this holds if $\varepsilon \ge 0$ and $\|L^*L - 1\|^2 \le \varepsilon^2 \dim \mathcal{X}$. By Theorem 41.2.2, $e_0\mathcal{P}^\circ$ is a near isometry with error $5b^{-4}$:

$$\|e_0\mathcal{P}^\circ \operatorname{pr}_Z\|^2 \ge \dim Z - 5b^{-4} D_X \qquad \text{for every subspace } Z \text{ of the coordinate space.}$$

Its proof writes the action of e_0 as a product of two commuting projections, one for each level prime, and bounds what each removes from $\mathcal{P}^\circ$ by a trace against ρ_{Bes}.

Few translates. Recall Theorems 9.3.1 and 9.4.1. *One translate*: let ρ be unitary, p the orthogonal projection onto a $\bar G$-stable subspace $\mathcal{Y}_0$, $\varepsilon \ge 0$, $p\mathcal{P}^\circ$ a near isometry with error ε, and $\dim \mathcal{Y}_0 \sum_s \|\mathcal{K}_s\|^2 \le \#\bar G\, (1+\varepsilon)(\dim \mathcal{X})^2$. Then for every subspace $\mathcal{F} \subset \mathcal{Y}_0$, with $\omega := \dim \mathcal{F}/\dim \mathcal{Y}_0$ if $\mathcal{Y}_0 \ne 0$ and $\omega := 0$ otherwise, some $s \in \bar G$ has $\dim\{x \in \mathcal{X} : p\rho(s)\mathcal{P}^\circ x \in \mathcal{F}\} \le \big(\frac{1+\omega}{2} + \frac{3}{2}\varepsilon\big) \dim \mathcal{X}$. *Few translates*: let $(B_s\colon \mathcal{X} \to \mathcal{Y}_0)_{s\in\mathcal{I}}$ be a family of linear maps between finite-dimensional complex spaces, indexed by a set $\mathcal{I}$, with $\mathcal{X} \ne 0 \ne \mathcal{Y}_0$ and $0 < \varepsilon < 1/16$, such that for every subspace $\mathcal{F} \subset \mathcal{Y}_0$ some s has $\dim B_s^{-1}(\mathcal{F}) \le \big(\frac{1+\omega}{2} + \frac{3}{2}\varepsilon\big) \dim \mathcal{X}$. Then there is a finite set $J \subset \mathcal{I}$ with

$$\#J \cdot \dim \mathcal{X} \le \tfrac{5}{2}\big(1 + \log \tfrac{1}{16\varepsilon}\big) \dim \mathcal{Y}_0, \qquad \dim \sum_{s\in J} B_s(\mathcal{X}) \ge (1 - 16\varepsilon) \dim \mathcal{Y}_0.$$

Problem 36.4.1. Let $\varepsilon := (8b^2)^{-1}$. (a) If $b \ge 9$, then $5b^{-4} \le \varepsilon$ and $9b^{-4} \le \varepsilon$. (b) If $b^2 \ge 2$, then $16\varepsilon = 2b^{-2}$ and $\frac{5}{2}\big(1 + \log(b^2/2)\big) \le 5\log(1 + 2b^2)$; if $b^2 > 2$, then $0 < \varepsilon < 1/16$.

By Problem 36.4.1(a), Theorems 41.2.2, 40.3.1 and 41.3.1 give the hypotheses of the first lemma with $\varepsilon = (8b^2)^{-1}$ and $\mathcal{Y}_0 = T$. Nonzero scalars and the isomorphism C do not change the dimensions of preimages.

Theorem 36.4.1 (one translate)**.** *For every subspace $\mathcal{F} \subset T$, with $\omega := \dim \mathcal{F}/d_T$ (and $\omega := 0$ if $d_T = 0$), there is $s \in \bar{G}$ such that the preimage of $\mathcal{F}$ under $e_0\rho(s)\mathcal{P}\colon S \to T$ has dimension at most $\big(\frac{1+\omega}{2} + \frac{3}{2}(8b^2)^{-1}\big)D_X$.*

Ramified forms. Theorem A of Chapter 42 concerns the ramified source forms S_{ram}, defined with the operators T_w, $w \mid \pi_N$, in Chapter 34; there are f such places, and $T_w^{N-1} = 1$. The proof shows $D_X > 0$, $\dim S_{\mathrm{ram}} \geq (1 - f/(N-1))D_X$ and $f/(N-1) \leq b^{-8}$.

Problem 36.4.2. For each $w \mid \pi_N$, $(N-1)^{-1}\sum_{i=0}^{N-2} T_w^i$ is the projection of S onto the fixed vectors of T_w along its other eigenspaces, and $\ker \sum_{i=0}^{N-2} T_w^i$ is the sum of the eigenspaces of T_w for eigenvalues $\neq 1$.

Problem 36.4.3. For linear maps $B_s\colon \mathcal{X} \to \mathcal{Y}$, a finite set J of indices and a subspace $Z \subset \mathcal{X}$, $\dim \sum_{s\in J} B_s(\mathcal{X}) \leq \dim \sum_{s\in J} B_s(Z) + \#J\,(\dim \mathcal{X} - \dim Z)$.

Problem 36.4.4. For $b \geq 2$, $5b^{-8}\log(1 + 2b^2) \leq 2b^{-2}$. Hence if $\#J \cdot D_X \leq 5d_T \log(1+2b^2)$ and $\dim S_{\mathrm{ram}} \geq (1-b^{-8})D_X$, then $\#J\,(D_X - \dim S_{\mathrm{ram}}) \leq 2b^{-2}d_T$.

The target is not zero, since the source is not zero and $e_0\mathcal{P}^\circ$ is a near isometry with error less than 1. Theorem 36.4.1, the second lemma with Problem 36.4.1(b), and Problems 36.4.3 and 36.4.4 prove the following.

Theorem 36.4.2 (Theorem B)**.** *For all data of Chapter 33, $d_T > 0$, and there is a finite set $J \subseteq \bar{G}$ with*

$$\#J \cdot \dim S_{\mathrm{ram}} \leq 5\,d_T \log(1+2b^2) \qquad \text{and} \qquad (1-4b^{-2})\,d_T \leq \dim \sum_{s\in J} e_0\rho(s)\mathcal{P}(S_{\mathrm{ram}}).$$

These maps $e_0\rho(s)\mathcal{P}$ on S_{ram} have the same ranges as the maps A_s of Chapter 42, which differ from them by the nonzero scalar $c_B c_{\mathrm{ss}}^{-1}\#\bar{G}$. Before restriction to S_{ram} the missing dimension is at most $2b^{-2}d_T$; the restriction costs at most a further $2b^{-2}d_T$. This is the step of the proof that supplies enough forms: Theorem 36.4.2 is the statement used, with Theorem A, in the final chapter.

In the Lean formalization. In the Lean proof [GL]: the Poincaré maps of Definition 36.2.1 are `Data.poincareAt`, with `inner_poincareAt`, and that of the fixed pair is `Data.poincare`; the scaled map is `Data.scaledPoincare`; ρ_{Bes} is `Filling.besselTranslate`, with `besselTranslate_eq_zero`, `besselTranslate_one`, `besselTranslate_mul` and `adjoint_besselTranslate` for its two properties; fillings are `Filling`, with `Filling.IsAdmissible` and `WeilData`. Theorem 36.4.1 follows from `isSpread_goodPoincare`, since `Data.goodPoincare` at s is $\#\bar{G}\,e_0\rho(s)\mathcal{P}$ and multiplication by $\#\bar{G}$ preserves the preimage of every subspace. The bounds for S_{ram} are `le_finrank_ramifiedSourceForms` and `f_div_N_sub_one_le`, and $D_X > 0$ is part of `Filling.Fits.finrank_levelSpace_eq_sourceDim`. Theorem 36.4.2 follows from `Data.enough_forms` for the normalized maps A_s, using `range_normalizedPoincare` and the nonzero factor $\#\bar{G}$.

Hints

§36.1.

36.1.1: Write $nv_{a+1} = v_{a+1} + \sum_{c \le a} x_c(n) v_c$, and compute the coefficients of $nn' v_{a+1}$; an element of $U(X)$ fixes every v_c and z.

36.1.2: An element of $U(X)$ preserves the span of the v_a and its orthogonal complement.

36.1.3: First the unipotent radical of the stabilizer of $Ev_1 + \cdots + Ev_\varrho$: $2\varrho(r - 2\varrho)$ dimensions from maps between the quotient, the middle and the isotropic subspace, and ϱ^2 from a skew-hermitian matrix over E. Then the unipotent radical of a Borel subgroup of $\mathrm{GL}_\varrho(E)$.

§36.2.

36.2.1: $\jmath\xi$ is fixed by Γ_X, and $\langle \psi, \gamma v \rangle = \langle \gamma^{-1}\psi, v \rangle$.

36.2.2: Problem 36.2.1.

36.2.3: Apply Problem 36.2.1 with $\psi = P\xi$, and group the cosets $\gamma\Gamma_X$ by double cosets.

§36.3.

36.3.1: Multiply $\mathrm{diag}(u_1, u_2)$ and the antidiagonal matrices by $\mathrm{diag}(u, 1)$ on both sides.

36.3.2: Representatives of Γ/Γ_X: $\mathrm{diag}(1, u)$ and $\begin{pmatrix} 0 & u \\ 1 & 0 \end{pmatrix}$; sum the powers of u.

36.3.3: Problem 21.3.2 for c_0; then Problems 36.2.3 and 36.3.1.

36.3.4: Problem 21.3.5.

36.3.5: Write $a = 8q$ or $a = 8q + 4$.

§36.4.

36.4.1: For (b), $\log(1 + 2b^2) \ge 1$ and $b^2/2 \le 1 + 2b^2$.

36.4.2: T_w is diagonalizable.

36.4.3: Choose a complement of Z in $\mathcal{X}$.

36.4.4: $\log(1 + 2b^2) \le 2b^2$.

References

[GGP] W. T. Gan, B. H. Gross and D. Prasad, *Symplectic local root numbers, central critical L-values, and restriction problems in the representation theory of classical groups*, Astérisque **346** (2012), 1–109.

[GL] L. Sernau, *GRH for Dirichlet L-functions, in Lean 4*, a shorter rewriting of the Lean proof, text by Claude, `https://github.com/lsernau/grh-lean`, commit `72fead1`, readable edition `grh/`.

UNFOLDING TWICE: GRAM OPERATORS AS SUMS OVER RATIONAL POINTS

Prerequisites. From Chapter 36: Sections 36.1–36.3, in particular Problems 36.2.3 and 36.3.3, and the scaled Poincaré map $\mathcal{P}^\circ$, its Gram operators $\mathcal{K}_s = \mathcal{P}^{\circ *}\rho(s)\mathcal{P}^\circ$, the covolume ν, the group $\bar{R}_0 \subseteq \bar{G}$ and its representation ρ_{Bes}, from Section 36.4 (Definitions 36.4.1 and 36.4.2), and Theorem 36.4.2. From Chapter 9: Hilbert–Schmidt norms (Problem 9.2.1) and Problems 9.2.2 and 9.2.5. From Chapter 10: Poincaré series on $\mathrm{SL}_2(\mathbb{Z})$, Problems 10.1.1, 10.2.1 and 10.2.4 with its proof, and Theorem 10.2.1. From Chapter 21: Problems 21.1.2 and 21.3.2. From Chapters 33 and 34: the data, $\bar{G}$, the source S and $D_X = \dim S$. Schur orthogonality for finite groups [Se, §2.2]. As in Chapter 36, inner products are linear in the first variable, norms of operators are Hilbert–Schmidt norms, and a function Θ on a group is of *positive type* if $\Theta(s^{-1}t) = \langle u_t, u_s\rangle$ for some vectors u_s.

This sheet serves the second moment in the proof of Theorem 36.4.2 of Chapter 36. There the scaled Poincaré map $\mathcal{P}^\circ$ is translated by the finite group $\bar{G}$, and the sizes of the Gram operators $\mathcal{K}_s$ decide how many translates span the target. The proof computes $\mathcal{K}_s$ by unfolding twice, as Petersson's formula computes the inner product of two Poincaré series: each entry of $\mathcal{K}_s$ becomes a sum over the rational points whose reduction is s. What does this sum look like when the group is finite, which part of it is forced, and what is the least possible second moment $\sum_s \|\mathcal{K}_s\|^2$?

37.1. A finite model

Over a definite unitary group with one class, at the principal level of an ideal, a form is a function on the finite group $\bar{G}$ of residues, equivariant for the integral points. We take this as the model.

Definition 37.1.1. A *finite model* consists of a finite group $\bar{G}$, a subgroup $\Gamma \subseteq \bar{G}$ (the integral points), a unitary representation π of Γ on a space V_π, a subgroup $\Gamma_X \subseteq \Gamma$, a unitary representation σ_X of Γ_X on a space V_X, and a Γ_X-equivariant linear map $\jmath\colon V_X \to V_\pi$ with $\jmath^*\jmath = c_0$ for a constant $c_0 > 0$. Its *forms* are the functions $\varphi\colon \bar{G} \to V_\pi$ with $\varphi(\gamma g) = \pi(\gamma)\varphi(g)$ for $\gamma \in \Gamma$; they form a space $\mathcal{Y}$ with $\langle \varphi, \varphi'\rangle := \sum_{g\in\Gamma\backslash\bar{G}} \langle \varphi(g), \varphi'(g)\rangle$, on which $\bar{G}$ acts by $(\rho(s)\varphi)(g) := \varphi(gs)$. Its *Poincaré map* $P\colon V_X \to \mathcal{Y}$ sends w to the function equal to $c_0^{-1/2}\pi(g)\jmath w$ at $g \in \Gamma$ and to 0 off Γ.

In this sheet P without subscript is always this map. In a finite model we write $\mathcal{K}_s := P^*\rho(s)P$, $\bar{R}_0 := \Gamma_X$, $\rho_{\mathrm{Bes}}(s) := \sigma_X(s)$ for $s \in \Gamma_X$ and $\rho_{\mathrm{Bes}}(s) := 0$ for $s \notin \Gamma_X$, and $D_X := \dim V_X$: they play the parts of the objects of the same names in Chapter 36.

Problem 37.1.1. $Pw \in \mathcal{Y}$, and $\langle \varphi, Pw\rangle = c_0^{-1/2}\langle \varphi(1), \jmath w\rangle$ for $\varphi \in \mathcal{Y}$: the map P represents the period $\varphi \mapsto c_0^{-1/2}\jmath^*\varphi(1)$.

Date: November 26, 2026.

Problem 37.1.2. $\mathcal{K}_s = c_0^{-1} \jmath^* \pi(s) \jmath$ for $s \in \Gamma$, and $\mathcal{K}_s = 0$ for $s \notin \Gamma$. In particular P is an isometry.

Problem 37.1.3. $\mathcal{K}_s = \rho_{\mathrm{Bes}}(s)$ for $s \in \bar{R}_0$. For $t \in \bar{R}_0$ and $s \in \bar{G}$, $\rho(t)P = P\rho_{\mathrm{Bes}}(t)$ and $\mathcal{K}_{st} = \mathcal{K}_s \rho_{\mathrm{Bes}}(t)$.

Problem 37.1.4. Let $\Gamma_X = \Gamma$, $V_X = V_\pi$ and $\jmath = 1$. Then $\dim \mathcal{Y} = [\bar{G} : \Gamma] \dim V_\pi$, $\sum_{s \in \bar{G}} \|\mathcal{K}_s\|^2 = \#\Gamma \dim V_\pi = \#\bar{G} (\dim V_\pi)^2 / \dim \mathcal{Y}$, and if J is a set of representatives of the cosets $s\Gamma$, then $\mathcal{Y}$ is the orthogonal sum of the $\rho(s)P(V_\pi)$, $s \in J$.

Now the smallest case. Let Γ_{I_2} be the group of monomial 2×2 matrices with entries in μ_4, of order 32 by Problem 21.1.2. In $\mathbb{F}_5$ the element 3 is a square root of -1, and reduction modulo $2 + \mathrm{i}$ is the ring map $\mathbb{Z}[\mathrm{i}] \to \mathbb{F}_5$, $\mathrm{i} \mapsto 3$.

Problem 37.1.5. Reduction modulo $2 + \mathrm{i}$ is an injective homomorphism $\Gamma_{I_2} \to \mathrm{GL}_2(\mathbb{F}_5)$, and its image Γ has index 15 in $\bar{G} := \mathrm{GL}_2(\mathbb{F}_5)$, a group of order 480. With π the standard representation of Γ_{I_2} on $V_\pi = \mathbb{C}^2$, transported to Γ, one has $\dim \mathcal{Y} = 30 = \#\bar{G} \cdot \mathrm{mass}_2 \cdot \dim V_\pi$, where $\mathrm{mass}_2 = 1/32$ is the mass of rank two, as in Chapter 36.

In this model take $\Gamma_X := \{\mathrm{diag}(u, 1) : u \in \mu_4\}$ (reduced modulo $2 + \mathrm{i}$), the stabilizer of $\mathbf{e}_2$ as in Section 36.3, $V_X := \mathbb{C}\mathbf{e}_1$ with $\sigma_X(\mathrm{diag}(u, 1)) = u$, and $\jmath$ the inclusion, so that $c_0 = 1$ and $D_X = 1$.

Problem 37.1.6. $\|\mathcal{K}_s\|^2 = 1$ for the 16 diagonal $s \in \Gamma$, and $\mathcal{K}_s = 0$ for the other 464 elements of $\bar{G}$. Hence $\sum_{s \in \bar{G}} \|\mathcal{K}_s\|^2 = 16$: the four elements of $\bar{R}_0$ contribute $\#\bar{R}_0 \cdot D_X = 4$, with $\mathcal{K}_s = \rho_{\mathrm{Bes}}(s)$ there, and the three cosets $\bar{R}_0 \,\mathrm{diag}(1, u)$, $u \neq 1$, contribute 4 each.

At level one the same elements land on the identity.

Problem 37.1.7. In the toy of Section 36.3, let $a \geq 4$ be divisible by 4, let the source be the orthogonal direct sum of the lines $\mathbb{C}\xi_j$ for $4 \mid j$ and $0 \leq 2j < a$, with their form norms, and let D_{toy} be its dimension. Let $\mathcal{K}$ be the operator whose matrix in the unit basis $(\xi_j / \|\xi_j\|)_j$ has the entries $\mathcal{K}_{jj'}$ of Problem 36.3.3. Then $\|\mathcal{K} - 1\|^2 = 9 D_{\mathrm{toy}} > b^{-12} D_{\mathrm{toy}}$ for every $b \geq 1$: the conclusion of Problem 37.4.3 below fails there.

By Problem 36.3.3 the excess $3\delta_{jj'}$ comes from the classes of $\mathrm{diag}(1, u)$, $u \neq 1$, which preserve the line of $z = \mathbf{e}_2$ without fixing z. In Problem 37.1.6 these elements reduce to $\mathrm{diag}(1, u) \notin \bar{R}_0$; they contribute to $\mathcal{K}_s$ for $s \neq 1$, and $\mathcal{K}_1 = 1$. The level has separated them from the Bessel subgroup.

37.2. The least second moment

By Problem 9.2.5, if p is the orthogonal projection onto a $\bar{G}$-stable subspace $\mathcal{Y}_0 \subseteq \mathcal{Y}$ and pP is an isometry, then $\#\bar{G}\, D_X^2 \leq \dim \mathcal{Y}_0 \cdot \sum_{s \in \bar{G}} \|\mathcal{K}_s\|^2$. When is this an equality?

Problem 37.2.1. If π is irreducible, then $\sum_{s \in \bar{G}} \|\mathcal{K}_s\|^2 = \#\Gamma\, D_X^2 / \dim V_\pi$, and equality holds in Problem 9.2.5 with $\mathcal{Y}_0 = \mathcal{Y}$. In Problem 37.1.6: $32 \cdot 1/2 = 16$ and $30 \cdot 16 = 480 = \#\bar{G}$.

Put $\deg := \dim V_\pi$, the formal degree of π for the Haar measure of total mass one, and $\mathrm{mass} := 1/\#\Gamma$. Then Problem 37.2.1 says that the second moment

equals $D_X^2/(\deg\cdot\mathrm{mass})$, the quantity D_{main} of Definition 37.3.2 below. Without irreducibility it is at least as large, by Problem 9.2.5, and it can be larger.

Problem 37.2.2. (a) Let $V_\pi = \mathrm{Sym}^a(\mathbb{C}^2)$, $a \geq 1$, with the inner product of Problem 21.3.2, the other data as in Problem 37.1.6 but $V_X = \mathbb{C}\,\mathbf{e}_1^j\mathbf{e}_2^{a-j}$, $0 \leq j \leq a$, with $\sigma_X(\mathrm{diag}(u,1)) = u^j$ and the norm induced from V_π. Then $\sum_s \|\mathcal{K}_s\|^2 = 16$, or 32 if $2j = a$, while $\#\Gamma\, D_X^2/\dim V_\pi = 32/(a+1)$; for $a = 8$, $j = 0$ the ratio is $9/2$. (b) Let $\bar{G} = \Gamma = S_3$ act on $V_\pi = \{x \in \mathbb{C}^3 : x_1 + x_2 + x_3 = 0\}$ by permuting coordinates, $\Gamma_X = 1$, $V_X = \mathbb{C}$ and $\jmath(1) = (\mathbf{e}_1 - \mathbf{e}_2)/\sqrt{2}$. In the lexicographic order of the permutations, written as $(s(1), s(2), s(3))$, the scalars $\mathcal{K}_s$ are $1, \frac{1}{2}, -1, -\frac{1}{2}, -\frac{1}{2}, \frac{1}{2}$, and $\sum_s |\mathcal{K}_s|^2 = 3 = 6/2$. Here π is irreducible, and this is the equality of Problem 37.2.1.

So D_{main} is the value for integral points that are equidistributed against the coefficients of π; in Problem 37.2.2(a) a finite group has too few. For the data the real group is not compact, and infinitely many rational γ lie over each s.

37.3. The block identity

In Chapter 10, unfolding $\langle P_n, P_m\rangle$ and expanding P_n group the terms by double cosets of Γ_∞.

Problem 37.3.1. In this problem and the next paragraph k, m, n, c and P_n are the weight, the two indices, the lower left entry and the Poincaré series of Chapter 10. By Problems 10.1.1 and 10.2.4, $\langle P_n, P_m\rangle = \Gamma(k-1)(4\pi m)^{1-k}p_n(m)$. In the series for P_n, the m-th Fourier coefficient of the sum of the terms with $\gamma \in \pm\Gamma_\infty$ is $\delta(n,m)$, and for each $c \geq 1$ that of the sum of the terms with lower left entry $\pm c$ is $2\pi \mathrm{i}^{-k}(m/n)^{(k-1)/2}c^{-1}S(n,m;c)J_{k-1}(4\pi\sqrt{mn}/c)$.

In Theorem 37.3.2 below, the rational points of the Bessel subgroup $R = \mathcal{U} \rtimes U(X_0)$ replace $\pm\Gamma_\infty$, a Bessel function at each infinite place replaces $e(mz)$, a pair of a class of $U(X_0)$ and a Bessel coordinate replaces m, and the sum over the rational γ outside the Bessel subgroup with reduction s replaces the Kloosterman terms $S(n,m;c)J_{k-1}$; the term $\delta(n,m)$ becomes $\rho_{\mathrm{Bes}}(s)$. The reduction $s \in \bar{G}$ has no counterpart at level one. The Bessel functions are the following.

Theorem 37.3.1 (Bessel functions)**.** *For the data, at each infinite place τ there are a finite nonempty set I_τ, a number $d_\tau > 0$ equal to the formal degree of the discrete series of the real unitary group G_τ of Y_0 with doubled Harish-Chandra parameter $2\varsigma_\tau$, an irreducible unitary representation of $U(X_0)_\tau$ on $\mathbb{C}^{I_\tau}$, and continuous functions $W_\tau, W_\tau^\flat \colon G_\tau \to \mathbb{C}^{I_\tau}$ such that:*

(a) *$W_\tau(xy) = \psi_{\mathcal{U}}(x)W_\tau(y)$ for $x \in \mathcal{U}_\tau$, and $W_\tau(hy)$ is the representation applied to $W_\tau(y)$ for $h \in U(X_0)_\tau$; the same holds for $W_\tau^\flat$;*

(b) *$\int_{\mathcal{U}_\tau\backslash G_\tau} W_{\tau,i}\overline{W_{\tau,j}} = \delta_{ij}$ for $i, j \in I_\tau$;*

(c) *$\int_{G_\tau} \left|\int_{\mathcal{U}_\tau\backslash G_\tau} \langle W_\tau(y), W_\tau(yg)\rangle\, dy\right|^2 dg = (\#I_\tau)^2/d_\tau$;*

(d) *by construction, $W_\tau^\flat$ is W_τ times a function of the Bessel length of y (a measure of the size of y modulo the Bessel subgroup on the left) with values in $[0,1]$, equal to 1 up to half the radius b^{6n+2}, $n = \varrho + 1$, and to 0 beyond the radius; and $\int_{\mathcal{U}_\tau\backslash G_\tau} \|W_\tau - W_\tau^\flat\|^2 \leq b^{-2r^3 f}\,\#I_\tau$;*

with further bounds that later sheets use.

Status: read from the proof, which constructs W_τ as an average of a discrete-series coefficient over the Bessel subgroup and shows by Laplace's method that the average is not zero; see the remark at the end of the chapter. We know no reference for the statement in this form. The formal degree and Schur orthogonality for discrete series are due to Harish-Chandra [HC66], [HC70]; (b) follows from the normalization $\int \|W_\tau\|^2 = \#I_\tau$ and the irreducibility, by Schur's lemma.

Write $W_i(y) := \prod_\tau W_{\tau,i_\tau}(y_\tau)$ for a Bessel coordinate $i = (i_\tau)_\tau$. The classes c with representatives h_c, the coordinates $e_{c,i}$ of the source (an orthonormal basis), the product G_∞ of the real groups in the rescaled bases with its product measure dy, the components γ_∞, γ_f of a rational $\gamma \in U(Y_0)(F)$, and integrality and reduction in the lattice basis are those of Definition 36.4.1. The *class cutoff* $u_c \geq 0$ is a measurable function on G_∞ whose translates by the rational points u of $\mathcal{U}$ with $h_c^{-1} u_f h_c$ in the principal level sum to 1.

Definition 37.3.1. For classes c, c' and $\gamma \in U(Y_0)(F)$, the *amplitude* of γ is the matrix with entries

$$\mathrm{Amp}_\gamma(c,c')_{ij} := \int_{G_\infty} u_c(y)\, u_{c'}(\gamma_\infty^{-1} y)\, W_i(y)\, \overline{W_j(\gamma_\infty^{-1} y)}\, dy.$$

For a set $\mathfrak{S} \subseteq U(Y_0)(F)$ and $s \in \bar{G}$, the *amplitude sum* $\mathrm{Amp}(\mathfrak{S}; c, s, c')$ is the sum of $\mathrm{Amp}_\gamma(c,c')$ over the $\gamma \in \mathfrak{S}$ such that $h_c^{-1}\gamma_f h_{c'}$ is integral with reduction s.

The following is the analogue of Problems 37.1.2 and 36.2.3.

Theorem 37.3.2 (the block identity)**.** *For all data, all classes c, c', Bessel coordinates i, j and $s \in \bar{G}$,*

$$\big\langle \mathcal{P}^\circ e_{c,i},\, \rho(s)\mathcal{P}^\circ e_{c',j} \big\rangle = \nu^{-1}\, \mathrm{Amp}\big(U(Y_0)(F); c, s, c'\big)_{ij}.$$

Equivalently, the $((c,i),(c',j))$ entry of $\mathcal{K}_s$ is the complex conjugate of $\nu^{-1}\mathrm{Amp}(U(Y_0)(F); c, s, c')_{ij}$.

Theorem 37.3.2 is not proved here; see the remark. Its proof unfolds one Poincaré series against the translate of the other, as in Problem 37.1.1; the coordinate $e_{c,i}$ selects the class c, and the finite indicator in the second series selects the γ of reduction s, as Γ does in Problem 37.1.2. Recall from Definition 36.4.2 that $\rho_{\mathrm{Bes}}(s)$ has the same entries with the sum restricted to the rational Bessel subgroup, that $\rho_{\mathrm{Bes}}(s) = 0$ for $s \notin \bar{R}_0$, and that ρ_{Bes} is a unitary representation of $\bar{R}_0$. Moreover, for the data, $\mathcal{K}_{st} = \mathcal{K}_s \rho_{\mathrm{Bes}}(t)$ for all $s \in \bar{G}$ and $t \in \bar{R}_0$, as in Problem 37.1.3.

Definition 37.3.2. $D_{\mathrm{id}} := \#\bar{R}_0 \cdot D_X$ and $D_{\mathrm{main}} := D_X^2/(\deg \cdot \mathrm{mass}_r)$, with deg the product of the d_τ and mass_r the mass of Chapter 36.

For the data, $b^{11kf} D_{\mathrm{id}} \leq D_{\mathrm{main}} \leq (M/b^6)^{kf} D_{\mathrm{id}}$; these two inequalities are read from the proof (see the remark).

Problem 37.3.2. $\|\mathcal{K}_s\|^2 = \nu^{-2} \sum_{c,c'} \|\mathrm{Amp}(U(Y_0)(F); c, s, c')\|^2$, where the norm of a matrix is the square root of the sum of the squared absolute values of its entries.

37.4. The Bessel subgroup and near isometry

The translates by $\bar{R}_0$ keep the special role they have in Problem 37.1.3. In Problems 37.4.1–37.4.5, ρ is a unitary representation of $\bar{G}$, and $\mathcal{P}^\circ$, $\mathcal{K}_s$, ρ_{Bes} need only satisfy the stated hypotheses.

Problem 37.4.1. If $\mathcal{K}_{st} = \mathcal{K}_s \rho_{\mathrm{Bes}}(t)$ for all $s \in \bar{G}$ and $t \in \bar{R}_0$, then $\rho(t)\mathcal{P}^\circ = \mathcal{P}^\circ \rho_{\mathrm{Bes}}(t)$ for $t \in \bar{R}_0$.

Problem 37.4.2. If in addition ρ_{Bes} is a unitary representation of $\bar{R}_0$, then $\mathcal{K}_{ts} = \rho_{\mathrm{Bes}}(t)\mathcal{K}_s$ for $t \in \bar{R}_0$, $s \in \bar{G}$, and $\|\mathcal{K}_t - \rho_{\mathrm{Bes}}(t)\| = \|\mathcal{P}^{\circ *}\mathcal{P}^\circ - 1\|$ for $t \in \bar{R}_0$. Moreover $\sum_{t \in \bar{R}_0} \|\rho_{\mathrm{Bes}}(t)\|^2 = D_{\mathrm{id}}$.

Problem 37.4.3. Under the hypotheses of Problem 37.4.2, if $\sum_{t \in \bar{R}_0} \|\mathcal{K}_t - \rho_{\mathrm{Bes}}(t)\|^2 \le b^{-12} D_{\mathrm{id}}$, then $\|\mathcal{P}^{\circ *}\mathcal{P}^\circ - 1\|^2 \le b^{-12} D_X$.

Problem 37.4.4. If $\|\mathcal{P}^{\circ *}\mathcal{P}^\circ - 1\|^2 \le b^{-12} D_X$ and $b \ge 1000$, then $\|\mathcal{K}_1\|^2 \le 2D_X$.

Problem 37.4.5. $s \mapsto \|\mathcal{K}_s\|^2$ is of positive type, and $\|\mathcal{K}_s\|^2 \le \|\mathcal{K}_1\|^2$ for every $s \in \bar{G}$.

Problem 37.4.6. In Problem 37.1.6, $D_{\mathrm{id}} = 4$ and $D_{\mathrm{main}} = 16$ (with deg and mass as in Section 37.2), so $D_{\mathrm{id}}/D_{\mathrm{main}} = 1/4$. For the data $D_{\mathrm{id}}/D_{\mathrm{main}} \le b^{-11kf}$: if $\|\mathcal{K}_1\|^2 \le 2D_X$, the elements of $\bar{R}_0$ contribute at most $2b^{-11kf} D_{\mathrm{main}}$ to $\sum_s \|\mathcal{K}_s\|^2$, so a second moment of size about D_{main} must come almost entirely from outside $\bar{R}_0$.

The hypothesis of Problem 37.4.3 follows, by dropping the terms with $s \notin \bar{R}_0$, from the estimate over the strip of Chapter 38. There the sum of $\|\mathcal{K}_s - \rho_{\mathrm{Bes}}(s)\|^2$ is written, by Theorem 37.3.2 and Problem 37.3.2, as a sum over the rational γ outside the Bessel subgroup, which that chapter estimates.

We have proved, in the finite model, the unfolding of the Gram operators, the role of the Bessel subgroup and the least second moment; for the data we have stated the block identity (Theorem 37.3.2) and the Bessel functions (Theorem 37.3.1), both taken from the proof, and derived from the block identity the norm formula of Problem 37.3.2, and from $\mathcal{K}_{st} = \mathcal{K}_s \rho_{\mathrm{Bes}}(t)$ the passage from the Bessel subgroup to near isometry and to $\|\mathcal{K}_1\|^2 \le 2D_X$. Also taken as given: the two properties of ρ_{Bes} recalled from Definition 36.4.2, the identity $\mathcal{K}_{st} = \mathcal{K}_s \rho_{\mathrm{Bes}}(t)$ for the data, and the two inequalities between D_{id} and D_{main}. What remains is the sum over the γ outside the Bessel subgroup: over a strip around $\bar{R}_0$ (Chapter 38) and then over all of $\bar{G}$, where it must be compared with D_{main}.

In the Lean formalization. In the Lean proof [GL], Theorem 37.3.2 is `Data.hasAmplitudeBlocks_scaledPoincare`, which is proved from `Filling.Fits.petersson_poincare`; the Lean inner product is conjugate-linear in its first variable, so its $\langle \rho(s)\mathcal{P}^\circ e_{c',j}, \mathcal{P}^\circ e_{c,i} \rangle$ is the left side of the display. The amplitude and the amplitude sum of Definition 37.3.1 are `Filling.amplitude` and `Filling.amplitudeSum`, the class cutoff is `Filling.classCutoff`, the sizes of Definition 37.3.2 are `Filling.identitySecondMoment` and `Filling.mainSecondMoment`, and their two inequalities for the data are fields of `Filling.IsAdmissible`. Theorem 37.3.1 is `Data.exists_besselSystem`, with the properties of the Bessel system it produces. The identity $\mathcal{K}_{st} = \mathcal{K}_s \rho_{\mathrm{Bes}}(t)$ is `Filling.HasAmplitudeBlocks.adjoint_comp_rep_mul_right`.

Hints

§37.1.

37.1.1: Only the coset Γ contributes to the inner product.

37.1.2: $\langle \rho(s)Pw, Pw' \rangle$ has at most one nonzero term, at the coset of 1.

37.1.3: $\jmath$ is equivariant and $\jmath^*\jmath = c_0$.
37.1.4: Problem 37.1.2; the support of $\rho(s)Pw$ is Γs^{-1}.
37.1.5: An element of Γ_{I_2} is determined by its residues, since μ_4 maps injectively into $\mathbb{F}_5^\times$.
37.1.6: Problem 37.1.2: $\mathcal{K}_s$ is the $(1,1)$ entry of the lift of s to Γ_{I_2}.
37.1.7: Problem 36.3.3.

§37.2.

37.2.1: Schur orthogonality: $\sum_{\gamma\in\Gamma}|\langle\pi(\gamma)v, v'\rangle|^2 = \#\Gamma\|v\|^2\|v'\|^2/\dim V_\pi$; apply it to an orthonormal basis of V_X and use Problem 37.1.2. For the equality, compute $\dim \mathcal{Y}$.
37.2.2: A monomial matrix sends a monomial to a multiple of a monomial.

§37.3.

37.3.1: Follow the proof of Problem 10.2.4, with Problem 10.2.1; for $c \neq 0$ the terms with lower left entry $\pm c$ are indexed by d modulo c and an integer translation, and Γ_∞ contains ± 1.
37.3.2: Problem 9.2.1 with the coordinate basis; complex conjugation does not change absolute values.

§37.4.

37.4.1: Compute $\mathcal{P}^{\circ *}\rho(s^{-1})d$ for $d := \rho(t)\mathcal{P}^\circ x - \mathcal{P}^\circ\rho_{\mathrm{Bes}}(t)x$.
37.4.2: Take adjoints in $\rho(t^{-1})\mathcal{P}^\circ = \mathcal{P}^\circ\rho_{\mathrm{Bes}}(t^{-1})$. Multiplication by a unitary does not change a Hilbert–Schmidt norm, and $\mathcal{K}_t = \mathcal{K}_1\rho_{\mathrm{Bes}}(t)$.
37.4.3: Problem 37.4.2: every term of the sum equals $\|\mathcal{P}^{\circ *}\mathcal{P}^\circ - 1\|^2$.
37.4.4: $\mathcal{K}_1 = \mathcal{P}^{\circ *}\mathcal{P}^\circ$, $\|1\|^2 = D_X$, and the triangle inequality.
37.4.5: Problem 9.2.2 and the Cauchy–Schwarz inequality; $\|\mathcal{P}^\circ\mathcal{P}^{\circ *}\| = \|\mathcal{P}^{\circ *}\mathcal{P}^\circ\|$.

References

[GL] L. Sernau, *GRH for Dirichlet L-functions, in Lean 4*, a shorter rewriting of the Lean proof, text by Claude, `https://github.com/lsernau/grh-lean`, commit `72fead1`, readable edition `grh/`.

[HC66] Harish-Chandra, *Discrete series for semisimple Lie groups. II*, Acta Math. **116** (1966), 1–111.

[HC70] Harish-Chandra, *Harmonic analysis on semisimple Lie groups*, Bull. Amer. Math. Soc. **76** (1970), 529–551.

[Se] J.-P. Serre, *Linear Representations of Finite Groups*, Grad. Texts in Math. 42, Springer, 1977.

WHICH TERMS SURVIVE: CHARACTERS, MINORS AND THE GAIN AT THE LEVEL

Prerequisites. From Chapter 37: amplitudes and amplitude sums $\mathrm{Amp}(\mathfrak{S}; c, s, c')$ over sets $\mathfrak{S}$ of rational points (Definition 37.3.1), the two sizes D_{id}, D_{main} (Definition 37.3.2), the block identity (Theorem 37.3.2), the full Bessel function W and its cut $W^\flat$ (Theorem 37.3.1), and Problems 37.4.3 and 37.4.4. From Chapter 36: the decomposition $Y_0 = \bigoplus_a Ev_a \oplus X_0 \oplus Ez \oplus \bigoplus_a Ev'_a$ with $h(z,z) = -N$, the groups $\mathcal{U}$ and $R = \mathcal{U} \rtimes U(X_0)$ (Section 36.1); the coordinate space with basis $e_{c,i}$, the scaled Poincaré map $\mathcal{P}^\circ$, the Gram operators $\mathcal{K}_s$ and the covolume ν (Definition 36.4.1); $\bar{R}_0$ and ρ_{Bes} (Definition 36.4.2); the lattice basis, in which integrality and reduction are taken. From Chapter 34: $\mathcal{M}_i$, $\bar{G} = \bar{G}_0 \times \bar{G}_1$ and Problem 34.1.1; from Definition 33.3.1: $b^{10} \le p_i \le b^{11}$, $M = p_0 p_1$; and $b \ge 1000$ (Chapter 36). From Chapter 10: Theorem 10.2.1 and Problem 10.3.2. The Bruhat decomposition of $\mathrm{GL}_n(\mathbb{F}_p)$ [Ca72, §8.2]. Hermitian forms and inner products are linear in the first variable; norms of operators are Hilbert–Schmidt norms.

This sheet serves the second moment in the proof of Theorem 36.4.2 of Chapter 36, *Theorem B: enough forms*. From three statements of the proof it derives the two estimates near the Bessel subgroup with which that proof begins: Theorem 38.3.3 and Problem 38.3.9. By Theorem 37.3.2, the $((c,i),(c',i'))$ entry of $\mathcal{K}_s$ is the complex conjugate of $\nu^{-1}\mathrm{Amp}(U(Y_0)(F); c, s, c')_{ii'}$, a sum over the rational points γ for which $h_c^{-1}\gamma_f h_{c'}$ is integral with reduction s. Which sets of terms have amplitude sum zero, and how large is the second moment of the terms outside $R(F)$ when s agrees with an element of $\bar{R}_0$ at one level prime?

38.1. Characters that disagree

Problem 38.1.1. Let U, U' be subgroups of a finite group H with characters ψ, ψ', and let $\phi\colon H \to \mathbb{C}$ satisfy $\phi(ugu') = \psi(u)\phi(g)\psi'(u')$ for $u \in U$, $u' \in U'$. If $ugu' = g$ for some u, u' with $\psi(u)\psi'(u') \ne 1$, then $\phi(g) = 0$.

Let $G = \mathrm{GL}_n(\mathbb{F}_p)$, and let $U \subset G$ be the upper unitriangular group, ψ a nontrivial character of $\mathbb{F}_p$, and $\psi_U(u) := \psi(\sum_i u_{i,i+1})$. A double coset UgU *supports* if $\psi_U(u)\psi_U(u') = 1$ whenever $ugu' = g$ (this does not depend on the representative g); by Problem 38.1.1 the functions ϕ with $\phi(ugu') = \psi_U(u)\phi(g)\psi_U(u')$ vanish off the supporting double cosets. By the Bruhat decomposition every double coset is $UwtU$ with w a permutation matrix and t diagonal.

Problem 38.1.2. In $\mathrm{GL}_2(\mathbb{F}_p)$, $U\,\mathrm{diag}(t_1,t_2)U$ supports if and only if $t_1 = t_2$, and every double coset in the big cell supports. So $(p-1) + (p-1)^2 = p(p-1)$ of the $2(p-1)^2$ double cosets support: 6 of 8 for $p = 3$, 20 of 32 for $p = 5$.

Problem 38.1.3. By machine: in $\mathrm{GL}_3(\mathbb{F}_2)$, 4 of the 6 double cosets support, of sizes $8, 32, 32, 64$ (the two simple reflections do not); in $\mathrm{GL}_3(\mathbb{F}_3)$, $18 = 2 + 8 + 8$ of the 48 support, of sizes 27, 243, 729 respectively.

Date: November 26, 2026.

In all four cases the number of supporting double cosets is $p^{n-1}(p-1)$. By Mackey's formula it is $\dim \mathrm{End}_G(\mathrm{Ind}_U^G \psi_U)$, and since the Gelfand–Graev representation $\mathrm{Ind}_U^G \psi_U$ is multiplicity free [Ca85, §8.1], it is the number of its irreducible constituents.

Problem 38.1.4. On $\mathbb{F}_p^2$ put $h(y,y') := y_1y_2' + y_2y_1'$, and for $g \in \mathrm{GL}_2(\mathbb{F}_p)$ let $\langle g\rangle_1 := h(g\mathbf{e}_1, \mathbf{e}_1)$. Then $\langle g\rangle_1 = g_{21}$; $\mathbb{F}_p g\mathbf{e}_1 = \mathbb{F}_p\mathbf{e}_1$ if and only if $\langle g\rangle_1 = 0$; and the g with $\langle g\rangle_1 = 0$ whose double coset supports are exactly the scalar multiples of elements of U.

38.2. Frames, discriminants and links

In the proof the roles of U, ψ_U and $\mathbf{e}_1$ are played by $\mathcal{U}$, the character $\psi_{\mathcal{U}}$ and the flag of $v_1, \dots, v_\varrho$. The group $U(Y_0)(F)$ of rational points contains the rational Bessel subgroup $R(F)$.

Definition 38.2.1. The *frame* is $(v_1, \dots, v_\varrho, v_{\varrho+1})$ with $v_{\varrho+1} := z$. For $\gamma \in U(Y_0)(F)$ the matrix of *frame products* is $\big(h(\gamma v_b, v_a)\big)_{1\le a,b\le \varrho+1}$: for $a \le \varrho$ its entry is the coefficient of v_a' in γv_b, and for $a = \varrho+1$ it is $-N$ times the coefficient of z. Its leading minors are $\langle\gamma\rangle_j := \det\big(h(\gamma v_b, v_a)\big)_{1\le a,b\le j}$ for $1 \le j \le \varrho+1$, and $\langle\gamma\rangle_0 := 1$.

Definition 38.2.2. The *discriminant* of γ is $\mathrm{disc}(\gamma) := \langle\gamma\rangle_{\varrho+1}\overline{\langle\gamma\rangle_{\varrho+1}} - N^2\langle\gamma\rangle_\varrho\overline{\langle\gamma\rangle_\varrho} \in E$.

In this sheet $\mathrm{Fl} := Ev_1 + \cdots + Ev_\varrho$, and for $y \in Y_0$ we write $[y] \in X_0 \oplus Ez$ for its component in $X_0 \oplus Ez$; for $y \perp \mathrm{Fl}$ it represents the class of y in $\mathrm{Fl}^\perp/\mathrm{Fl}$.

Definition 38.2.3. The *link* of γ is the subspace $\mathrm{lk}(\gamma) := \{([y], [\gamma^{-1}y]) : y \perp \mathrm{Fl},\ y \perp \gamma\mathrm{Fl}\}$ of $(X_0 \oplus Ez)^2$.

The *characters agree* on γ if, for all $u, u' \in \mathcal{U}(F)$ with $u\gamma = \gamma u'$, the character that the proof fixes on the finite adelic points of $\mathcal{U}$ takes the same value at the finite components of u and u'. In this sheet

$$\Gamma^* := \{\gamma : \mathrm{disc}(\gamma) \ne 0\} \cup \{\gamma : \text{the characters agree on } \gamma,\ \mathrm{disc}(\gamma) = 0,\ \gamma\mathrm{Fl} \ne \mathrm{Fl}\}$$

is the set of *remaining terms*.

Definition 38.2.4. For $\zeta \in \mathcal{O}_E$ with $\zeta\bar\zeta = 1$, the *scalar coset* $\zeta\bar R_0$ is the set of $s \in \bar G$ for which some $t \in \bar R_0$ has $s_w = (\zeta \bmod w)\, t_w$ for every $w \in \mathcal{M}$. A set $\mathcal{B} \subseteq \bar G$ *avoids the scalar cosets* if it meets no $\zeta\bar R_0$ with $\zeta \ne 1$.

Theorem 38.2.1 (the terms that survive)**.** *If $\mathcal{B} \subseteq \bar G$ avoids the scalar cosets and $s \in \mathcal{B}$, then for all classes c, c', for W and for W^b,*

$$\mathrm{Amp}\big(U(Y_0)(F) \smallsetminus R(F); c, s, c'\big) = \mathrm{Amp}(\Gamma^*; c, s, c').$$

Status: read from the proof, where it is stated for an admissible filling (Section 36.4) over a CM field equipped with a CM type and containing a primitive 5040-th root of unity, which the data provide. Problem 38.1.1 is its finite model; the declaration is named in the remark at the end of the chapter.

Problem 38.2.1. In a three-dimensional model over E, let $\varrho = 1$ and $X_0 = 0$, with basis v_1, z, v_1', $h(v_1, v_1') = 1$, $h(v_1, v_1) = h(v_1', v_1') = 0$, $h(z,z) = -N$ and $z \perp v_1, v_1'$. The two maps $\gamma_\pm$ exchanging v_1 and v_1' with $z \mapsto \pm z$ are isometries of square 1

with $\langle\gamma_\pm\rangle_1 = 1$, $\langle\gamma_\pm\rangle_2 = \mp N$, $\mathrm{disc}(\gamma_\pm) = 0$ and $\gamma_\pm \mathrm{Fl} \neq \mathrm{Fl}$; the characters agree on them, whatever the character of $\mathcal{U}$, so both lie in Γ^*, and $\mathrm{lk}(\gamma_\pm)$ is spanned by $(z, \pm z)$.

Reductions act on the lattice modulo w in the lattice basis, in which the frame vectors are basis vectors. For $s \in \bar{G}$ and $w \in \mathcal{M}$, let s act modulo w by s_w, and modulo $\bar{w}$ by the adjoint inverse of s_w for the bilinear form whose matrix is the Gram matrix of the lattice basis reduced modulo w, which is invertible. For $w \in \mathcal{M}_i$, $\#k_w = p_i$ (Problem 34.1.1).

Definition 38.2.5. The element s *meets* at w (or at $\bar{w}$) if, modulo that place, the span of the frame and the span of its image under s share a nonzero vector. The *meet norm* $\mathrm{mt}(s)$ is the product, over $w \in \mathcal{M}$, of a factor $\#k_w$ if s meets at w and a further factor $\#k_w$ if s meets at $\bar{w}$.

Definition 38.2.6. The element s is *open* if at some $w \in \mathcal{M}_0$ the leading minors of orders $1, \dots, \varrho$ of the matrix $\big(h(s_w v_b, v_a)\big)_{a,b \le \varrho+1}$, formed with the reduced form, are all nonzero.

Definition 38.2.7. Let $D_0 \subseteq \mathcal{M}_0$, and for each $w \in D_0$ choose w or $\bar{w}$ and a nonzero vector y_w of the span of the frame modulo it. The *fixer* of these vectors is the subgroup of the $s \in \bar{G}$ whose action modulo the chosen place fixes y_w, for every $w \in D_0$.

For $j = 0, 1$, the *strip* $\mathcal{B}_j$ is the set of $s \in \bar{G}$ whose component in $\bar{G}_j$ equals that of an element of $\bar{R}_0$.

Problem 38.2.2. If $\zeta \in \mathcal{O}_E$, $\zeta\bar{\zeta} = 1$ and $\zeta \equiv 1$ modulo every $w \in \mathcal{M}_j$, then $\zeta = 1$. For example, in $\mathbb{Z}[\mathrm{i}]$ reduction modulo $2 + \mathrm{i}$ is injective on μ_4.

Problem 38.2.3. Every $s \in \mathcal{B}_j$ meets at w and at $\bar{w}$ for every $w \in \mathcal{M}_j$, so $\mathrm{mt}(s) \ge p_j^{2f} \ge (M/b)^f$; and $\mathcal{B}_j$ avoids the scalar cosets.

Problem 38.2.4. Every fixer contains the reduction of the finite adelic points of $U(X_0)$ that preserve the lattice, and each element of a fixer meets at the chosen place over every $w \in D_0$.

38.3. The gain at the level

On the strip $\mathcal{B}_j$ every reduction meets at the $2f$ places $w, \bar{w}$, $w \in \mathcal{M}_j$. In Petersson's formula the same mechanism appears when the terms are sorted by their reduction modulo p.

Problem 38.3.1. Let p be a prime and $k' \ge 2$, $m', n' \ge 1$ integers (primed, since k and m belong to the data); for even $k' \ge 4$ these are the weight and the indices of Theorem 10.2.1. If $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ is upper triangular modulo p and $\gamma_{21} \neq 0$, then $|\gamma_{21}| \ge p$ and $|J_{k'-1}(4\pi\sqrt{m'n'}/|\gamma_{21}|)| \le (2\pi\sqrt{m'n'}/p)^{k'-1}/(k'-1)!$.

Problem 38.3.2. Let $\mathbf{e}_1, \mathbf{e}_2$ be the standard basis of $\mathbb{Z}^2$. The integral columns $\mathbf{e}_1$ and $\mathbf{e}_1 + p\mathbf{e}_2$ agree modulo p; the lattice they span has determinant p and Gram determinant p^2 ($2, 4$ for $p = 2$; $3, 9$ for $p = 3$).

In this sheet $\mathrm{Amp}^\flat$ denotes the amplitude sums formed with $W^\flat$ in place of W, and $\|\cdot\|$ the Euclidean norm of the entries. The sums defining amplitude sums converge absolutely.

Definition 38.3.1. For $\mathfrak{S} \subseteq U(Y_0)(F)$ and $\mathcal{B} \subseteq \bar{G}$, the *second moment* of $\mathfrak{S}$ over $\mathcal{B}$ is $\nu^{-2}\sum_{c,c'}\sum_{s\in\mathcal{B}}\|\mathrm{Amp}(\mathfrak{S};c,s,c')\|^2$ (and likewise with $W^\flat$; without qualification, the second moment is formed with W). The *link second moment* of $\mathfrak{S}$ over $\mathcal{B}$ is $\sum_{c,c'}\sum_{s\in\mathcal{B}}\sum_{\Lambda}\|\mathrm{Amp}^\flat(\mathfrak{S}\cap\{\mathrm{lk}=\Lambda\};c,s,c')\|^2 \in [0,\infty]$, the inner sum over the subspaces Λ of $(X_0\oplus Ez)^2$.

Recall from Theorem 37.3.2 that, for all classes c,c', Bessel coordinates i,i' and $s\in\bar{G}$,

$$\langle \mathcal{P}^\circ e_{c,i}, \rho(s)\mathcal{P}^\circ e_{c',i'}\rangle = \nu^{-1}\mathrm{Amp}\big(U(Y_0)(F);c,s,c'\big)_{ii'},$$

and that the corresponding pairings for $\rho_{\mathrm{Bes}}(s)$ satisfy $\langle e_{c,i},\rho_{\mathrm{Bes}}(s)e_{c',i'}\rangle = \nu^{-1}\mathrm{Amp}(R(F);c,s,c')_{ii'}$.

Problem 38.3.3. $\|\mathcal{K}_s-\rho_{\mathrm{Bes}}(s)\|^2=\nu^{-2}\sum_{c,c'}\|\mathrm{Amp}(U(Y_0)(F)\smallsetminus R(F);c,s,c')\|^2$, the second moment of $U(Y_0)(F)\smallsetminus R(F)$ over $\{s\}$.

Problem 38.3.4. For vectors q_Λ of an inner product space, finitely many nonzero, $\|\sum_\Lambda q_\Lambda\|^2 \le \sum_\Lambda\|q_\Lambda\|^2+\sum_{\Lambda\neq\Lambda'}|\langle q_\Lambda,q_{\Lambda'}\rangle|$.

Theorem 38.3.1 (links at meeting reductions)**.** *If $z_0\ge 1$ is an integer with $z_0\le \mathrm{mt}(s)$ for every $s\in\mathcal{B}$, then the link second moment of $\{\gamma:\mathrm{disc}(\gamma)\neq 0\}$ over $\mathcal{B}$ is at most $(b^{2f}/z_0)^k D_{\mathrm{main}}\,\nu^2$.*

Theorem 38.3.2 (the cut)**.** *If $\mathcal{B}$ avoids the scalar cosets, $C_0\ge 0$, and the link second moment of $\{\gamma:\mathrm{disc}(\gamma)\neq 0\}$ over $\mathcal{B}$ is at most $C_0\nu^2$, then the second moment of $U(Y_0)(F)\smallsetminus R(F)$ over $\mathcal{B}$ has square root at most $\sqrt{C_0}+b^{-15}\sqrt{D_{\mathrm{id}}}$.*

Status: both are read from the proof, where they are stated for an admissible filling over a CM field equipped with a CM type and containing a primitive 5040-th root of unity. By Theorem 38.2.1, the blocks in Theorem 38.3.2 are those of Γ^*. In each cut block the terms of zero discriminant form one piece, and the terms of nonzero discriminant form one piece for each link. The proof bounds the norm of the block by the sum of the norms of these pieces and squares that bound. The squares of the pieces of nonzero discriminant, summed over the blocks, give the link second moment; after summation over the blocks and division by ν^2, all other products contribute at most $b^{-kf}D_{\mathrm{id}}$. For any set of terms, passing from $W^\flat$ to W costs at most $b^{-20}\sqrt{D_{\mathrm{id}}}$ in the square root of the second moment. The proof of Theorem 38.3.1 uses Hua's determinant integral over complex matrices [Hua, Ch. II], sums over sublattices and Liouville's inequality for Gram determinants; the next two problems give the one-row integral and a sublattice sum over $\mathbb{Z}^2$. For related lattice counts see [Sch].

Problem 38.3.5. For every integer $k\ge 1$, $\int_{\mathbb{C}^k}(1+|y|^2)^{-k-1}\,dy=\pi^k/k!$, for Lebesgue measure on $\mathbb{C}^k=\mathbb{R}^{2k}$; the values for $k=1,2,3,6,7$ are approximately 3.14, 4.93, 5.17, 1.34, 0.60, and the integral is at most 1 for $k\ge 7$.

Problem 38.3.6. For $n'\ge 1$, $\mathbb{Z}^2$ has $\sum_{e\mid n'}e$ sublattices of index n' (3 and 7 for $n'=2,4$); hence $\sum_{L'}[\mathbb{Z}^2:L']^{-\omega}=\zeta(\omega)\zeta(\omega-1)$ for real $\omega>2$, the sum over all sublattices L' of finite index.

Recall from Chapter 37 that $D_{\mathrm{main}}\le (M/b^6)^{kf}D_{\mathrm{id}}$ for the data; the proof also shows $kf\ge 40$.

Problem 38.3.7. With $z_0:=p_j^{2f}$, $(b^{2f}/z_0)^k D_{\mathrm{main}}\le b^{-3kf}D_{\mathrm{id}}\le b^{-30}D_{\mathrm{id}}$.

Problem 38.3.8. The second moment of $U(Y_0)(F) \smallsetminus R(F)$ over $\mathcal{B}_j$ has square root at most $2b^{-15}\sqrt{D_{\mathrm{id}}}$, and $4b^{-30} \le b^{-12}$.

Problems 38.2.2, 38.2.3, 38.3.3, 38.3.7 and 38.3.8, with Theorems 38.3.1 and 38.3.2, prove the following.

Theorem 38.3.3 (the strip)**.** *For the data and $j = 0, 1$,*

$$\sum_{s \in \mathcal{B}_j} \|\mathcal{K}_s - \rho_{\mathrm{Bes}}(s)\|^2 \le b^{-12} D_{\mathrm{id}}.$$

The proof states Theorem 38.3.3 for an admissible filling over a CM field equipped with a CM type and containing a primitive 5040-th root of unity, any representation ρ of its finite group on a finite-dimensional complex inner product space, unitary or not, and any linear map from the coordinate space that satisfies the block identity of Theorem 37.3.2. The data satisfy these hypotheses.

Recall Problem 37.4.3: under the hypotheses of Problem 37.4.2, which hold for the data, if $\sum_{t \in \bar{R}_0} \|\mathcal{K}_t - \rho_{\mathrm{Bes}}(t)\|^2 \le b^{-12} D_{\mathrm{id}}$, then

$$\|\mathcal{P}^{\circ *}\mathcal{P}^{\circ} - 1\|^2 \le b^{-12} D_X;$$

and Problem 37.4.4: then $\|\mathcal{K}_1\|^2 \le 2D_X$ for $b \ge 1000$.

Problem 38.3.9. For the data, $\|\mathcal{P}^{\circ *}\mathcal{P}^{\circ} - 1\|^2 \le b^{-12} D_X$ and $\|\mathcal{K}_1\|^2 \le 2D_X$.

What has been proved. Theorem 38.3.3 is the bound $b^{-12} D_{\mathrm{id}}$ for the sum of the squared Hilbert–Schmidt errors on each strip, and the first inequality of Problem 38.3.9 makes $\mathcal{P}^{\circ}$ a near isometry in the sense of Chapter 36. Taken as given: the block identity and the Bessel functions (Theorems 37.3.2 and 37.3.1), and Theorems 38.2.1, 38.3.1 and 38.3.2 and the inequalities $D_{\mathrm{main}} \le (M/b^6)^{kf} D_{\mathrm{id}}$ and $kf \ge 40$. Problem 38.2.3 gives a lower bound for the meet norm on each strip only. Chapters 39 and 40 use the open reductions of Definition 38.2.6 and the fixers of Definition 38.2.7 to bound $\sum_{s \in \bar{G}} \|\mathcal{K}_s\|^2$ by $(1 + 9b^{-4}) D_{\mathrm{main}}$ (Theorem 40.3.1).

In the Lean formalization. In the Lean proof [GL]: Theorem 38.3.3 is `Filling.HasAmplitudeBlocks.sum_hilbertSchmidtNorm_sub_besselTranslate_sq_le`; Theorem 38.2.1 is `Filling.AvoidsScalarCosets.amplitudeSum_compl_besselS_eq`; Theorem 38.3.1 is `Filling.linkSecondMoment_le_of_le_meetNorm`; Theorem 38.3.2 is `Filling.sqrt_secondMoment_compl_besselS_le`. The discriminant, the link, the meet norm, open reductions, fixers and the avoidance of scalar cosets are `Filling.termDisc`, `link`, `Filling.meetNorm`, `Filling.IsOpenElement`, `Filling.fixer` and `Filling.AvoidsScalarCosets`.

Hints

§38.1.

38.1.1: Evaluate $\phi(ugu')$ in two ways.

38.1.2: For $g = \mathrm{diag}(t_1, t_2)$ and $u' = \left(\begin{smallmatrix} 1 & y \\ 0 & 1 \end{smallmatrix}\right)$, find the u with $ugu' = g$. In the big cell $U \cap wUw^{-1} = 1$.

38.1.3: Sage or Python: run over $\mathrm{GL}_3(\mathbb{F}_p)$, form each UgU with the value $\psi_U(u)\psi_U(u')$ attached to ugu', and test consistency.

38.1.4: Use Problem 38.1.2; the g with $g_{21} = 0$ form the upper triangular group.

§38.2.

38.2.1: Compute the matrices of frame products of $\gamma_{\pm}$, and the intersection $\mathcal{U} \cap \gamma_{\pm}\mathcal{U}\gamma_{\pm}^{-1}$.

38.2.2: If $\zeta \neq 1$, the ideal $(\zeta - 1)$ is divisible by the f distinct primes $w \in \mathcal{M}_j$, of norm p_j; bound $|\sigma(\zeta) - 1| \leq 2$ for every embedding σ.

38.2.3: An integral element t of $R(\mathbb{A}_f)$ fixes v_1 and satisfies $h(ty, v_1) = h(y, v_1)$; reduce modulo w, and deduce that the adjoint inverse of t_w also fixes v_1. For a scalar coset, compare the entries at v_1 of s_w and t_w and use Problem 38.2.2. For $p_j^2 \geq M/b$ use $p_{1-j} \leq b\, p_j$.

38.2.4: Which vectors does $U(X_0)$ fix? Compare the definition of a fixer with Definition 38.2.5.

§38.3.

38.3.1: $p \mid \gamma_{21}$; then Problem 10.3.2.

38.3.3: Expand the norm in the basis $e_{c,i}$, and split $U(Y_0)(F)$ into $R(F)$ and its complement.

38.3.4: Expand the square.

38.3.5: Polar coordinates: the sphere S^{2k-1} has volume $2\pi^k/(k-1)!$.

38.3.6: Each sublattice is spanned by the columns of exactly one $\left(\begin{smallmatrix} g_1 & g_3 \\ 0 & g_2 \end{smallmatrix}\right)$ with $g_1 g_2 = n'$, $0 \leq g_3 < g_1$.

38.3.7: Problem 38.2.3.

38.3.8: Theorem 38.3.2 with $\mathcal{B} = \mathcal{B}_j$ and $C_0 = b^{-30} D_{\mathrm{id}}$, after Theorem 38.3.1 and Problems 38.2.3 and 38.3.7.

38.3.9: $\bar{R}_0 \subseteq \mathcal{B}_0$.

References

[Ca72] R. W. Carter, *Simple Groups of Lie Type*, Wiley, London, 1972.

[Ca85] R. W. Carter, *Finite Groups of Lie Type: Conjugacy Classes and Complex Characters*, Wiley, Chichester, 1985.

[GL] L. Sernau, *GRH for Dirichlet L-functions, in Lean 4*, a shorter rewriting of the Lean proof, text by Claude, `https://github.com/lsernau/grh-lean`, commit `72fead1`, readable edition `grh/`.

[Hua] L.-K. Hua, *Harmonic Analysis of Functions of Several Complex Variables in the Classical Domains*, Transl. Math. Monographs **6**, Amer. Math. Soc., Providence, 1963.

[Sch] W. M. Schmidt, *Asymptotic formulae for point lattices of bounded determinant and subspaces of bounded height*, Duke Math. J. **35** (1968), 327–339.

THE OPEN CELL: SIEGEL'S FORMULA AND POISSON SUMMATION

Prerequisites. From Chapter 36: the hermitian space $Y_0 = \bigoplus_a Ev_a \oplus X_0 \oplus Ez \oplus \bigoplus_a Ev'_a$ with $h(z,z) = -N$, the unipotent group $\mathcal{U}$ (Section 36.1), and the covolume ν (Definition 36.4.1). From Chapter 37: the degrees d_τ of Theorem 37.3.1, $\deg = \prod_\tau d_\tau$, and the sizes D_{id}, $D_{\mathrm{main}} = D_X^2/(\deg \cdot \mathrm{mass}_r)$ of Definition 37.3.2. From Chapter 38: the frame and the leading minors $\langle\gamma\rangle_j$ (Definition 38.2.1), disc (Definition 38.2.2), links, open reductions, fixers and link second moments (Definitions 38.2.3, 38.2.6, 38.2.7, 38.3.1). From Chapter 22: the densities α_∞, α_p of Section 22.2 and Braun's formula (3). Problem 21.1.4; Problem 10.4.5. Fourier analysis on finite abelian groups; Hensel's lemma; Schur orthogonality for square-integrable representations [Kn, Ch. IX]. Hermitian forms are linear in the first variable, and $|\cdot|^2$ is the product with the complex conjugate. In this sheet j, l are integers or residues, y is a vector, ω is an isometry, $\mathrm{e}(\cdot) := e^{2\pi \mathrm{i} \cdot}$ on $\mathbb{R}$, and K' is a level (not the field K).

The second moment of the Gram operators of Chapter 36 is bounded in Theorem 40.3.1 by splitting the reductions $s \in \bar{G}$ into the open ones and the rest. This sheet treats the open ones. Over the open reductions that fix chosen vectors of the span of the frame at $\#\mathcal{D}$ chosen places, the link second moment of the terms with disc $\neq 0$ is at most $(1+b^{-4})\, b^{-6k\#\mathcal{D}}\, D_{\mathrm{main}}\, \nu^2$ (Theorem 39.3.3). Where does D_{main} come from? A term over an open reduction is a head, a last entry and a residual isometry. The residual isometries with a given last entry are counted by vectors of a given norm, and Siegel's formula counts these exactly. The heads are summed by Poisson summation, one entry at a time: the zero frequencies give an integral, and the other frequencies are small. The bound has no small instance: in the proof $\varrho \geq 10^5$. We meet the steps separately: one isometry over $\mathbb{Q}$, six squares, and the groups $\mathbb{Z}/5$ and $\mathbb{Z}/3$.

39.1. Head, last entry and residual isometry

Let $V = \bigoplus_{a \leq \varrho} Ev_a \oplus X \oplus Ez \oplus \bigoplus_{a \leq \varrho} Ev'_a$ be a hermitian space of the shape of Section 36.1, with X of rank k and totally positive definite, and $h(z,z) = -N$. A *residual isometry* is an isometry ω of V with $\omega v_a = v_a$ and $\omega v'_a = v'_a$ for all a. It preserves the orthogonal complement $X \oplus Ez$ of the v_a, v'_a.

Problem 39.1.1. As a model with $E = \mathbb{Q}$ (trivial involution), let $\varrho = 0$, $N = 5$ and $X = \mathbb{Q}\mathbf{e}$ of rank one: $V = \mathbb{Q}\mathbf{e} \oplus \mathbb{Q}z$ with $h(\mathbf{e},\mathbf{e}) = 1$, $h(z,z) = -5$. The matrix $\omega = \left(\begin{smallmatrix} 3/2 & 5/2 \\ 1/2 & 3/2 \end{smallmatrix}\right)$ in the basis $\mathbf{e}, z$ (columns are the images) is an isometry, $h(z, \omega z) = -15/2$, and the coefficient $5/2$ of $\mathbf{e}$ in ωz satisfies $5 \cdot (5/2)^2 = (15/2)^2 - 25$.

Problem 39.1.2. Let ω be a residual isometry, and write $\omega z = y + c_\omega z$ with $y \in X$, $c_\omega \in E$. Then $|h(z,\omega z)|^2 = N^2 |c_\omega|^2$ and

$$N\, h(y,y) = |h(z,\omega z)|^2 - N^2.$$

Date: November 26, 2026.

Hence $|\tau h(z,\omega z)| \geq N$ at every infinite place τ, with strict inequality at every τ if $y \neq 0$ and equality at every τ if $y = 0$.

Now let $V = Y_0$, with the frame $(v_1, \dots, v_\varrho, z)$ and the leading minors $\langle\gamma\rangle_j$, $0 \leq j \leq \varrho+1$, of Definition 38.2.1, so that $\langle\gamma\rangle_0 = 1$ and $\langle\gamma\rangle_{\varrho+1}$ is the determinant of the matrix of frame products.

Definition 39.1.1. Let $\gamma \in U(Y_0)(F)$ have $\langle\gamma\rangle_j \neq 0$ for $1 \leq j \leq \varrho$. Its *head* is $\mathrm{hd}(\gamma) := \big(\langle\gamma\rangle_{a+1}/\langle\gamma\rangle_a\big)_{0\leq a<\varrho} \in (E^\times)^\varrho$. If also $\langle\gamma\rangle_{\varrho+1} \neq 0$, its *last entry* is $\mathrm{le}(\gamma) := \langle\gamma\rangle_{\varrho+1}/\langle\gamma\rangle_\varrho$. A *residual isometry of the last floor* is a residual isometry of Y_0.

By Definition 38.2.2, $\mathrm{disc}(\gamma) = |\langle\gamma\rangle_\varrho|^2\big(|\mathrm{le}(\gamma)|^2 - N^2\big)$ whenever $\mathrm{le}(\gamma)$ is defined. In the proof, if s is open, then every term γ over (c,s,c') has $\langle\gamma\rangle_j \neq 0$ for $j \leq \varrho$. Moreover $\gamma = n^{-1}\mathfrak{w}\,\omega\,n'$ with $n, n' \in \mathcal{U}(F)$, ω a residual isometry of Y_0, and $\mathfrak{w}$ a Weyl element that exchanges each line Ev_a with Ev'_a, fixes $X_0 \oplus Ez$ and depends only on $\mathrm{hd}(\gamma)$. The (z,z) entry $h(\omega z, z)$ of the matrix of frame products of ω is $\mathrm{le}(\gamma)$, so $|\mathrm{le}(\gamma)| = |h(z,\omega z)|$. By Problem 39.1.2 the last entry is therefore always defined there, and $\mathrm{disc}(\gamma) \neq 0$ exactly when the X_0-part y of ωz is nonzero.

Consider a block of the link second moment over an open reduction s whose sum is nonzero. In the proof one residual isometry ω names the link, and the heads of the contributing terms lie in a finite set $\mathcal{E}^\varrho$, where $\mathcal{E} \subset E^\times$ consists of quotients of integers of bounded size. The block is the sum, over $\mathfrak{h} \in \mathcal{E}^\varrho$, of the sums of the amplitudes of the $n^{-1}\mathfrak{w}\,\omega\,n'$ over (c,s,c'), for $n, n' \in \mathcal{U}(F)$, where $\mathfrak{w}$ is the Weyl element of $\mathfrak{h}$. Different nonzero blocks give different (c, c', s, ω). So the heads are summed inside the square, and the residual isometries outside it. By Problem 39.1.2, the sum over the ω with a given last entry is controlled by a sum over vectors $y \in X_0$ with $N\,h(y,y) = |\mathrm{le}|^2 - N^2$, one for each class.

39.2. Siegel's formula for six squares

The smallest rank to which Braun's formula (3) applies is 3, and for $\mathbb{Z}[\mathrm{i}]^3$ the class set is $\{I_3\}$ (Problem 21.1.4). So the mean over the class set is a count: $r_{I_3}(j) := \#\{y \in \mathbb{Z}[\mathrm{i}]^3 : y^*y = j\}$ equals $\alpha_\infty(j)\prod_p \alpha_p(j)$, with the densities of Section 22.2 for the form $Q(y) = y^*y$, a sum of six squares on $\mathbb{Z}^6$. Let χ_{-4} be the nontrivial character modulo 4.

Problem 39.2.1. By machine, $r_{I_3}(1) = 12$, $r_{I_3}(2) = 60$ and $r_{I_3}(5) = 312$.

Problem 39.2.2. For odd p, the number of $x \in (\mathbb{Z}/p)^6$ with $\sum_i x_i^2 = 1$ is $p^5 - \chi_{-4}(p)p^2$, and the same holds with 1 replaced by any j prime to p: by machine 252, 3100, 16856 for $p = 3, 5, 7$. By machine, there are $61236 = 3^5 \cdot 252$ solutions modulo 9, and $3 \cdot 2^{5e}/4$ solutions modulo 2^e for $e = 2, 3$ (768, 24576). For $e \geq 3$ the count modulo 2^{e+1} is 2^5 times the count modulo 2^e. Hence $\alpha_p(1) = 1 - \chi_{-4}(p)p^{-3}$ for odd p, and $\alpha_2(1) = 3/4$.

Problem 39.2.3. For real $j > 0$, $\mathrm{vol}\{y \in \mathbb{C}^3 : |y|^2 \leq j\} = \pi^3 j^3/6$, so $\alpha_\infty(j) = \pi^3 j^2/2$.

Problem 39.2.4. With $L(3, \chi_{-4}) = \pi^3/32$: $\frac{\pi^3}{2} \cdot \frac{3}{4} \cdot \prod_{p \text{ odd}}\big(1 - \chi_{-4}(p)p^{-3}\big) = 12 = r_{I_3}(1)$. For $j = 5$ the factor at 5 is $\alpha_5(5) = 3224/3125$, the factor at infinity is $\alpha_\infty(5) = 25\pi^3/2$, the other factors are those of $j = 1$, and the product is $312 = r_{I_3}(5)$.

The general statement is for a CM field with Weil data: E contains a primitive 5040th root of unity, and there are a $j_E \in E$ with $\bar{j}_E = -j_E$, $\operatorname{Im}\tau(j_E) > 0$ at every τ and $(1 - j_E^{-1})/2$ an algebraic integer, a finite idele that makes $\hat{\mathcal{O}}_E$ self-dual for the pairing defined by j_E and the additive character ψ_f of the finite adeles, and a splitting character that is -1 at the chosen uniformizer of every finite place fixed by complex conjugation [GL]. Here $\operatorname{vol}(\hat{\mathcal{O}}_E) = 2^f |d_E|^{-1/2}$, with d_E the discriminant of E.

Theorem 39.2.1 (Siegel's formula for one vector)**.** *Let E be a CM field with Weil data, $k \geq 3$, K' an open subgroup of the stabilizer of $\hat{\mathcal{O}}_E^k$ in the finite adelic unitary group of y^*y, $\phi \geq 0$ a locally constant, compactly supported, K'-invariant function on $\mathbb{A}_{E,f}^k$, and $\mathfrak{n} \in E$ with $\bar{\mathfrak{n}} = \mathfrak{n}$ and $\tau\mathfrak{n} > 0$ at every infinite place. Then each sum $\sum_{y \in E^k,\, y^*y = \mathfrak{n}} \phi(g^{-1}y)$ converges, and*

$$\sum_{[g]} \frac{1}{\#\mathrm{Aut}(g)} \sum_{\substack{y \in E^k \\ y^*y = \mathfrak{n}}} \phi(g^{-1}y)$$
$$= \Big(\sum_{[g]} \frac{1}{\#\mathrm{Aut}(g)}\Big) |d_E|^{1/4} \prod_{\tau} \frac{\pi^k (\tau\mathfrak{n})^{k-1}}{(k-1)!} \iint \phi(u)\, \psi_f\big(\tfrac{1}{2}\zeta(u^*u - \mathfrak{n})\big)\, du\, d\zeta,$$

where $[g]$ runs over the classes of level K', u over $\mathbb{A}_{E,f}^k$ with $\hat{\mathcal{O}}_E$ of volume $\operatorname{vol}(\hat{\mathcal{O}}_E)$ in each coordinate, and ζ over the self-adjoint finite adeles with the codifferent of volume 1.

Status: classical; due to Siegel [Si] for quadratic forms and Braun [Br] for hermitian forms, and a case of Weil's theorem [We65, Thm. 5]. The last integral is the product of the local densities, left as one adelic integral; its normalization is not compared here with that of Chapter 22. If there is one class, or every class has trivial automorphism group, the formula is a statement about counts; Problem 39.2.1 is the case of one class, over a field without Weil data.

In the proof, Theorem 39.2.1 is applied, for each last entry, to the vectors $y \in X_0$ with $N\, h(y,y) = |\mathrm{le}|^2 - N^2$, that is at $\mathfrak{n} = (\mathrm{le}\ \overline{\mathrm{le}} - N^2)/N$. It is used as an upper bound, with an extra factor $1 + b^{-6}$ from the local densities.

39.3. Poisson summation, one entry at a time

In the proof, each double-coset sum of Section 39.1 is a Kloosterman sum at finitely many finite places times an orbital integral at the infinite places. Squaring the sum over heads gives a sum over pairs of heads, and the pairs of different heads are kept. They are summed by Poisson summation in one entry at a time. For a function $\mathfrak{f}$ on $\mathbb{Z}/p$ let $\hat{\mathfrak{f}}(l) := p^{-1} \sum_j \mathfrak{f}(j)\, \mathrm{e}(-lj/p)$, so that $\mathfrak{f}(j) = \sum_l \hat{\mathfrak{f}}(l)\, \mathrm{e}(lj/p)$.

Problem 39.3.1. On $\mathbb{Z}/5$, $\mathfrak{f}(j) = 2 + \cos(2\pi j/5)$ has $\hat{\mathfrak{f}} = (2, \frac{1}{2}, 0, 0, \frac{1}{2})$. So $\mathfrak{f}(0) = 3$, while the zero frequency alone gives 2.

Problem 39.3.2. Let $\mathfrak{f}$ be a function on a finite abelian group $\mathcal{G}$, and $\hat{\mathfrak{f}}(\psi') := \#\mathcal{G}^{-1} \sum_{j \in \mathcal{G}} \mathfrak{f}(j)\overline{\psi'(j)}$ for the characters ψ' of $\mathcal{G}$. Then $|\mathfrak{f}(j)| \leq \sum_{\psi'} |\hat{\mathfrak{f}}(\psi')|$ for every j, and $\hat{\mathfrak{f}}(\psi_0)$ is the mean of $\mathfrak{f}$, for the trivial character ψ_0. If $\mathfrak{f}$ is real and $\sum_{\psi' \neq \psi_0} |\hat{\mathfrak{f}}(\psi')| \leq c$, then $\mathfrak{f}(j) \leq \hat{\mathfrak{f}}(\psi_0) + c$.

For $j \in \mathbb{Z}/p$ let $\mathrm{Kl}(j) := \sum_{l \in (\mathbb{Z}/p)^\times} \mathrm{e}\big((l + jl^{-1})/p\big)$, a Kloosterman sum.

Problem 39.3.3. For $p = 5$ the values $\mathrm{Kl}(0), \dots, \mathrm{Kl}(4)$ are

$$-1, \quad \tfrac{3-\sqrt{5}}{2}, \quad -1-\sqrt{5}, \quad \sqrt{5}-1, \quad \tfrac{3+\sqrt{5}}{2},$$

and $\sum_j |\mathrm{Kl}(j)|^2 = 20$.

Problem 39.3.4. $\sum_{j \in \mathbb{Z}/p} |\mathrm{Kl}(j)|^2 = p(p-1)$. In the expansion of the square, the terms with $l \neq l'$ cancel after the sum over j: the matrix $\big(\sum_j \mathrm{e}(j(l^{-1} - l'^{-1})/p)\big)_{l,l'}$ is p times the identity.

So once a free variable is summed, different heads are orthogonal. At a fixed nonzero frequency they are not orthogonal, but the frequency gains a factor in each free direction.

Problem 39.3.5. Let $\mathfrak{A}_l := \big(\mathrm{e}(ljj'/3)\big)_{j,j' \in \mathbb{Z}/3}$. Then $\mathfrak{A}_1 \mathfrak{A}_1^* = 3 \cdot 1$, and $\mathfrak{A}_0 \mathfrak{A}_0^*$ is the matrix with all entries 3. Their squared operator norms are 3 and 9, and those of the k-th tensor powers are 3^k and 9^k.

In the proof, the rank k of X_0 pays for the nonzero frequencies in the same way. At each infinite place the bound at a nonzero frequency decays at least like the $(k-(\varrho+1)^7)$-th power of its inverse size. We do not derive these local bounds here.

Problem 39.3.6. The entrywise product of two positive semidefinite matrices of the same size is positive semidefinite.

In the proof, the form on pairs of heads with a common last entry is the entrywise product of positive semidefinite kernels, one at each infinite place and one at the finite places. So it is positive semidefinite, by Problem 39.3.6, and the densities obtained from it by integrating out entries are nonnegative. Nonnegativity is what Theorem 39.3.1 below needs.

Problem 39.3.7. Let π be an irreducible unitary representation of a unimodular group $\mathcal{G}'$ with square-integrable matrix coefficients and formal degree d_π, so that $\int_{\mathcal{G}'} \langle \pi(g)u_1, u_3\rangle \overline{\langle \pi(g)u_2, u_4\rangle}\, dg = d_\pi^{-1} \langle u_1, u_2\rangle \overline{\langle u_3, u_4\rangle}$. For every vector u with $\|u\|^2 = D'$,

$$\int_{\mathcal{G}'} |\langle \pi(g)u, u\rangle|^2\, dg = \frac{D'^2}{d_\pi}.$$

For the representation of Problem 10.4.5 and $D' = 1$, this is the reciprocal of the formal degree found there.

Identity (c) of Theorem 37.3.1 at each infinite place τ is the relation of Problem 39.3.7 for the single vector W_τ, whose squared norm is $\#I_\tau$, with $d_\pi = d_\tau$. In the proof, at the zero frequency the integral of a form over a common entry is exactly the form of one length less, and the form of length zero has modulus at most $(1 + b^{-10})/d_\tau$ at the infinite place τ. This is the factor $\prod_\tau 1/d_\tau = 1/\deg$ of c_{bot} below. Poisson summation is used in the following one-sided form.

Theorem 39.3.1 (one-sided Poisson summation)**.** *Let E be a totally complex number field with chosen complex embeddings, ψ the standard character of $\mathbb{A}_E/E$, and du the Haar measure on $\mathbb{A}_E$ for which E has covolume 1. Let $\mathfrak{f}\colon \mathbb{A}_E \to \mathbb{R}$ be nonnegative and integrable, and lower semicontinuous at each point of a finite set $\mathcal{Z} \subset E$, and put $\hat{\mathfrak{f}}(l) := \int \mathfrak{f}(u)\psi(-lu)\, du$. If $\sum_{l \in \mathcal{Z}'} |\hat{\mathfrak{f}}(l)| \leq c_{\mathfrak{f}}$ for every finite $\mathcal{Z}' \subset E$, then $\sum_{u \in \mathcal{Z}} \mathfrak{f}(u) \leq c_{\mathfrak{f}}$.*

Status: an inequality form of Poisson summation on $\mathbb{A}_E/E$ [Ta], for functions that need not be continuous. We use it as the proof proves it, where the test function is smoothed by a bump on the compact quotient.

Theorem 39.3.2 (the sieve)**.** *In the proof, fix $\mathcal{D}$ and the vectors of Theorem 39.3.3. There are real numbers $\Sigma_0, \dots, \Sigma_{\varrho+1}$, the sums of the densities of the pairs of heads of length i (tuples of i entries) with entries in $\mathcal{E}$ and a common last entry (for $i = 0$, the density of the empty pair), and $\lambda_0, \dots, \lambda_\varrho \geq 0$, the sums of the weights of the heads of length i with entries in $\mathcal{E}$. They satisfy, for $0 \leq i \leq \varrho$,*

$$\Sigma_0 \leq c_{\mathrm{bot}}, \qquad \Sigma_{i+1} \leq c_i\big(\Sigma_i + 2c_{\mathrm{fr}}\lambda_i^2\big), \qquad \lambda_i^2 \leq c_{\mathrm{wt}} \prod_{i'<i} c_{i'},$$

and $\Sigma_{\varrho+1}$ bounds the sum, over the last entries, of the top form over all pairs of heads. Here $c_i > 0$ is the constant of Poisson summation in the entry i: $\mathrm{vol}(\hat{\mathcal{O}}_E)$ *divided by the Jacobian, at the infinite places, of the rescaling that the proof applies to that entry. Further $c_{\mathrm{bot}} = \prod_\tau \big((1 + b^{-10})/d_\tau\big) \cdot (1 + b^{-6})\, b^{-6k\#\mathcal{D}}$, $c_{\mathrm{fr}} = b^{2002(\varrho+1)^9 f} c_{\mathrm{dec}}$ with an explicit constant $c_{\mathrm{dec}} > 0$, and $c_{\mathrm{wt}} = b^{400(\varrho+1)^9 f}$.*

Status: read from the proof. Each step of the recurrence is Theorem 39.3.1 in the entry i. The zero frequency gives c_i times the sum of the densities over all pairs of heads of length i; the pairs with a common last entry give $c_i\Sigma_i$, and those whose last entries differ give the error $c_i c_{\mathrm{fr}}\lambda_i^2$. The nonzero frequencies give the other error $c_i c_{\mathrm{fr}}\lambda_i^2$. The local bounds behind c_{fr} are not derived here.

Problem 39.3.8. Under Theorem 39.3.2, $\Sigma_i \leq \big(\prod_{i'<i} c_{i'}\big)\big(c_{\mathrm{bot}} + 2i\, c_{\mathrm{wt}} c_{\mathrm{fr}}\big)$ for $0 \leq i \leq \varrho + 1$.

In the proof, Theorem 39.2.1 bounds the open link moment, up to one normalizing constant, by $(1 + b^{-6})$ times the constant of Siegel's step times $\Sigma_{\varrho+1}$; this constant is the constant of Siegel's formula times the number of classes, the order of the reduction of the integral points of $\mathcal{U}$, and $\#\bar{R}_0$ (Chapter 37). Apply Problem 39.3.8 with $i = \varrho+1$. The product of the c_i, of the constant of Siegel's step and of c_{bot} is at most $(1 + b^{-9})^2(1 + b^{-6})\, b^{-6k\#\mathcal{D}} D_{\mathrm{main}}\nu^2$, up to the same normalizing constant. The factors are: $1 + b^{-9}$ for the constants, $(1 + b^{-10})^f \leq 1 + b^{-9}$ for the degrees (in the proof $f \leq b/1000$), and $1 + b^{-6}$ from c_{bot}. The error terms are at most $b^{-10} \cdot b^{-6k\#\mathcal{D}} D_{\mathrm{main}}\nu^2$, because the large powers of b in c_{fr} and c_{wt} are paid by $b^{11kf} D_{\mathrm{id}} \leq D_{\mathrm{main}}$ (Chapter 37). Since $b \geq 1000$, the following inequality collects these factors.

Problem 39.3.9. For $b \geq 1000$: $(1 + b^{-6})\big((1 + b^{-9})^2(1 + b^{-6}) + b^{-10}\big) \leq 1 + b^{-4}$.

Problems 39.1.2, 39.3.2, 39.3.6, 39.3.7, 39.3.8 and 39.3.9 model the steps of the following theorem. The proof proves it by these steps, with Theorems 39.2.1, 39.3.1 and 39.3.2 and the statements read from the proof in this sheet.

Theorem 39.3.3. *For the data, let $\mathcal{D} \subseteq \mathcal{M}_0$ be a set of chosen places above p_0, and for each $w \in \mathcal{D}$ choose w or $\bar{w}$ and a nonzero vector of the span of the frame modulo it, as in Definition 38.2.7 with $D_0 = \mathcal{D}$; let the fixer of $\mathcal{D}$ be the fixer of these vectors. Then the link second moment of the terms γ with $\mathrm{disc}(\gamma) \neq 0$, over the reductions that are open and lie in the fixer of $\mathcal{D}$, is at most*

$$(1 + b^{-4})\, b^{-6k\#\mathcal{D}}\, D_{\mathrm{main}}\, \nu^2.$$

Status: read from the proof, where it is stated for an admissible filling over a CM field with Weil data, which the data provide. The local bounds at nonzero frequencies and the matching of the constants are not derived here; see the remark below.
What has been proved. A term over an open reduction is a head, a last entry and a residual isometry (Section 39.1). Its last entry has $|\mathrm{le}|^2 - N^2 = N\,h(y,y)$ (Problem 39.1.2), so the residual isometries are counted by Siegel's formula (Theorem 39.2.1, modelled in Problems 39.2.1–39.2.4). The heads are summed by Poisson summation one entry at a time: zero frequencies give integrals and the degrees d_τ, and the rank k pays for the rest (Problems 39.3.1–39.3.7, Theorems 39.3.1 and 39.3.2). Taken as given: Theorems 39.2.1, 39.3.1 and 39.3.2, and the statements marked "in the proof". Chapter 40 combines Theorem 39.3.3 with the cut and the absolute bound of Chapter 38, and bootstraps over fixers, to bound the second moment over all of $\bar{G}$.

In the Lean formalization. Theorem 39.3.3 is `New.Filling.linkSecondMoment_isOpenElement_le` in the Lean proof [GL]. Theorem 39.2.1 is `New.classSum_eq_mul_normDensity`, Theorem 39.3.1 is `New.IsDualFamily.sum_le_of_fourier`, and Theorem 39.3.2 is read from `New.Filling.sieve`. Problem 39.3.8 is `densitySum_le`, Problem 39.1.2, for $V = Y_0$, is `mul_star_dotProduct_eq_last_frameProducts` with the strict inequality, Problem 39.3.6 is used as `posSemidef_prod_mul`, and the matching of the constants is `sieve_constant_le`. The block as a sum over heads is `exists_amplitudeSum_eq_sum_cosetAmplitude`, and the Kloosterman factorization is `IsFillingData.cosetAmplitude_eq_kloostermanSum_smul`. The other statements marked "in the proof" are at these places of [GL], commit `72fead1`: minors of open terms, the normal form and its minors, distinct blocks, Siegel's step for the blocks, Siegel's formula as an upper bound, the product of kernels, nonnegative densities, the zero frequency, the decay, the recurrence, $\varrho \geq 10^5$, $f \leq b/1000$, and $b^{11kf} D_{\mathrm{id}} \leq D_{\mathrm{main}}$.

Hints

§39.1.

39.1.1: Check that ω preserves the Gram matrix $\mathrm{diag}(1,-5)$.
39.1.2: Expand $h(\omega z, \omega z) = h(z,z)$, using $y \perp z$.

§39.2.

39.2.1: In Sage or Python, enumerate the vectors of $\mathbb{Z}^6$ with entries in $[-2,2]$.
39.2.2: By machine: convolve the histogram of the squares modulo m six times. For the formula, detect the equation with $\mathrm{e}(\cdot/p)$ and use the quadratic Gauss sum: every nonzero frequency gives the same sixth power. Solutions modulo p with a unit coordinate lift by Hensel's lemma; compare the counts modulo 3 and 9. Every solution has an odd coordinate; for $e \geq 3$, adding 2^{e-1} to it changes the sum of squares by 2^e modulo 2^{e+1}.
39.2.3: The unit ball of $\mathbb{R}^6$ has volume $\pi^3/6$.
39.2.4: $\prod_{p\ \mathrm{odd}} (1 - \chi_{-4}(p) p^{-3}) = L(3,\chi_{-4})^{-1}$. For $j = 5$, compute modulo 25 and 125 at 5, and at 2 use that $y \mapsto (2+\mathrm{i})y$ is a bijection modulo 2^e from the solutions of $y^* y \equiv 1$ to those of $y^* y \equiv 5$.

§39.3.

39.3.2: Fourier inversion and the triangle inequality.

39.3.4: Expand $|\mathrm{Kl}(j)|^2$ and sum over j first.

39.3.5: The rows of $\mathfrak{A}_1$ are the characters of $\mathbb{Z}/3$; the operator norm is multiplicative under tensor products.

39.3.6: The entrywise product is a principal submatrix of the Kronecker product; compare [HJ, Thm. 7.5.3].

39.3.7: Apply the orthogonality relation with $u_1 = u_2 = u_3 = u_4 = u$.

39.3.8: Induction on i.

39.3.9: Each of b^{-6}, b^{-9}, b^{-10} is at most $b^{-4}/100$.

References

[Br] H. Braun, *Zur Theorie der hermitischen Formen*, Abh. Math. Sem. Hansischen Univ. **14** (1941), 61–150.

[GL] L. Sernau, *GRH for Dirichlet L-functions, in Lean 4*, a shorter rewriting of the Lean proof, text by Claude, `https://github.com/lsernau/grh-lean`, commit `72fead1`, readable edition `grh/`.

[HJ] R. A. Horn and C. R. Johnson, *Matrix Analysis*, 2nd ed., Cambridge Univ. Press, 2013.

[Kn] A. W. Knapp, *Representation Theory of Semisimple Groups: an Overview Based on Examples*, Princeton Univ. Press, 1986.

[Si] C. L. Siegel, *Über die analytische Theorie der quadratischen Formen*, Ann. of Math. **36** (1935), 527–606.

[Ta] J. T. Tate, *Fourier analysis in number fields and Hecke's zeta-functions*, in J. W. S. Cassels and A. Fröhlich (eds.), *Algebraic Number Theory*, Academic Press, 1967, Ch. XV.

[We65] A. Weil, *Sur la formule de Siegel dans la théorie des groupes classiques*, Acta Math. **113** (1965), 1–87.

POSITIVE TYPE AND THE BOOTSTRAP: THE SECOND MOMENT

Prerequisites. Hermitian forms and inner products are linear in the first variable; norms of operators are Hilbert–Schmidt norms. Additive characters of a finite field and their orthogonality [LN, Ch. 5, §1]. From Chapter 9: Problem 9.2.2. From Chapter 36: the Bessel subgroup and the vectors $v_1, \dots, v_\varrho$, z (Section 36.1; they belong to the lattice basis of Definition 36.4.1), the scaled Poincaré map $\mathcal{P}^\circ$, the Gram operators $\mathcal{K}_s$ and the covolume ν (Definition 36.4.1), the group $\bar{R}_0$ and ρ_{Bes} (Definition 36.4.2), and admissible fillings (Section 36.4). From Chapter 37: Theorem 37.3.2, the sizes $D_{\mathrm{id}} = \#\bar{R}_0 \cdot D_X$ and D_{main} (Definition 37.3.2), Problems 37.4.3, 37.4.4 and 37.4.5. From Chapter 38: frame products and their leading minors $\langle s \rangle_j$ (Definition 38.2.1), meeting and the meet norm mt (Definition 38.2.5), open reductions (Definition 38.2.6), fixers (Definition 38.2.7), scalar cosets (Definition 38.2.4), second moments and link second moments (Definition 38.3.1), Theorems 38.3.1, 38.3.2 and 38.3.3. From Chapter 39: Theorem 39.3.3.

Chapter 36 deduces Theorem B from three estimates for the Gram operators $\mathcal{K}_s = \mathcal{P}^{\circ *}\rho(s)\mathcal{P}^\circ$, $s \in \bar{G}$. This sheet proves the second-moment estimate $\sum_{s\in\bar{G}} \|\mathcal{K}_s\|^2 \le (1 + 9b^{-4}) D_{\mathrm{main}}$. Chapter 39 bounds the open reductions that fix given frame vectors; the others, where a leading minor of the frame products vanishes, are many (three sevenths of $\mathrm{GL}_3(\mathbb{F}_2)$ in the toy below). How can one show that they carry little of $s \mapsto \|\mathcal{K}_s\|^2$ without knowing that this function is spread evenly over $\bar{G}$?

40.1. Positive type and singular minors

In this sheet a real function Θ on a finite group G is *of positive type* if there are vectors u_a, $a \in G$, of a complex inner product space with $\langle u_a, u_b \rangle = \Theta(a^{-1}b)$ for all a, b. A subset of G *carries* the sum of Θ over it. By Problem 9.2.2, if ρ is a unitary representation of G and L a linear map into its space, then $s \mapsto \|L^*\rho(s)L\|^2$ is of positive type, with $u_a = \rho(a)LL^*\rho(a)^*$ in the Hilbert–Schmidt inner product.

Problem 40.1.1. Let Θ be of positive type on G, with vectors u_a. (a) $\Theta(s^{-1}) = \Theta(s)$ and $|\Theta(s)| \le \Theta(1) = \|u_a\|^2$ for all s, a. (b) For a subgroup $\Gamma' \subseteq G$, $\sum_{s\in\Gamma'} \Theta(s) = \|\sum_{a\in\Gamma'} u_a\|^2/\#\Gamma' \ge 0$, and the restriction of Θ to Γ' is of positive type.

Let ψ be a nontrivial additive character of $\mathbb{F}_q$; vectors are columns, y^t is a transpose and g^{-t} the inverse transpose of $g \in \mathrm{GL}_n(\mathbb{F}_q)$.

Problem 40.1.2. For a $j \times j$ matrix Z over $\mathbb{F}_q$, $\#\{y \in \mathbb{F}_q^j : y^t Z = 0\} = q^{-j} \sum_{y,v\in\mathbb{F}_q^j} \psi(y^t Z v)$, and this number is at least q if $\det Z = 0$.

Date: November 26, 2026.

The toy. In this sheet let J be the permutation matrix exchanging e_1 and e_3 and fixing e_2, the Gram matrix of the symmetric bilinear form $(x, x') \mapsto x^t J x'$ on $\mathbb{F}_p^3$. Take the frame (e_1, e_2): e_1 is isotropic and paired with e_3. The only proper leading minor of the frame products of $s \in \mathrm{GL}_3(\mathbb{F}_p)$ is $e_1^t J s e_1 = s_{31}$, so the open elements are those with $s_{31} \neq 0$. An element may fix a frame vector x in two ways: $sx = x$, or $s^{-t}(Jx) = Jx$, that is, s fixes the linear form $x' \mapsto x^t J x'$; for $x = e_1$ the second is $e_3^t s = e_3^t$.

Problem 40.1.3. By machine: in $\mathrm{GL}_3(\mathbb{F}_p)$ the group, the set $\{s_{31} = 0\}$, the fixer of e_1 and the fixer $\{s : e_3^t s = e_3^t\}$ of the form e_3^t have $168, 72, 24, 24$ elements for $p = 2$ and $11232, 3456, 432, 432$ for $p = 3$. Both fixers lie in $\{s_{31} = 0\}$.

So a weight concentrated on a fixer lives entirely where the minor vanishes. The next two problems show that this is the only obstruction: a vanishing minor is detected by characters, and the character sums are bounded by the weight of stabilizers.

Problem 40.1.4. Let $\pi\colon G \to \mathrm{GL}_n(\mathbb{F}_q)$ be a homomorphism, Θ of positive type on G, $y, v \in \mathbb{F}_q^n$ and Y real. If the s with $\pi(s)v = v$, and the s with $\pi(s)^{-t}y = y$, each carry at most Y, then

$$\Big|\sum_{s\in G} \Theta(s)\,\psi\big(y^t \pi(s) v\big)\Big| \leq q^{n/2} Y.$$

Problem 40.1.5. Let π be as in Problem 40.1.4, $\Theta \geq 0$ of positive type, A_0, A_1 two $n \times j$ matrices over $\mathbb{F}_q$ and $Y \geq 0$. Suppose that for every $v \in \mathbb{F}_q^j \smallsetminus 0$ the s with $\pi(s)A_0 v = A_0 v$, and the s with $\pi(s)^{-t}A_1 v = A_1 v$, each carry at most Y. Then

$$q \sum_{\det(A_1^t \pi(s) A_0) = 0} \Theta(s) \leq 2 \sum_{s\in G} \Theta(s) + q^j q^{n/2}\, Y.$$

Problem 40.1.6. In the toy take $j = 1$, $A_0 = e_1$, $A_1 = Je_1 = e_3$, so that $\det(A_1^t s A_0) = s_{31}$. (a) For $\Theta \equiv 1$ and Y the order of a fixer in Problem 40.1.3, Problem 40.1.5 reads $144 \leq 471.764\ldots$ for $p = 2$ and $10368 \leq 29198.213\ldots$ for $p = 3$. (b) For $p = 2$ the indicator Θ of the fixer of e_1 is of positive type; all of its mass 24 lies in $\{s_{31} = 0\}$, the least admissible Y is 24, and Problem 40.1.5 reads $48 \leq 183.764\ldots$.

For the uniform weight the elements with $s_{31} = 0$ are a proportion $3/7$ of $\mathrm{GL}_3(\mathbb{F}_2)$; for the weight of (b) they are everything. The function $s \mapsto \|\mathcal{K}_s\|^2$ is neither, and the proof never replaces its non-open part by a proportion for the uniform measure. It chooses a subgroup on which stabilizers carry little, and then Problem 40.1.5 makes the singular part small. In the toy the lemma gains almost nothing: for $p = 2$ its right side $471.7\ldots$ exceeds the trivial bound $2 \cdot 168$, and for $p = 3$ it is $29198.2\ldots$ against $3 \cdot 11232 = 33696$. It gains when $q^{j+n/2}\, Y$ is small against $q \sum \Theta$; for the data this is Problem 40.2.1 with $Y = b^{-6k} H$.

40.2. The open part and the terminal fixer

We work as the proof does: with an admissible filling (Section 36.4) over a CM field E with Weil data (Chapter 39); the data provide one, the group $\bar{G} = \prod_{w\in\mathcal{M}} \mathrm{GL}_r(k_w)$, $\mathcal{M} = \mathcal{M}_0 \cup \mathcal{M}_1$ the chosen places above p_0 and p_1, a unitary representation ρ of $\bar{G}$ on a finite-dimensional complex inner product space, and a linear

map $\mathcal{P}^\circ$ from the coordinate space with the block identity of Theorem 37.3.2. In this sheet $\mathrm{en}(s) := \|\mathcal{K}_s\|^2$, formed with the full Bessel function. By Problem 37.4.5, en is of positive type, with $u_a = \rho(a)\mathcal{P}^\circ\mathcal{P}^{\circ *}\rho(a)^*$, and $\mathrm{en}(s) \le \mathrm{en}(1)$. The proof also gives $\mathrm{en}(1) = \|\mathcal{K}_1\|^2 \le 2D_X$ in this generality (see the remark), by Theorem 38.3.3 and Problems 37.4.3 and 37.4.4, whose hypotheses ($\mathcal{K}_{st} = \mathcal{K}_s\rho_{\mathrm{Bes}}(t)$ for $t \in \bar{R}_0$, and ρ_{Bes} a unitary representation of $\bar{R}_0$) it states for every admissible filling with the block identity. Of the conditions of admissibility we use: $b \ge 1000$; $b^{10} \le p_0 \le b^{11}$ and $M = p_0p_1 \le b^{23}$; $1000(2\varrho + 2) \le k \le f$ and $\varrho + 1 \le b$; there are f chosen places above each p_i, each with residue field of p_i elements, all distinct, and no conjugate of a chosen place is chosen; $b^{11kf}D_{\mathrm{id}} \le D_{\mathrm{main}}$. The matrices s_w have size $r = k + 2\varrho + 1$.

We recall Definitions 38.2.6, 38.2.7 and 38.2.5 at a chosen place w above p_0, with one abbreviation. In this sheet a *frame vector* at w is a nonzero vector x of the span of the frame modulo w, with a side: s fixes it on the side of w if $s_wx = x$, and on the side of $\bar{w}$ if s_w^{-t} fixes Jx, where J is the Gram matrix of the lattice basis modulo w. The fixer of frame vectors given at a set $\mathcal{D} \subseteq \mathcal{M}_0$ of such places is the subgroup of the s fixing each. An element s is *open* if at some $w \in \mathcal{M}_0$ the leading minors $\langle s\rangle_1, \dots, \langle s\rangle_\varrho$ of its frame products are nonzero. With A_0 the matrix whose columns are the first j vectors $v_1, \dots, v_j$ of the frame and $A_1 = JA_0$, the minor $\langle s\rangle_j$ at w is $\det(A_1^t s_w A_0)$. An element *meets* at w (or at $\bar{w}$) if modulo that place the span of the frame and that of its image share a nonzero vector, and $\mathrm{mt}(s)$ is the product of $\#k_w$ over the places w and $\bar{w}$, $w \in \mathcal{M}$, at which s meets; an element that fixes a frame vector on a side meets at that place. An element of $\bar{R}_0$ fixes v_1 modulo every chosen place: $\mathcal{U}$ and $U(X_0)$ fix v_1 (Section 36.1), and v_1 is a vector of the lattice basis. For $s \notin \bar{R}_0$ we have $\rho_{\mathrm{Bes}}(s) = 0$, and $\mathrm{en}(s)$ is the second moment at s of the terms outside the Bessel subgroup.

Three statements are used, for sets $\mathcal{B} \subseteq \bar{G}$. Theorem 38.3.1: if z_0 is a positive integer with $z_0 \le \mathrm{mt}(s)$ for all $s \in \mathcal{B}$, the link second moment of the terms with disc $\ne 0$ over $\mathcal{B}$ is at most

$$(b^{2f}/z_0)^k\, D_{\mathrm{main}}\, \nu^2.$$

Theorem 38.3.2: if $\mathcal{B}$ avoids the scalar cosets and that link second moment is at most $C_0\nu^2$, $C_0 \ge 0$, then the second moment over $\mathcal{B}$ of the terms outside the Bessel subgroup, for the full Bessel function, has square root at most

$$\sqrt{C_0} + b^{-15}\sqrt{D_{\mathrm{id}}}.$$

Theorem 39.3.3: for a set $\mathcal{D}$ of h chosen places above p_0 with a frame vector at each, the link second moment of the terms with disc $\ne 0$ over the open elements of their fixer is at most

$$(1 + b^{-4})\, b^{-6kh}\, D_{\mathrm{main}}\, \nu^2.$$

In this sheet $y_h := b^{-6kh}D_{\mathrm{main}}$ for $0 \le h \le f$; since $b^{11kf}D_{\mathrm{id}} \le D_{\mathrm{main}}$, we have $b^{5kf}D_{\mathrm{id}} \le y_h$.

Problem 40.2.1. $p_0^j\sqrt{p_0^r} \le b^{6k}$ for $0 \le j \le \varrho$.

Problem 40.2.2. Let $\Gamma' \subseteq \bar{G}$ be a subgroup, $H := \sum_{s\in\Gamma'} \mathrm{en}(s)$ (in this sheet), and w a chosen place above p_0. Suppose that for every frame vector at w, on either side, the elements of Γ' fixing it carry at most $b^{-6k}H$. Then the elements of Γ' that are not open carry at most $b^{-4}H$.

Problem 40.2.3. If $s_w v_1 \in k_w v_1$ at a chosen place w above p_0, then $\langle s\rangle_1 = 0$ at w. Hence no $s \in \bar{G}$ with $s_w = \zeta_w t_w$ for every $w \in \mathcal{M}$, for some $t \in \bar{R}_0$ and some integral finite adele ζ with residues ζ_w, is open; in particular the open elements avoid the scalar cosets and lie outside $\bar{R}_0$.

Problem 40.2.4. Let Γ' be the fixer of frame vectors at a set of h chosen places above p_0. The open elements of Γ' carry at most $(1 + 4b^{-4})\, y_h$.

The terminal case fixes vectors at all f places above p_0.

Problem 40.2.5. (a) $(b^{2f}/p_0^f)^k\, D_{\mathrm{main}} \le y_f/8$. (b) $8M^f D_{\mathrm{id}} \le y_f$. (c) At most $M^f \# \bar{R}_0$ elements of $\bar{G}$ have the form $s_w = \zeta_w t_w$ of Problem 40.2.3.

Problem 40.2.6. Let Γ' be the fixer of frame vectors at all f chosen places above p_0. Then $\mathrm{mt}(s) \ge p_0^f$ for $s \in \Gamma'$, and Γ' carries at most y_f.

40.3. The bootstrap

Problem 40.2.2 needs a subgroup on which stabilizers carry little, and fixing a vector costs a factor b^{-6k} in Problem 40.2.4. For a set $\mathcal{D}$ of chosen places above p_0 and frame vectors at its places, let $\Gamma_{\mathcal{D}}$ be their fixer (the vectors understood); $\Gamma_{\varnothing} = \bar{G}$. The proof maximizes the *objective* $b^{6k\#\mathcal{D}} \sum_{s\in\Gamma_{\mathcal{D}}} \mathrm{en}(s)$ over the finitely many choices, the empty one included.

Problem 40.3.1. In the toy with $p = 2$, $\Theta \equiv 1$, one place, and the factor b^{6k} replaced by c: every frame vector, on either side, has a fixer of 24 elements, and the objective at (no place, the place) is $(168, 24c)$; it is $(168, 96)$ for $c = 4$ and $(168, 192)$ for $c = 8$. Either choice can be the maximum.

Problem 40.3.2. Let $\mathcal{D}$ with its frame vectors maximize the objective, $h := \#\mathcal{D}$ and $H := \sum_{s\in\Gamma_{\mathcal{D}}} \mathrm{en}(s)$. If $h < f$ and $w \notin \mathcal{D}$ is a chosen place above p_0, then the elements of $\Gamma_{\mathcal{D}}$ fixing a frame vector at w, on either side, carry at most $b^{-6k}H$, and

$$H \le (1 + 4b^{-4})\, y_h + b^{-4}H.$$

Problem 40.3.3. If $H \le (1 + 4\delta)Y + \delta H$ with $0 \le \delta \le 1/10$ and $Y \ge 0$, then $H \le (1 + 9\delta)Y$. For $\delta = 1/16$: $(1 + 4\delta)/(1 - \delta) = 4/3 \le 25/16 = 1 + 9\delta$.

Problem 40.3.4. With $\mathcal{D}$ as in Problem 40.3.2, $H \le (1 + 9b^{-4})\, y_h$; hence $\sum_{s\in\bar{G}} \mathrm{en}(s) \le (1 + 9b^{-4})\, D_{\mathrm{main}}$.

Problems 40.1.1, 40.1.2, 40.1.4, 40.1.5 and 40.2.1–40.3.4, with Theorems 38.3.1, 38.3.2 and 39.3.3 and the two properties of en recalled in Section 40.2 (positive type, and $\mathrm{en}(1) \le 2D_X$), prove the following.

Theorem 40.3.1 (the second moment)**.** *Let an admissible filling over a CM field with Weil data be given, ρ a unitary representation of $\bar{G}$ on a finite-dimensional complex inner product space, and $\mathcal{P}^\circ$ a linear map from the coordinate space satisfying the block identity of Theorem 37.3.2. Then*

$$\sum_{s\in\bar{G}} \|\mathcal{K}_s\|^2 \le (1 + 9b^{-4})\, D_{\mathrm{main}}.$$

In particular this holds for the data, with $\mathcal{P}^\circ$ the scaled Poincaré map and ρ the representation of Chapter 36.

In the Lean formalization. In the Lean proof [GL] the theorem is `Filling.HasAmplitudeBlocks.sum_hilbertSchmidtNorm_sq_le`, and for the data `Data.sum_hilbertSchmidtNorm_scaledPoincare_sq_le`; it is deduced from `Filling.sum_secondMoment_le`, which bounds the sum over $\bar{G}$ of the second moments at s of all terms, for an admissible filling with Weil data, assuming that this function of s is of positive type and at most $2D_X$ at $s = 1$, by the maximization of Section 40.3. The bound $\mathrm{en}(1) \le 2D_X$ under the block identity, for any representation, is `Filling.HasAmplitudeBlocks.hilbertSchmidtNorm_adjoint_comp_sq_le`. Problem 40.1.5 is `card_mul_sum_det_eq_zero_le`, whose proof bounds only the real part of the sum of Problem 40.1.4; Problem 40.2.2 is the case en of `Filling.sum_not_isOpenElement_le`, stated there for every function ≥ 0 of positive type; the second sentence of Problem 40.2.3, up to "in particular", is `Filling.InScalarCoset.not_isOpenElement`; Problem 40.2.4 is `Filling.secondMoment_fixer_isOpenElement_le`; the bound for the fixer in Problem 40.2.6 is `Filling.secondMoment_fixer_univ_le`, which assumes $\mathrm{en} \le 2D_X$; the first sentence of Problem 40.3.3 is `Filling.le_one_add_nine_mul_of_le_add`.

What has been proved is the second moment over the whole group, from the link bound and the cut, which Chapter 38 reads from the proof, and the open-cell bound, whose steps Chapter 39 models with statements read from the proof. With the count of Theorem 41.3.1 it gives the hypothesis of Theorem 9.3.1 on the second moment (Problem 41.3.6); the other hypothesis, the near isometry of the projected map, is Theorem 41.2.2.

Hints

§40.1.

40.1.1: $\langle u_a, u_a\rangle = \Theta(1)$ and Cauchy–Schwarz. Expand $\|\sum_a u_a\|^2$ and group the pairs (a, b) by $a^{-1}b$.

40.1.2: $\sum_v \psi(z^t v)$ is q^j if $z = 0$ and 0 otherwise; a nonzero y in the kernel gives a line.

40.1.3: Run through the p^9 matrices.

40.1.4: Write the sum as an inner product of two vectors of $\mathbb{C}^{\mathbb{F}_q^n} \otimes \mathrm{span}(u_a)$, one built from point masses, the other from the normalized characters $\xi \mapsto q^{-n/2}\psi(z^t\xi)$; then Cauchy–Schwarz.

40.1.5: Bound q times the indicator of $\det Z_s = 0$, $Z_s := A_1^t \pi(s) A_0$, by Problem 40.1.2; sum against Θ. Separate the pairs with $y = 0$ or $v = 0$, and use $y^t Z_s v = (A_1 y)^t \pi(s)(A_0 v)$ for the others.

40.1.6: For (b), $u_a := \delta_{ae_1}$.

§40.2.

40.2.1: Show $11(2j{+}r) \le 12k$, using $p_0 \le b^{11}$, $r = k{+}2\varrho{+}1$, $1000(2\varrho{+}2) \le k$.

40.2.2: A non-open element has $\langle s\rangle_j = 0$ at w for some $1 \le j \le \varrho$. For each j, Problem 40.1.5 for Γ', $\pi(s) = s_w$, $\Theta = \mathrm{en}$ and $Y = b^{-6k}H$: $A_0 v$ and $A_1 v = J(A_0 v)$ are a frame vector and its form. Then Problem 40.2.1 and $\varrho + 1 \le b$.

40.2.3: v_1 is isotropic.

40.2.4: By Problem 40.2.3, Theorems 39.3.3 and 38.3.2 apply to the open elements of Γ'. Then $\sqrt{1+\epsilon} \le 1+\epsilon/2$, $b^{-15} \le b^{-4}/2$ and $D_{\mathrm{id}} \le y_h$.

40.2.5: (a) $p_0 \ge b^{10}$. (b) $23f+1 \le 5kf$. (c) Only the residues of ζ at the $2f$ chosen places matter.

40.2.6: The pairs (place, side) at which the fixed vectors sit are distinct places above M. Split Γ' into the elements of Problem 40.2.5(c) and the rest; use $\mathrm{en} \le 2D_X$, Theorems 38.3.1 with $z_0 = p_0^f$ and 38.3.2, and $(\sqrt{C}+\sqrt{C'})^2 \le 2C+2C'$.

§40.3.

40.3.1: A nonzero vector of $\mathbb{F}_2^3$, or a nonzero form, has 7 images.

40.3.2: Adding w with one frame vector replaces $\Gamma_{\mathcal{D}}$ by its intersection with the fixer of that vector; compare the objectives. Then Problems 40.1.1(b), 40.2.2 and 40.2.4.

40.3.3: $(1-\delta)(1+9\delta) - (1+4\delta) = \delta(4-9\delta)$.

40.3.4: If $h = f$, Problem 40.2.6; otherwise $\delta = b^{-4}$. Then compare with $\mathcal{D} = \varnothing$.

References

[GL] L. Sernau, *GRH for Dirichlet L-functions, in Lean 4*, a shorter rewriting of the Lean proof, text by Claude, `https://github.com/lsernau/grh-lean`, commit `72fead1`, readable edition `grh/`.

[LN] R. Lidl and H. Niederreiter, *Finite Fields*, 2nd ed., Encyclopedia of Mathematics and its Applications **20**, Cambridge University Press, 1997.

GOOD FORMS AND THE COUNT OF THE TARGET

Prerequisites. Characters of finite groups, central idempotents, induced representations and Mackey's formula [Se, §§2, 6, 7]; the characters of $\mathrm{GL}_2(\mathbb{F}_q)$ [FH, §5.2]. From Chapter 34, *Spaces, forms and twists*: the chosen places $\mathcal{M} = \mathcal{M}_0 \cup \mathcal{M}_1$, the groups $\bar{G} = \bar{G}_0 \times \bar{G}_1$, labels, the characters Ξ_c, the idempotents e_c, good families and the idempotent e_0 (Section 34.1), with the integer q_2 of the data; the space W_m and the standard lattice stabilizer $K^\circ(V)$ (Section 34.3); principal forms $H(V)$, good forms $H_g(V)$, the target T of dimension d_T (Section 34.4); D_X (Section 34.5). From Chapter 36: the unipotent group $\mathcal{U}$ (Section 36.1) and the character $\psi_{\mathcal{U}}$ that the proof fixes on its points (Section 36.2), the scaled Poincaré map $\mathcal{P}^\circ$ and the Gram operators $\mathcal{K}_s$ (Definition 36.4.1), the group $\bar{R}_0$ and its representation ρ_{Bes} (Definition 36.4.2), the product deg of the degrees of the Bessel systems, the mass mass_r, and admissible fillings with Weil data (Section 36.4). From Chapter 37: the block identity (Theorem 37.3.2), the sizes D_{id}, D_{main} (Definition 37.3.2) and Problems 37.4.2 and 37.4.3. From Chapter 38: Theorem 38.3.3 and Problems 38.1.1, 38.3.9, 38.1.2 and 38.1.3. From Chapter 9: Hilbert–Schmidt norms $\|L\|^2 = \operatorname{tr} L^*L$, near isometries, Problem 9.3.1 and Theorem 9.3.1. From Chapter 21: class sets, masses, forms and Weyl's formula (4) (Section 21.3). From Chapter 57: Corollary 57.4.1.

Theorem B (Chapter 36) is deduced from three estimates for the scaled Poincaré map: a second moment over $\bar{G}$, the near isometry of $e_0\mathcal{P}^\circ$, and an upper bound for d_T. This sheet proves the last two from Chapters 37 and 38 and from equal multiplicities. Why does cutting $\mathcal{P}^\circ$ down to the good forms lose so little, and why is the target no larger than $\#\bar{G} \cdot \deg \cdot \mathrm{mass}_r$? The first answer is a trace against the Bessel representation, small because the conjugacy average of $\psi_{\mathcal{U}}$ is small; the second is a count of classes on the definite space W_m, where the level is free.

41.1. Central idempotents and their shares

For a finite group H, an element of $\mathbb{C}[H]$ is written $g = \sum_{t \in H} g(t)\, t$; in a representation ρ it acts by $\rho(g) := \sum_t g(t)\rho(t)$. It is a *central idempotent* if $g^2 = g$ and $t \mapsto g(t)$ is a class function.

Definition 41.1.1. The *share* of a central idempotent $g \in \mathbb{C}[H]$ is its coefficient $g(1)$ at the identity.

In this sheet q is the number of elements of a residue field.

Problem 41.1.1. The labels of degree 2 over $\mathbb{F}_3$ are X^2+1, X^2+2, X^2+X+2 and X^2+2X+2. The multiplicative orders of their roots in $\mathbb{F}_9^\times$ are $(4,4)$, $(1,2)$, $(8,8)$ and $(8,8)$. Three of them have no root 1, and two are irreducible with a root of order $8 = 3^2 - 1$.

Date: November 26, 2026.

Green's degrees. For a label c of degree r over a finite field k with $q = \#k$, the value $d := \Xi_c(1)$ of the character of Section 34.1 satisfies

$$\operatorname{Re} d \geq 0, \qquad \frac{|d|^2}{\#\mathrm{GL}_r(k)} \geq \frac{1 - r/q}{q^r}.$$

Status: classical; Green [Gr, Thms. 12–14]. For $r = 2$ the degree is $q+1$ for a label with two roots in k, $q-1$ for an irreducible one [FH, §5.2].

Problem 41.1.2. In $\mathrm{GL}_2(\mathbb{F}_3)$, of order 48, the idempotent e_c of the label $X^2 + 2$ has share $1/3$, and that of each irreducible label has share $1/12 \geq (1-2/3)/9$. The sum of the e_c over the three labels without root 1 is a central idempotent of share $1/4$.

Problem 41.1.3. Let g be a central idempotent of $\mathbb{C}[H]$, H finite. In every unitary representation of H, g acts as an orthogonal projection, and $g(1)$ is the share $\dim(g\mathbb{C}[H])/\#H$ of the regular representation that g keeps. Moreover $\sum_{t\in H} |g(t)|^2 = g(1)$, and $1 - g$ is a central idempotent.

The idempotents of the data. For $i = 0, 1$ let $g_i \in \mathbb{C}[\bar{G}_i]$ be the sum, over the families $(c_w)_{w\in\mathcal{M}_i}$ of labels such that no c_w has a root $z \in k_w$ with $z^{q_2} = 1$ and some c_w is irreducible with a root of order $p_i^r - 1$, of the tensor products $\bigotimes_w e_{c_w}$. These are central idempotents, and $g_0 \otimes g_1 \in \mathbb{C}[\bar{G}]$ acts on $H(Y_0)$ as e_0. Call a label over k_w *allowed* if it has no root $z \in k_w$ with $z^{q_2} = 1$, and *primitive* if it is irreducible with a root of order $q^r - 1$; at one place $w \in \mathcal{M}_i$, with $q = p_i$, let A be the set of allowed labels, B the set of monic polynomials of degree r over k_w that are not primitive labels, and $m' := (1 - r/q)/q^r$. For $1 < r < q$ the proof shows that each tensor product $\bigotimes_w e_{c_w}$ has share at least m'^f (by Green's degrees), that $\#A \cdot m' \geq 1 - \varepsilon'$ whenever $\varepsilon' \geq (1 + q_2 + 2r)/q$, and that $\#B \cdot m' \leq \eta := \exp\bigl(-1/(2r(2r\log q + 1))\bigr)$.

Problem 41.1.4. Let $f \geq 1$ be an integer, A, B finite sets, $m' > 0$, $0 \leq \varepsilon' \leq 1$ and $\eta \geq 0$, with $\#A \cdot m' \geq 1 - \varepsilon'$ and $\#B \cdot m' \leq \eta$. Then $(1 - \varepsilon')^f \geq 1 - f\varepsilon'$ and $m'^f(\#A^f - \#B^f) \geq 1 - f\varepsilon' - \eta^f$. Hence, in the paragraph above, the families counted in g_i include every family of allowed labels not all in B, and $\operatorname{Re}(1 - g_i)(1) \leq f\varepsilon' + \eta^f$.

With one place, η is close to 1; only its f-th power is small. The proof takes $\varepsilon' = (1 + q_2 + 2r)/p_i$ and checks, for the data, $1 < r < p_i$, $\varepsilon' \leq 1$, $2r(2r\log p_i + 1) \cdot 9\log b \leq f$ and $f\varepsilon' + e^{-9\log b} \leq b^{-8}/2$. So $\operatorname{Re}(1 - g_i)(1) \leq b^{-8}/2$ for $i = 0, 1$.

Problem 41.1.5. If p is an orthogonal projection, q' any operator on $\mathcal{Y}$ and $L\colon \mathcal{X} \to \mathcal{Y}$, then $\|(1 - pq')L\|^2 \leq \|(1 - p)L\|^2 + \|(1 - q')L\|^2$. In the regular representation of $C_5 \times C_5$, with p and q' the projections removing one character of the first and of the second factor and $L = 1$, the two sides divided by 25 are $9/25 \leq 2/5$.

41.2. The trace on the Bessel subgroup

In this section, as in Theorem 38.3.3, consider an admissible filling over a CM field E with Weil data, a unitary representation ρ of $\bar{G}$ on a finite-dimensional complex inner product space, and a linear map $\mathcal{P}^\circ$ from the coordinate space of Definition 36.4.1 to it that satisfies the block identity of Theorem 37.3.2; $\mathcal{K}_s = \mathcal{P}^{\circ *}\rho(s)\mathcal{P}^\circ$, ρ_{Bes}, $\bar{R}_0$, D_X and $D_{\mathrm{id}} = \#\bar{R}_0 \cdot D_X$ are as there. In this setting, as for the data, $\rho_{\mathrm{Bes}}(s) = 0$ for $s \notin \bar{R}_0$, ρ_{Bes} is a unitary representation of $\bar{R}_0$, and $\mathcal{K}_{st} = \mathcal{K}_s\rho_{\mathrm{Bes}}(t)$, $\mathcal{K}_{ts} = \rho_{\mathrm{Bes}}(t)\mathcal{K}_s$ for $t \in \bar{R}_0$ (read from the proof; Problem 37.4.2).

In this sheet $\iota_i\colon \bar G_i \to \bar G$ is the inclusion with identity component in the other factor, and $\rho(g) := \sum_t g(t)\rho(\iota_i(t))$ for $g \in \mathbb{C}[\bar G_i]$.

Problem 41.2.1. (a) Let $\varphi\colon H' \to H$ be a homomorphism of finite groups, g a central idempotent of $\mathbb{C}[H']$, and F a function on H with values in an inner product space. Then $\sum_{s\in H}\|\sum_{t\in H'} g(t)F(s\varphi(t))\|^2 \le \sum_{s\in H}\|F(s)\|^2$.

(b) Let $g \in \mathbb{C}[\bar G_i]$ be a central idempotent and $D_g := \sum_{t\in\bar G_i} g(t)\big(\mathcal{K}_{\iota_i(t)} - \rho_{\mathrm{Bes}}(\iota_i(t))\big)$. Then $\#\bar R_0 \cdot \|D_g\|^2 \le b^{-12}D_{\mathrm{id}}$, so $\|D_g\|^2 \le b^{-12}D_X$ and $|\operatorname{tr} D_g| \le b^{-6}D_X$.

There remains the trace of ρ_{Bes} against g. The proof shows: if $s \in \bar G$ has component 1 in $\bar G_0$ or in $\bar G_1$, then

$$\operatorname{tr}\rho_{\mathrm{Bes}}(s) = D_X\,\psi_{\mathcal{U}}(s),$$

where, in this sheet, $\psi_{\mathcal{U}}(s)$ is the value of that character at an integral finite adelic element of $\mathcal{U}$ reducing to s, which does not depend on the element, and $\psi_{\mathcal{U}}(s) := 0$ if there is none. (A Bessel term reducing to 1 at one prime has trivial definite part, by an argument like that of Problem 41.3.2; the unipotent part multiplies the identity block by $\psi_{\mathcal{U}}$.)

Definition 41.2.1. The *conjugacy average* of a function ψ on a finite group H is $\psi^\natural(s) := (\#H)^{-1}\sum_{y\in H}\psi(ysy^{-1})$.

Problem 41.2.2. In S_3 let $\varphi = 1$ at 1, -1 at (12) and 0 elsewhere. Its conjugacy average is 1, $-1/3$, 0 on the identity, the transpositions and the 3-cycles, and $\sum_s|\varphi(s)|^2 = 2$, $\sum_s|\varphi^\natural(s)|^2 = 4/3$.

Problem 41.2.3. For a character ψ of a subgroup $R \subseteq H$, extended by zero to H, $\sum_{s\in H}|\psi^\natural(s)|^2 = \#R^2 \cdot \dim \operatorname{End}_H(\operatorname{Ind}_R^H \psi)/\#H$.

Problem 41.2.4. Let $U \subset \mathrm{GL}_2(\mathbb{F}_p)$ be the upper unitriangular group and $\psi_U(u) := e^{2\pi i u_{12}/p}$. By Problem 38.1.2, $\sum_s|\psi_U^\natural(s)|^2 = p^2/(p^2-1)$: 9/8 for $p = 3$, 25/24 for $p = 5$. For the upper unitriangular group of $\mathrm{GL}_3(\mathbb{F}_2)$ and $\psi_U(u) = (-1)^{u_{12}+u_{23}}$, Problem 38.1.3 gives 32/21.

The conjugacy average of $\psi_{\mathcal{U}}$. For an admissible filling with Weil data,

$$\sum_{s\in\bar G}|\psi_{\mathcal{U}}^\natural(s)|^2 \le 2.$$

Status: read from the proof. There the conjugacy average is written as an integral over the integral points at the chosen places and their conjugates, and bounded by a count of shells; this sheet does not treat it.

Problem 41.2.5. Let $g \in \mathbb{C}[\bar G_i]$ be a central idempotent with $\operatorname{Re} g(1) \le b^{-8}/2$. Then $\big|\sum_t g(t)\operatorname{tr}\rho_{\mathrm{Bes}}(\iota_i(t))\big| \le D_X\sqrt{2\operatorname{Re} g(1)} \le b^{-4}D_X$, and $\|\rho(g)\mathcal{P}^\circ\|^2 \le 2b^{-4}D_X$.

Recall from Chapter 9 that $L\colon \mathcal{X} \to \mathcal{Y}$ is a near isometry with error ε if $\dim Z - \varepsilon\dim\mathcal{X} \le \|L\operatorname{pr}_Z\|^2$ for every subspace $Z \subset \mathcal{X}$, where pr_Z is the orthogonal projection onto Z, and that by Problem 9.3.1 this holds if $\varepsilon \ge 0$ and $\|L^*L - 1\|^2 \le \varepsilon^2\dim\mathcal{X}$.

Problem 41.2.6. If L is a near isometry with error ε, p is an orthogonal projection and $\|(1-p)L\|^2 \le \varepsilon'\dim\mathcal{X}$, then pL is a near isometry with error $\varepsilon + \varepsilon'$.

For central idempotents $g_0 \in \mathbb{C}[\bar{G}_0]$, $g_1 \in \mathbb{C}[\bar{G}_1]$, the element $g_0 \otimes g_1 \in \mathbb{C}[\bar{G}]$ has coefficient $g_0(s_0)g_1(s_1)$ at (s_0, s_1), and $\rho(g_0 \otimes g_1) = \rho(g_0)\rho(g_1)$, a product of two commuting orthogonal projections. Problems 41.1.3, 41.1.5 and 41.2.5 (with $g = 1 - g_i$) prove part (a) of the following theorem; Problem 38.3.9, whose proof (Theorem 38.3.3 on $\bar{R}_0$ and Problem 37.4.3) holds in the setting of this section, and Problems 9.3.1 and 41.2.6 then prove part (b). Part (c) follows from (b) and the paragraph on the idempotents of the data.

Theorem 41.2.2 (good forms)**.** *In the setting of this section, let $g_i \in \mathbb{C}[\bar{G}_i]$ be central idempotents with $\mathrm{Re}(1 - g_i)(1) \le b^{-8}/2$ for $i = 0, 1$, and $e := \rho(g_0 \otimes g_1)$. Then*

(a) $\|(1 - e)\mathcal{P}^\circ\|^2 \le 4b^{-4}D_X$*;*
(b) $\|e\mathcal{P}^\circ \,\mathrm{pr}_Z\|^2 \ge \dim Z - 5b^{-4}D_X$ *for every subspace Z of the coordinate space: $e\mathcal{P}^\circ$ is a near isometry with error $5b^{-4}$.*

(c) For the data, with ρ the action of $\bar{G}$ on $H(Y_0)$ and $\mathcal{P}^\circ$ the scaled Poincaré map, which satisfy the hypotheses of this section (Chapter 37), the idempotents g_0, g_1 of Section 41.1 satisfy these hypotheses and e is the action of e_0: $e_0\mathcal{P}^\circ$ is a near isometry with error $5b^{-4}$.

41.3. The count of the target

On a definite group a form is a vector of the weight at each class, fixed by the stabilizer of the class. First the smallest case.

Problem 41.3.1. Let $E = \mathbb{Q}(\mathrm{i})$, and let the unitary group of rank one over E, at the level K of the lattice $\mathbb{Z}[\mathrm{i}]$, have class number one, stabilizer $\Gamma \cap K = \mu_4$ (Γ the rational points) and mass $\mathrm{mass}_1 = 1/4$. At the split prime $13 = (3 + 2\mathrm{i})(3 - 2\mathrm{i})$ take the place $w = (3 + 2\mathrm{i})$, where $\mathrm{i} \equiv 5$. Then μ_4 reduces to $\{1, 5, 12, 8\} \subset \mathbb{F}_{13}^\times$, no unit other than 1 reduces to 1, and the level of integral elements reducing to 1 at w has $12/4 = 3$ classes, which is $\#\bar{G} \cdot \mathrm{mass}_1$ for $\bar{G} = \mathbb{F}_{13}^\times$.

In Problem 41.3.2, $n \ge 1$ is a size.

Problem 41.3.2. Let E be a CM field, γ a rational unitary matrix of size n of the standard definite space over E, and h a finite adelic unitary matrix such that $h^{-1}\gamma h$ is integral at every finite place and reduces to 1 at distinct finite places $w_1, \dots, w_l$ with $(2n)^{[E:\mathbb{Q}]} < \prod_i \#k_{w_i}$. Then $\gamma = 1$. In particular this holds if $(2n)^2 < p$, $[E : \mathbb{Q}] = 2f$, and $w_1, \dots, w_f$ have residue fields with p elements.

The proof checks this inequality at the f chosen places above p_0 for the rank r of W_m. So every class of W_m at the principal level has trivial stabilizer.

Problem 41.3.3. Let Γ be the rational points of the finite adelic unitary group G_f of a definite space, $K' \subseteq K$ compact open subgroups of G_f, and $\Gamma_h(K) := \Gamma \cap hKh^{-1}$. (a) $\sum_{[h] \in \Gamma\backslash G_f/K'} 1/\#\Gamma_h(K') = [K : K'] \sum_{[h] \in \Gamma\backslash G_f/K} 1/\#\Gamma_h(K)$. (b) If every $\Gamma_h(K')$ is trivial and π is a representation of Γ on a space A, the functions $\varphi\colon G_f \to A$ with $\varphi(\gamma hk) = \pi(\gamma)\varphi(h)$ for $\gamma \in \Gamma$, $k \in K'$ form a space of dimension $\#(\Gamma\backslash G_f/K') \cdot \dim A$. (c) For W_m, $K = K^\circ(W_m)$ and K' the principal level, $[K : K'] = \#\bar{G}$, and, since the principal level is free and mass_r is the sum of (a) at the level K, the number of classes at the principal level is $\#\bar{G} \cdot \mathrm{mass}_r$.

Harish-Chandra's formal degree. Let ε be signs of rank r and $l = (l_1, \dots, l_r)$ distinct integers $\equiv r - 1 \pmod 2$ with $|l_i - l_j| \ge 2(500r^3 + 10r^5)$ whenever $\varepsilon_i \ne \varepsilon_j$. The

formal degree of the discrete series of the unitary group of the signs ε with doubled parameter l is

$$\prod_{l_i>l_j} \frac{l_i-l_j}{2} \Big/ \prod_{a=0}^{r-1} a!,$$

whatever the signs. *Status*: classical; Harish-Chandra [HC, Thm. 16]. For definite signs it is Weyl's formula (4) with $z = l/2 + (r-1)/2$.

Problem 41.3.4. For the doubled parameter $(6, 2, -2)$ the quotient is 8, the dimension of $\mathbb{S}_{(2,1,0)}(\mathbb{C}^3)$.

In the proof the degree of the Bessel system at each infinite place τ is this product for the doubled parameter $2\varsigma_\tau$, so deg is the product over τ of the formal degrees; and on the definite space W_m the principal forms are the functions of Problem 41.3.3(b), at the principal level, with values in a representation of dimension deg.

Problem 41.3.5. Hence $\dim H(W_m) = \#\bar{G} \cdot \mathrm{mass}_r \cdot \deg$, and with Corollary 57.4.1 for $j = m$, $d_T \le \#\bar{G} \cdot \deg \cdot \mathrm{mass}_r$. In the toy of Chapter 37, where the 32 elements of Γ_{I_2} have distinct reductions modulo $2+\mathrm{i}$ in $\mathrm{GL}_2(\mathbb{F}_5)$ (order 480), and the weight is $\mathbb{C}^2$: $30 = 480 \cdot \frac{1}{32} \cdot 2$.

Problems 41.3.2, 41.3.3 and 41.3.5, with Corollary 57.4.1, Harish-Chandra's formal degree and the facts read from the proof stated after Problems 41.3.2 and 41.3.4, prove the following.

Theorem 41.3.1 (the count)**.** *For all data,* $d_T \le \#\bar{G} \cdot \deg \cdot \mathrm{mass}_r$.

The second moment, Theorem 40.3.1, reads

$$\sum_{s\in\bar{G}} \|\mathcal{K}_s\|^2 \le (1 + 9b^{-4})\, D_{\mathrm{main}}.$$

Problem 41.3.6. Then $d_T \sum_{s\in\bar{G}} \|\mathcal{K}_s\|^2 \le \#\bar{G}\,(1 + 9b^{-4})\, D_X^2$: with Theorem 41.2.2(c), this is the hypothesis of Theorem 9.3.1 for $\Gamma = \bar{G}$, S the coordinate space, $B = \mathcal{P}^\circ$ and p the action of e_0 on $H(Y_0)$, whose image T_0 is the target T, and any $\varepsilon \ge 9b^{-4}$.

This sheet has proved Theorem 41.2.2(a), (b) from Theorem 38.3.3, Problem 38.3.9 and two statements taken as given (the trace of ρ_{Bes} and the bound for the conjugacy average of $\psi_{\mathcal{U}}$), and Theorem 41.3.1 from equal multiplicities, freeness and class sums. Also taken as given: Green's degrees, Harish-Chandra's formal degree, the facts read from the proof after Problems 41.3.2 and 41.3.4 and in the paragraph on the idempotents of the data. Chapter 36 combines both theorems with the second moment to obtain Theorem B.

In the Lean formalization. In the Lean proof [GL] (`grh/src/`, namespace `New` omitted), Theorem 41.2.2(a), (b) are `Filling.HasAmplitudeBlocks.hilbertSchmidtNorm_one_sub_piTensorElem_comp_sq_le` and `Filling.HasAmplitudeBlocks.isNearIsometry_piTensorElem_comp`; (c) is `Data.bad_types_rare` with `Data.isNearIsometry_e₀_comp_scaledPoincare`. The facts read from the proof opening Section 41.2 are `Filling.besselTranslate_eq_zero`, `Filling.besselTranslate_one`, `Filling.besselTranslate_mul`, `Filling.adjoint_besselTranslate`,

`Filling.HasAmplitudeBlocks.adjoint_comp_rep_mul_right` and `Filling.HasAmplitudeBlocks.adjoint_comp_rep_mul_left`. The last bound of Problem 41.2.5 is `Filling.HasAmplitudeBlocks.hilbertSchmidtNorm_asAlgebraHom_comp_sq_le`; for its first bound `Filling.re_sum_coeff_mul_trace_besselTranslate_le` states the real part, and its proof bounds the absolute value. The share bounds are `re_coeff_one_sub_sum_tupleIdem_le` and `Data.re_coeff_one_sub_goodIdempotentAbove_le`, and the three facts of the paragraph on the idempotents of the data are `prod_le_re_tupleIdem_coeff_one`, `one_sub_le_card_allowed_mul` and `card_not_primitive_mul_le`; the trace of ρ_{Bes} is `Filling.trace_besselTranslate_eq_mul_reducedChar`; Definition 41.2.1 for $\psi_{\mathcal{U}}$ is `Filling.reducedCharMean`, and its bound is `Filling.sum_norm_reducedCharMean_sq_le`. Green's degrees are `labelChar_degree_bounds`, Harish-Chandra's formal degree the first part of `Orbital.harish_chandra_degree_and_orbital`. Theorem 41.3.1 is `Data.targetDim_le_card_mul_besselDegree_mul_mass`; freeness is `Variety.eq_one_of_reduceAt_eq_one`, stated there for E with at least two infinite places, and applied to W_m through `Variety.classAut_eq_bot` in `Data.classAut_eq_bot_of_le_levelOf_chosenPlace`, used by `Data.classAut_eq_bot_of_le_chosenLevel`; $\dim H(W_m)$ is `Data.finrank_principalForms_spaceW`, and the degree of the Bessel system is the field `deg_eq` of `Filling.IsDiscreteSeriesBessel`, at the parameter $2\varsigma_\tau$ by `Data.isDiscreteSeriesBessel_filling_besselSystem`.

Hints

§41.1.

41.1.1: $\mathbb{F}_9 = \mathbb{F}_3[\mathrm{i}]$.

41.1.2: The share of e_c is $\Xi_c(1)^2/\#\mathrm{GL}_2(\mathbb{F}_3)$. Which labels are irreducible?

41.1.3: Write g as a sum of the idempotents e_χ of the irreducible characters. For the last identity compare the coefficients at 1 of g^2 and g.

41.1.4: Induction on f. The good tuples are the tuples of allowed labels minus those with no primitive member.

41.1.5: Split $1 - pq'$ into two orthogonal pieces.

§41.2.

41.2.1: (a) H' acts unitarily on functions on H by right translation through φ. (b) Apply (a), with $\varphi = \iota_i$ and the Hilbert–Schmidt inner product, to $\mathcal{K}_s - \rho_{\mathrm{Bes}}(s)$ on the set of Theorem 38.3.3 pinned in $\bar{G}_{1-i}$, and 0 elsewhere.

41.2.3: $\psi^\natural$ is a multiple of the induced character.

41.2.4: By Mackey, $\dim \mathrm{End}_H(\mathrm{Ind}_U^H \psi_U)$ is the number of double cosets supporting the functions of Problem 38.1.1.

41.2.5: Since g is a class function, $\psi_{\mathcal{U}}$ may be replaced by $\psi_{\mathcal{U}}^\natural$. For the second bound, $\|\rho(g)\mathcal{P}^\circ\|^2 = \mathrm{tr}(\mathcal{P}^{\circ *}\rho(g)\mathcal{P}^\circ)$.

§41.3.

41.3.1: The classes are the orbits of μ_4 on $\mathbb{F}_{13}^\times$.

41.3.2: Consider the norm from E to $\mathbb{Q}$ of $\mathrm{tr}(\gamma) - n$.

41.3.3: (a) Each K-class splits into K'-classes; count by orbit and stabilizer. (c) W_m has identity Gram matrix, so $\Gamma_h(K^\circ(W_m))$ is the automorphism

group of the lattice h applied to the standard one. Reduction maps $K^\circ(W_m)$ onto $\bar{G}$: the p_i split completely and $\mathcal{M}$ contains no two conjugate places.

41.3.5: The principal forms on W_m contain the good ones.

References

[FH] W. Fulton and J. Harris, *Representation Theory: A First Course*, Grad. Texts in Math. 129, Springer, 1991.

[GL] L. Sernau, *GRH for Dirichlet L-functions, in Lean 4*, a shorter rewriting of the Lean proof, text by Claude, `https://github.com/lsernau/grh-lean`, commit `72fead1`, readable edition `grh/`.

[Gr] J. A. Green, *The characters of the finite general linear groups*, Trans. Amer. Math. Soc. **80** (1955), 402–447.

[HC] Harish-Chandra, *Discrete series for semisimple Lie groups. II*, Acta Math. **116** (1966), 1–111.

[Se] J.-P. Serre, *Linear Representations of Finite Groups*, Grad. Texts in Math. 42, Springer, 1977.

THEOREM A: SHORT FORMS

Prerequisites. Modules over a discrete valuation ring: a submodule of finite index in $\mathbb{Z}_{(p)}^n$ is free of rank n, and a matrix over $\mathbb{Q}$ can be brought to diagonal form by invertible matrices over $\mathbb{Z}_{(p)}$ [La, Ch. III, §7]. From Chapter 5, the principle that size is compared with divisibility. From Chapter 33: the data (scales $x < x_1 < b$, $a = xb$, $L = \log b$; the CM field E with its set Φ of f infinite places; m, k, the weights κ, the principal level $M = p_0p_1$, with $p_0 \neq p_1$ primes, and the prime level N), the amounts h_{main} and rem and the unit $U = faL^3$. From Chapter 34: the source forms, the group $\bar{G}$, the idempotent e_0, the target T, tame characters, twists and the lower chain. From Chapter 36: the Poincaré map. From Chapter 43: the composite lift and the seesaw identity. From Chapter 48: the gain $\mathrm{gain}(p)$, the set Π of primes $p < x_1$ with $\chi_K(p) \neq 1$, and the divisibility of the composite lift. From Chapter 51: the size of the composite lift. Chapter 23 treats small-rank examples of single definite lifts and their norms.

Theorem A says that the ramified source is spanned by integral forms whose translated images have short lifts at the trivial twist. It also bounds the index of every finite family of translated images of integral ramified forms in terms of the number of translates used. The last chapter of this part uses both bounds. The normalization multiplies by a positive rational number c_B, with exponent $-\lfloor \mathrm{gain}(p) - \mathrm{err}(p) \rfloor$ at each prime p in the product, including the level prime N; the price of the shortness is paid in index. We first do this with rational vectors, and then follow the exponents in the proof; the size of the composite lift is the subject of Chapter 51.

42.1. Index and colength over $\mathbb{Z}$

Let $\mathbb{Z}_{(p)}$ be the ring of rationals with denominator prime to p, and v_p the p-adic valuation, normalized by $v_p(p) = 1$, with $v_p(0) = +\infty$. Let $y = (y_i)_{i \in \mathcal{J}}$ be a finite family in $\mathbb{Q}^n$. A square matrix $u = (u_{ik})_{i,k \in \mathcal{J}}$ over $\mathbb{Z}_{(p)}$ *carries* y *with loss* δ_p if every $\sum_k u_{ik} y_k$ lies in $\mathbb{Z}_{(p)}^n$ and $v_p(\det u) \leq \delta_p$. The family *has index at most* δ if there are real numbers $\delta_p \geq 0$ with $\sum_p \delta_p \log p \leq \delta$ such that for every prime p some matrix carries y with loss δ_p.

Problem 42.1.1. The family $(1/6)$ in $\mathbb{Q}$ has index at most $\log 6$, and not at most δ for any $\delta < \log 6$.

Problem 42.1.2. A finite family y in $\mathbb{Q}^n$ has index at most δ if and only if $\delta \geq \log [\Lambda_y : \mathbb{Z}^n]$, where $\Lambda_y = \mathbb{Z}^n + \sum_i \mathbb{Z} y_i$. For the family $((\frac{1}{2}, \frac{1}{2}), (0, \frac{1}{4}))$ in $\mathbb{Q}^2$ one has $[\Lambda_y : \mathbb{Z}^2] = 8$.

Problem 42.1.3. If $\mathcal{J} = \mathcal{J}' \sqcup \mathcal{J}''$ and the two subfamilies have index at most δ' and δ'', then y has index at most $\delta' + \delta''$. Hence a family that is the union of h subfamilies of index at most δ has index at most $h\delta$. For the families $(\frac{1}{2}, \frac{1}{3})$ and $(\frac{1}{2}, \frac{1}{2})$ in $\mathbb{Q}$, split into singletons, the bound is $\log 6$ and $2 \log 2$, and the index is $\log 6$ and $\log 2$.

Date: November 26, 2026.

Problem 42.1.4. Let W be a submodule of $\mathbb{Z}_{(p)}^k$ with $\mathbb{Z}_{(p)}^k/W$ of order p^j. For every finite family $(\varphi_i)_{i\in\mathcal{J}}$ in $\mathbb{Z}_{(p)}^k$ there is a square matrix u over $\mathbb{Z}_{(p)}$ with $v_p(\det u)\le j$ and $\sum_k u_{ik}\varphi_k \in W$ for every i.

Problem 42.1.5. Let $A\colon \mathbb{Q}^k\to\mathbb{Q}^n$ be linear. Suppose that for every prime p there is a submodule $W_p\subseteq\mathbb{Z}_{(p)}^k$ of index p^{j_p} with $A(W_p)\subseteq\mathbb{Z}_{(p)}^n$, and $j_p=0$ for almost all p. Then every finite family in $A(\mathbb{Z}^k)$ has index at most $\sum_p j_p\log p$.

42.2. A model of Theorem A

Let $B\colon\mathbb{Q}^k\to\mathbb{Q}^n$ be linear; it stands for the chain of lifts. Let Π_0 be a finite set of primes, and suppose that for each $p\in\Pi_0$ we are given a real number γ_p and a submodule $W_p\subseteq\mathbb{Z}_{(p)}^k$ of index p^{j_p} on which B is divisible: $v_p(B\varphi)\ge\gamma_p$ coordinatewise for $\varphi\in W_p$. For $p\notin\Pi_0$ put $\gamma_p=j_p=0$ and $W_p=\mathbb{Z}_{(p)}^k$, and suppose $B(\mathbb{Z}_{(p)}^k)\subseteq\mathbb{Z}_{(p)}^n$ for these p. Put

$$g_p=\lfloor\gamma_p\rfloor,\qquad c_B=\prod_{p\in\Pi_0}p^{-g_p},\qquad A=c_BB.$$

Problem 42.2.1. For every prime p, $v_p(c_B)=-g_p$ and $A(W_p)\subseteq\mathbb{Z}_{(p)}^n$. Hence every finite family in $A(\mathbb{Z}^k)$ has index at most $\sum_p j_p\log p$, and $|A\varphi|^2=c_B^2|B\varphi|^2$ with $2\log c_B\le -2\sum_{p\in\Pi_0}\gamma_p\log p+2\sum_{p\in\Pi_0}\log p$.

Problem 42.2.2. Let $k=n=2$, $\Pi_0=\{2,3\}$ and $B(\varphi_1,\varphi_2)=(4\varphi_1+6\varphi_2,12\varphi_2)$.

(1) With $\gamma_2=1$, $W_2=\mathbb{Z}_{(2)}^2$ and $\gamma_3=1$, $W_3=\{\varphi:3\mid\varphi_1\}$, one has $c_B=1/6$; the least δ such that (Ae_1,Ae_2) has index at most δ is $\log 3$, and $|Ae_1|^2=4/9$, $|Ae_2|^2=5$.
(2) With $\gamma_2=2$, $W_2=\{\varphi:2\mid\varphi_2\}$ and the same choice at 3, one has $c_B=1/12$; this least δ is $\log 6$, and $|Ae_1|^2=1/9$, $|Ae_2|^2=5/4$.

Problem 42.2.3. The vectors of $\mathbb{Z}^k$ with all coordinates in $\{0,\pm1\}$ span $\mathbb{C}^k$. If $T_1,\dots,T_f$ are commuting complex-linear isometries of $\mathbb{C}^k$ preserving $\mathbb{Z}^k$, the image of $\prod_i(1-T_i)$ is spanned by integral vectors of squared norm at most 4^fk.

In Problem 42.2.2, increasing γ_2 by one halves c_B, shortens the image, and increases the index of the family by $\log 2$. For each prime p and each ring homomorphism $\mathbb{C}\to\mathbb{C}_p$, the divisibility theorem of Chapter 48 gives a submodule of the integral ramified source forms of colength exponent at most $\mathrm{err}(p)$ times the dimension of the full source. On this submodule the composite lift has valuation at least $\mathrm{gain}(p)-\mathrm{err}(p)$ for every twist of level prime to p and every chain datum for that twist.

42.3. Theorem A

Put $\Sigma:=\sum_{p\in\Pi}\mathrm{gain}(p)\log p$, as in Chapter 51. The composite lift $B_{\vartheta,\Psi}$ of Chapter 43 is defined on all source forms; for a twist ϑ it depends on a chain datum Ψ for ϑ, a finitely supported function on the translations. Write $G_f(V)$ for the group of finite adelic points of the unitary group of a space V. For a form F on X_0 or on Y_m and $\sigma\in\mathrm{Aut}(\mathbb{C})$, $|\sigma F(g)|^2$ denotes the Weyl squared norm of the conjugate value. By Theorem 51.3.6, if Ψ is a chain datum for the trivial twist,

$\sigma \in \mathrm{Aut}(\mathbb{C})$, $\varphi \in S$, $c \in \mathbb{R}$, and $|\sigma\varphi(g)|^2 \le e^c$ for every $g \in G_f(X_0)$, then for every $y \in G_f(Y_m)$

$$|\sigma(B_{1,\Psi}\varphi)(y)|^2 \le \exp\bigl(c + h_{\mathrm{main}} - m\,\mathrm{rem} + 2\Sigma + U\bigr).$$

This is a statement at the trivial twist only.

The spaces $S \supseteq S_{\mathrm{ram}}$ of source forms and ramified source forms, the set $S^{\mathrm{int}}_{\mathrm{ram}}$ of ramified forms integral at every ι, the dimension $D_X = \dim S$, the group $\bar{G}$ and its action ρ on the principal forms $H(Y_0)$, the target T, tame characters ξ, twists and m-fold twists ϑ with their moduli Q_ϑ, and the lower chain Θ_ξ are as in Chapter 34; the Poincaré map $\mathcal{P}\colon S \to H(Y_0)$ is that of Chapter 36. A form is integral at a ring homomorphism $\eta\colon \mathbb{C} \to \mathbb{C}_p$ if all its values have gauge at most 1 at η; integrality at ι is integrality at the homomorphism induced by ι, and $\mathcal{O}_\iota$ is the ring of $z \in \mathbb{C}$ with $|\iota(z)|_p \le 1$. For $Z > 0$ a form φ is *Z-short* if it is integral at every $\eta\colon \mathbb{C} \to \mathbb{C}_p$, for every prime p, and $|\sigma\varphi(g)|^2 \le Z$ for all $\sigma \in \mathrm{Aut}(\mathbb{C})$ and all g. For a form F on Y_m of specified level K and character, $\|F\|^2_\sigma$ is the sum over the double classes at level K of $|\sigma F(g)|^2$ at the chosen representatives g, each weighted by the reciprocal of the order of its stabilizer. For $\lambda \in \mathbb{C}$ the squared norm of $\sigma(\lambda F(g))$ is $|\sigma(\lambda)|^2$ times that of $\sigma F(g)$, and the gauge of $\lambda F(g)$ at η is $|\eta(\lambda)|_p$ times that of $F(g)$.

The text uses five inputs. Inputs 2 and 4 are theorems of the chapters named; input 1 is derived below from one statement read from the proof [GL]; inputs 3 and 5 are read from the proof, and no chapter develops them.

(1) The e^U-short forms in S_{ram} span S_{ram}. Problems 42.3.1 and 42.3.2 derive this from the statement before them (compare Problem 42.2.3).

(2) *Seesaw.* There is $c_{\mathrm{ss}} \in \mathbb{C}^\times$ such that for every twist ϑ there is a chain datum Ψ for ϑ with $\Theta_\vartheta(\mathcal{P}\varphi) = c_{\mathrm{ss}} B_{\vartheta,\Psi}\varphi$ for all $\varphi \in S_{\mathrm{ram}}$ (Theorem 43.4.1, at the point and the linear form that define $\mathcal{P}$).

(3) *Good part.* Let $z \in H(Y_0)$ and $s \in \bar{G}$. If $|\sigma(\Theta_1 z)(g)|^2 \le e^c$ for all $g \in G_f(Y_m)$, with $c \in \mathbb{R}$ and a fixed $\sigma \in \mathrm{Aut}(\mathbb{C})$, then $\|\Theta_1(\#\bar{G}\,\rho(e_0)\rho(s)z)\|^2_\sigma \le e^{x^{99}+c}$. For every prime p, every ring homomorphism $\eta\colon \mathbb{C} \to \mathbb{C}_p$, every tame character ξ and every $\lambda \in \mathbb{C}$, if $\lambda\,\Theta_\xi z$ is integral at η, so is $\lambda\,\Theta_\xi(\#\bar{G}\,\rho(e_0)\rho(s)z)$. We use both estimates as inputs.

(4) *Divisibility.* Theorem 48.7.2. We write M_η for its module $S_{\mathrm{ram},\eta}$ of forms in S_{ram} integral at η, and $j_{p,\eta}$ and $S'_{p,\eta}$ for the integer l and the module S' of its part (d) at (p,η). That the colength of $S'_{p,\eta}$ in M_η divides $p^{j_{p,\eta}}$ means (Section 42.1) that every finite family in M_η is carried into $S'_{p,\eta}$ by a square matrix over $\mathcal{O}_\eta$, the ring of $z \in \mathbb{C}$ with $|\eta(z)|_p \le 1$, whose determinant divides $p^{j_{p,\eta}}$.

(5) $\dim S_{\mathrm{ram}} \ge (1 - f/(N-1))D_X$, and $f/(N-1) \le b^{-8}$.

Moreover the data satisfy (Chapter 33) $b \ge 2$, $N \ge x_1$, $\sum_{p \in \Pi \cup \{N\}} \log p \le b$ and $x^{99} + 4U + 2b \le faL^4$.

For input 1 the proof [GL] constructs, from bases of the lattice classes of X_0 whose vectors are short at every complex embedding, source forms supported on one class, and obtains: *the $4^{-f}e^U$-short forms in S span S. Status*: read from the proof.

Problem 42.3.1. Let $w \mid \pi_N$ be a prime of E, T_w the operator of Section 34.5, and $Z > 0$. If $\varphi \in S$ is Z-short, then $(1 - T_w)\varphi$ is $4Z$-short.

Problem 42.3.2. There are f primes $w \mid \pi_N$ of E. Hence $\prod_{w|\pi_N}(1-T_w)$ maps $4^{-f}e^U$-short forms to e^U-short forms, and the e^U-short forms in S_{ram} span S_{ram}.

Definition 42.3.1. Fix err as in input 4 and c_{ss} as in input 2. As in Section 42.2, put $g_p = \lfloor \mathrm{gain}(p) - \mathrm{err}(p) \rfloor$ and $c_B = \prod_{p \in \Pi \cup \{N\}} p^{-g_p}$, a positive rational number. For $s \in \bar{G}$ the *normalized translate* $A_s \colon S_{\mathrm{ram}} \to T$ is

$$A_s\varphi = c_B\, c_{\mathrm{ss}}^{-1}\, \#\bar{G}\, \rho(e_0)\rho(s)\, \mathcal{P}\varphi.$$

Problem 42.3.3. $\log c_B \le -\Sigma + U + b$.

Problem 42.3.4. For every prime p and every ι above p, $|\iota(c_B)|_p = p^{g_p}$, and $g_p = 0$ for $p \notin \Pi \cup \{N\}$.

Problem 42.3.5. $U + (h_{\mathrm{main}} - m\,\mathrm{rem} + 2\Sigma + U) + x^{99} + 2\log c_B \le h_{\mathrm{main}} - m\,\mathrm{rem} + x^{99} + 4U + 2b$.

Problem 42.3.6. Every e^U-short $\varphi \in S_{\mathrm{ram}}$ lies in $S_{\mathrm{ram}}^{\mathrm{int}}$ and satisfies $\|\Theta_1 A_s\varphi\|_\sigma^2 \le \exp(h_{\mathrm{main}} - m\,\mathrm{rem} + faL^4)$ for all $s \in \bar{G}$ and $\sigma \in \mathrm{Aut}(\mathbb{C})$.

Problem 42.3.7. $D_X \le 2 \dim S_{\mathrm{ram}}$.

Vectors of T integral at ι, and the index of a finite family in T, are those of the target lattice (Definition 34.11.1): $y \in T$ is integral at ι above p if $\Theta_\vartheta y$ is integral at ι for every m-fold twist ϑ of level prime to p, and a family has index at most δ if matrices over the rings $\mathcal{O}_\iota$, with determinants of total weighted valuation at most δ, carry it into the integral vectors. This is the carrying condition of Section 42.1 at each ι, with one matrix carrying the family into the vectors integral for all allowed twists at once.

Problem 42.3.8. Let ι lie above p, and let η be the homomorphism induced by ι. Then $A_s\varphi$ is integral at ι for every $\varphi \in S'_{p,\eta}$ and every $s \in \bar{G}$.

Problem 42.3.9. For each $s \in \bar{G}$, every finite family in $A_s(S_{\mathrm{ram}}^{\mathrm{int}})$ has index at most $\dim S_{\mathrm{ram}} \cdot 2U$.

The proof [GL] establishes the following two statements.

Theorem 42.3.2 (Theorem A)**.** (a) *The complex span of the set of $\varphi \in S_{\mathrm{ram}}^{\mathrm{int}}$ such that*

$$\|\Theta_1 A_s\varphi\|_\sigma^2 \le \exp\bigl(h_{\mathrm{main}} - m\,\mathrm{rem} + faL^4\bigr) \quad \textit{for all } s \in \bar{G} \textit{ and } \sigma \in \mathrm{Aut}(\mathbb{C})$$

is S_{ram}.

(b) *Let $J \subseteq \bar{G}$ be finite, $n \in \mathbb{N}$, and $y_1, \dots, y_n \in T$. If each y_i lies in $A_s(S_{\mathrm{ram}}^{\mathrm{int}})$ for some $s \in J$, then $(y_1, \dots, y_n)$ has index at most $\#J \cdot \dim S_{\mathrm{ram}} \cdot 2faL^3$.*

Neither part asks the forms to be independent or the images to span; Theorem B of Chapter 36 supplies few translates whose images span almost all of T. In the exponent of (a) the gains have disappeared and the remainder appears with the factor m. The last chapter of this part compares this upper bound with a lower bound in which the main amount h_{main} appears without the remainder.

In the Lean formalization. In the Lean proof [GL], Theorem 42.3.2 is `span_short_integralRamified_eq_top` (a) and `indexLe_normalizedPoincare` (b), with c_B, A_s and $S^{\mathrm{int}}_{\mathrm{ram}}$ the definitions `Data.invGainFactor`, `Data.normalizedPoincare` and `Data.integralRamified`. Input 1 is `Data.span_isShort_ramifiedSourceForms_eq_top`, the statement read for it is `Data.span_isShort_eq_top`, and Problem 42.3.1 is `IsShort.sub_translate`; input 3 is `normSqAt_goodProjTranslate_le` with `goodProjTranslate_mem_integralForms`, input 5 is `le_finrank_ramifiedSourceForms` with `f_div_N_sub_one_le`. The definitions of c_B and A_s use the witnesses `Data.divisibilityError` for err and `Data.seesawConst` for c_{ss}.

Hints

§42.1.

42.1.1: A 1×1 matrix u carries $1/6$ at p only if $v_p(u) \geq -v_p(1/6)$.

42.1.2: Write the matrix of the family as PDQ with P, Q invertible over $\mathbb{Z}_{(p)}$ and D diagonal.

42.1.3: Block diagonal matrices; Problem 42.1.2 for the examples.

42.1.4: Pull W back along $\mathbb{Z}^{\mathcal{J}}_{(p)} \to \mathbb{Z}^k_{(p)}$, $e_i \mapsto \varphi_i$, and take a basis of the preimage.

42.1.5: Choose preimages of the family in $\mathbb{Z}^k$. Which local matrices can act on these preimages?

§42.2.

42.2.1: How does multiplication by c_B change each coordinate valuation on W_p?

42.2.2: Problem 42.1.2.

42.2.3: The norm of $(1 - T_i)v$ is at most twice that of v.

§42.3.

42.3.1: z_w is an integral unit scalar: translation by it changes neither the gauges nor the set of values $\sigma\varphi(g)$. Then $|u - u'|^2 \leq 4\max(|u|^2, |u'|^2)$, and the gauge is ultrametric.

42.3.2: N splits completely in E and $[E : K] = f$. Problem 52.1.1: S_{ram} is the image of the product, so it is spanned by the images of a spanning set.

42.3.3: $-g_p \leq -\mathrm{gain}(p) + \mathrm{err}(p) + 1$, and $\mathrm{gain}(N) = 0$.

42.3.4: Which factors of c_B can have nonzero valuation at p? Compare with the support conditions on the gain and error.

42.3.5: Problem 42.3.3.

42.3.6: The seesaw at the trivial twist, Theorem 51.3.6 with $c = U$, the good part, and Problem 42.3.5.

42.3.7: Input 5.

42.3.8: Fix an m-fold twist of level prime to p. Compare the gauge bound from the seesaw and divisibility with the local absolute value of c_B, then use the good-part input.

42.3.9: As in Problem 42.1.5, with $\delta_p = D_X \mathrm{err}(p)$; then Problem 42.3.7.

References

[GL] L. Sernau, *GRH for Dirichlet L-functions, in Lean 4*, a shorter rewriting of the Lean proof, text by Claude, `https://github.com/lsernau/grh-lean`, commit `72fead1`, readable edition `grh/`.

[La] S. Lang, *Algebra*, 3rd ed., Grad. Texts in Math. 211, Springer, 2002.

THE SEESAW IDENTITY

Prerequisites. From Chapter 21: the lattices I_n over $\mathcal{O} = \mathbb{Z}[\mathrm{i}]$, the groups Γ_L, forms of weight (a) and their norm (Sections 21.1 and 21.3), and Problems 21.1.2 and 21.1.4. From Chapter 23: the lifts $\Theta_{(a)}$, the moments c_a, and Problems 23.1.4, 23.1.5, 23.2.1, 23.2.3, 23.2.4, 23.2.5, 23.4.2 and 23.5.1. From Chapter 36: the finite Poincaré map of Section 36.3, the Poincaré map $\mathcal{P}$, the maps A_s, and Theorem 36.4.2. From Chapter 33: the data and the spaces, forms and twists of Chapter 34, in the notation fixed there. Inner products of forms on definite lattices are linear in the first variable.

In the proof, Theorem A concerns lifts of the normalized translates A_s along the chain $Y_0 \to \cdots \to Y_m$, whose first space is indefinite, while the estimates of size and divisibility are proved along the chain $X_0 \to \cdots \to X_m$ of definite spaces. How does the proof pass between the chains? For each twist, the seesaw identity expresses the lift along the first chain of the Poincaré image of a ramified form φ as one nonzero constant times a combination of lifts of φ along the definite chain, restricted to Y_m. This chapter states the identity and deduces it from four theorems, proved in Chapters 44–47. We first study an analogue for one lift between lattices of ranks one and two.

43.1. A Poincaré map between definite lattices

We use the finite Poincaré map of Chapter 36, Section 36.3. Let $X := \mathcal{O}e_1$ and $Y := I_2 = X \perp \mathcal{O}e_2$ (in Section 23.4 the line X is called Y). By Problem 21.1.4 a form of weight (a) on I_n, $n \le 2$, is a single vector of $\mathrm{Sym}^a(\mathbb{C}^n)$ fixed by Γ_{I_n}, which we identify with the form; the inner product of forms is $\langle \psi, \psi' \rangle = |\Gamma_{I_n}|^{-1} \langle \psi, \psi' \rangle_{\mathrm{Sym}}$, with $\langle\,,\rangle_{\mathrm{Sym}}$ the inner product of $\mathrm{Sym}^a(\mathbb{C}^n)$. Let $0 \le j \le a$ be integers divisible by 4, and let $\varphi_j \in \mathcal{A}_{(j)}(1)$ be the form with value e_1^j. For $\varphi \in \mathcal{A}_{(j)}(1)$ let

$$P\varphi := \sum_{\gamma \in \Gamma_Y / \Gamma_{e_2}} \gamma \left(\varphi \, e_2^{a-j} \right) \in \mathcal{A}_{(a)}(2),$$

where Γ_{e_2} is the stabilizer of e_2; it is the map P of Chapter 36 with $\iota(\varphi) = \varphi \, e_2^{a-j}$. By Problem 36.2.1, $\langle \psi, P\varphi \rangle$ is the period $|\Gamma_X|^{-1} \langle \psi, \varphi \, e_2^{a-j} \rangle_{\mathrm{Sym}}$ of $\psi \in \mathcal{A}_{(a)}(2)$ along X, that of Section 23.4; and by Problem 36.3.2, $P\varphi_j = 4\big(e_1^j e_2^{a-j} + e_1^{a-j} e_2^j\big)$.

43.2. One lift

Now lift $P\varphi$ from Y to a lattice $L' = I_{n'}$, $n' \in \{1, 2\}$, with standard basis $e'_1, \ldots, e'_{n'}$; write $\mathcal{A}_{(d)}(L') := \mathcal{A}_{(d)}(n')$. For $x \colon Y \to L'$ write $x_k := x e_k$, and also view x_1 as the map $\mathbb{C}e_1 \to L'_{\mathbb{C}}$, $e_1 \mapsto x_1$. Put

$$\beta_{L'} := \sum_{v \in L'} v^{a-j} \, e^{-\pi h(v,v)} \in \mathrm{Sym}^{a-j}(L'_{\mathbb{C}}),$$

Date: November 26, 2026.

the vector obtained from the line $\mathcal{O}e_2$ alone. Products are taken in the symmetric algebra, as in Chapter 21.

Problem 43.2.1. For $x = (x_1, x_2)$ and $\varphi \in \mathrm{Sym}^j(\mathbb{C}e_1)$, $\mathrm{Sym}^a(x)(\varphi\, e_2^{a-j}) = \big(\mathrm{Sym}^j(x_1)\varphi\big)\, x_2^{a-j}$.

Problem 43.2.2. For $\varphi \in \mathcal{A}_{(j)}(1)$, with $\Theta_{(a)}\colon \mathcal{A}_{(a)}(2) \to \mathcal{A}_{(a)}(L')$ and $\Theta_{(j)}\colon \mathcal{A}_{(j)}(1) \to \mathcal{A}_{(j)}(L')$ the lifts of Chapter 23,

$$\Theta_{(a)}(P\varphi) = \big(\Theta_{(j)}\varphi\big)\, \beta_{L'}.$$

The right side lifts φ from the smaller space X, with the kernel multiplied by the fixed vector $\beta_{L'}$.

Problem 43.2.3. $\beta_{L'}$ is fixed by $\Gamma_{L'}$. For $L' = I_1$, $\beta_{I_1} = c_{a-j}\, {e_1'}^{a-j}$ and $\Theta_{(a)}(P\varphi_j) = \frac{1}{4} c_j c_{a-j}\, {e_1'}^{a}$, in agreement with Problem 23.2.5. For $L' = I_2$, $a = 8$ and $j = 4$,

$$\Theta_{(8)}(P\varphi_4) = \tfrac{1}{4} c_0^2 c_4^2 \big({e_1'}^8 + 2{e_1'}^4 {e_2'}^4 + {e_2'}^8\big).$$

Problem 43.2.4. For $\psi \in \mathcal{A}_{(a)}(L')$, let $\Theta'_{(a)}\psi \in \mathcal{A}_{(a)}(2)$ be its lift back to Y. Then

$$\big\langle \Theta'_{(a)}\psi,\ P\varphi \big\rangle = \big\langle \psi,\ (\Theta_{(j)}\varphi)\, \beta_{L'} \big\rangle.$$

For $L' = I_1$ this is Problem 23.4.2.

43.3. Chains, weighted sums, and translates of the vacuum

Problem 43.3.1. In this problem take $a = 8$ and $j = 4$. Let $\Theta^{(2)}$ be the composite $\mathcal{A}_{(8)}(2) \to \mathcal{A}_{(8)}(1) \to \mathcal{A}_{(8)}(2)$ of two lifts. Then $\Theta^{(2)} P\varphi_4 = \Theta_{(8)}\big((\Theta_{(4)}\varphi_4)\, \beta_{I_1}\big) = \frac{1}{16} c_4^2 \big(c_0 c_8\, {e_1'}^8 + 70\, c_4^2\, {e_1'}^4 {e_2'}^4 + c_0 c_8\, {e_2'}^8\big)$.

By Problem 23.5.1, the kernel of $\Theta^{(2)}$ is the sum over the middle classes of the products of the two weight-eight kernels, each divided by the order of the middle stabilizer. In general the data of a chain of lifts form a tensor, with one factor for each lift, and the seesaw produces a particular tensor.

The general proof pairs both sides with a form on Y_m and transfers the Bessel period along the lower chain one lift at a time (Chapter 44). The finite variables in the resulting outer integrals are summed over finite sets of cosets of a level, the cuts, with reciprocal multiplicities as weights (Chapter 46). Here is a finite model for those weights.

Problem 43.3.2. Let a finite group G_0 act on a finite set $\mathcal{X}$, let $\mathrm{Cut} \subset \mathcal{X}$ meet every orbit, and put $\mathrm{mult}(y) := \#\{\gamma \in G_0 : \gamma^{-1} y \in \mathrm{Cut}\}$. Then for every function $f\colon \mathcal{X} \to \mathbb{C}$,

$$\sum_{y \in \mathcal{X}} f(y) = \sum_{\gamma \in G_0} \sum_{c \in \mathrm{Cut}} \frac{f(\gamma c)}{\mathrm{mult}(\gamma c)}.$$

If f is G_0-invariant, the right side is $|G_0| \sum_{c \in \mathrm{Cut}} f(c)/\mathrm{mult}(c)$; if Cut has exactly one point in each orbit, then $\mathrm{mult}(c) = |\mathrm{Stab}_{G_0}(c)|$ for $c \in \mathrm{Cut}$. For $G_0 = (\mathbb{Z}/5)^\times$ acting on $\mathcal{X} = \mathbb{Z}/5$ by multiplication, $\mathrm{Cut} = \{0, 1, 2\}$ and $f = 1$, the multiplicities are $4, 2, 2$ and both sides equal 5.

In the proof the sums are formed for a tame character ξ (Definition 46.3.2), and each multiplicity that occurs divides a power of $\operatorname{Nm} Q_\xi$ (Problem 46.3.4).

The data for the definite chain in the seesaw are finite sums of tensors built from translates of the integral vacuum of each lift. In the simplest local model the vacuum is the characteristic function $\mathbf{1}_{\Lambda_0}$ of a lattice $\Lambda_0 \subset \mathbb{Q}_p^n$, and the elementary translation operators are the shifts $f(v) \mapsto f(v-x)$ and the multiplications $f(v) \mapsto \chi(v)f(v)$ by additive characters χ of $\mathbb{Q}_p^n$.

Problem 43.3.3. Let $\Lambda \subset \Lambda_0 \subset \mathbb{Q}_p^n$ be lattices with $[\Lambda_0 : \Lambda] = p^e$. Then $\mathbf{1}_{\Lambda_0} = \sum_{x \in \Lambda_0/\Lambda} \mathbf{1}_{x+\Lambda}$, and $\mathbf{1}_\Lambda = p^{-e} \sum_\chi \chi\, \mathbf{1}_{\Lambda_0}$, where χ runs over one extension to $\mathbb{Q}_p^n$ of each of the p^e characters of Λ_0/Λ. Hence the characteristic function of every lattice commensurable with Λ_0 is a combination of shifts of the products $\chi \mathbf{1}_{\Lambda_0}$ with coefficients in $\mathbb{Z}[1/p]$.

43.4. The seesaw identity

We use the field E, the levels $M = p_0 p_1$ and N, the elements π_M and π_N, the spaces X_j and Y_j, the source forms $S \supseteq S_{\mathrm{ram}}$, tame characters ξ and twists ϑ with their moduli Q, and the characters μ_j^0 of the lifts, as in Chapter 34. Put $\varrho := m/2 - 1$.

Definition 43.4.1 (the lower chain)**.** For $0 \le j \le m$ let $K_j^{Y\circ} := K^\circ(Y_j)$ be the standard lattice stabilizer of Y_j (Section 34.3) and, for a tame character ξ, $K_j^Y(\xi) \subseteq K_j^{Y\circ}$ its subgroup of elements that reduce to the identity at the places dividing π_M and at those in Q_ξ; K_M is the principal level of Y_0 (Section 34.4), so that $K_0^Y(\xi) \subseteq K_M \subseteq K_0^{Y\circ}$. Let $R_0 = \mathcal{U} \rtimes U(X_0)$ be the Bessel subgroup of Y_0 and $\psi_\mathcal{U}$ its character (Chapter 36). The Bessel function $\mathcal{W}_{\lambda,\varphi}$ of a source form φ formed with a linear form λ, and the Poincaré map $\mathcal{P}_{g,\lambda}\colon S \to H(Y_0)$ for a point g of the archimedean unitary group of Y_0, are those of Definition 36.2.1. With the Petersson product conjugate linear in the first variable, as in this chapter, the defining identity reads $\langle y, \mathcal{P}_{g,\lambda}\varphi\rangle = \int_{[R_0]} \mathcal{W}_{\lambda,\varphi}(r)\, \overline{y(r(g,1))}\, dr$. Let υ be the fixed splitting character restricted to the norm-one torus. For a tame character ξ and $1 \le j \le m$, *lift j of the lower chain*, $\Theta_{\xi,j}$, goes from forms on Y_{j-1} to forms on Y_j. Its Weil representation ω_j, of $U(Y_{j-1})(\mathbb{A}) \times U(Y_j)(\mathbb{A})$ on the data on $\operatorname{Hom}(Y_{j-1}, Y_j)$, uses on each of the two spaces, of rank n, the character $\mu_j^0 \xi^j \upsilon^{\lfloor n/2 \rfloor}$. Its datum $\phi_j(\xi)$ is the prescribed joint harmonic at infinity times the finite datum $\mathbf{1}_j(\xi)$, given at the places dividing π_M and at those in Q_ξ by the indicator of the reduction of the inclusion matrix and at the other finite places by the vacuum. The lift is the theta lift with this datum multiplied by the index $[K_{j-1}^{Y\circ} : K_{j-1}^Y(\xi)]$. The composite $\Theta_{\xi,m} \cdots \Theta_{\xi,1}$, followed by the passage to algebraic forms on Y_m, is the lower chain Θ_ξ of Chapter 34.

Definition 43.4.2 (the definite chain)**.** Let $\mathcal{T}$ be the set of tuples $\mathfrak{t} = (\mathfrak{t}_j)_{j \ge 0}$ of matrices $\mathfrak{t}_j$ of finite adeles of E, with rows indexed by the basis of X_{j+1} and columns by that of X_j. Write $\mathrm{Heis}(\cdot)$ for the finite Heisenberg operators on the finite data on $\operatorname{Hom}(X_j, X_{j+1})$. The *translated vacuum* $v_j(\mathfrak{t})$ is the integral vacuum of $\operatorname{Hom}(X_j, X_{j+1})$ (Section 34.8) translated by $\mathrm{Heis}(\mathfrak{t}_j)$. For a tame character ξ, $1 \le j \le m$ and a finite datum v on $\operatorname{Hom}(X_{j-1}, X_j)$, $\Theta_{\xi,j}^X(v)$ is lift j of the definite chain: the theta lift from the algebraic forms on X_{j-1} to those on X_j, of the weights of Definition 34.2.1, formed with the twist ξ, the prescribed harmonic at infinity and the finite datum v; it is linear in v, and lift j uses data on $\operatorname{Hom}(X_{j-1}, X_j)$, such

as $v_{j-1}(\mathfrak{t})$. For $j \geq 0$, ω_j^X is the finite Weil action of $U(X_j)(\mathbb{A}_f) \times U(X_{j+1})(\mathbb{A}_f)$ on these data for the twist ξ (written ω^X when the lift is clear), and K_j^X is the level of X_j: the integral finite adelic unitary matrices that reduce to the identity at every $w \in \mathcal{M}$ and have last row congruent to $(0, \dots, 0, 1)$ modulo π_N; K_0^X is the level of the source forms. A *pair tensor* for pair i ($0 \leq i \leq \varrho$) is a tensor of finite data on $\mathrm{Hom}(X_{2i}, X_{2i+1})$ and on $\mathrm{Hom}(X_{2i+1}, X_{2i+2})$. For pair tensors $\Phi_0, \dots, \Phi_\varrho$,

$$\Theta_\xi^X(\Phi_\varrho \otimes \cdots \otimes \Phi_0)$$

is the composite of the $\varrho + 1$ double lifts from S to forms on X_m, pair i acting through $v \otimes v' \mapsto \Theta^X_{\xi,2i+2}(v') \circ \Theta^X_{\xi,2i+1}(v)$, extended linearly; in a tensor over pairs, later pairs stand on the left.

Definition 43.4.3 (gluing, restriction, the composite lift)**.** For $0 \leq i \leq \varrho$ the *pair gluing* Gl_i, for the double lift $X_{2i} \to X_{2i+1} \to X_{2i+2}$, sums over the vectors y of residues modulo N, each represented in $\{0, \dots, N-1\}$, indexed by a basis of X_{2i+1} and the places $w \mid \pi_N$: it translates the first factor by the last column $-y/N$ supported at these places, and the second by the conjugate last row supported at their conjugates. The *glued vacuum tensor* of $\mathfrak{t} \in \mathcal{T}$ is $\mathrm{gl}(\mathfrak{t}) := \mathrm{gl}_{\varrho+1}(\mathfrak{t})$, where

$$\mathrm{gl}_0(\mathfrak{t}) := 1 \in \mathbb{C}, \qquad \mathrm{gl}_{i+1}(\mathfrak{t}) := \mathrm{Gl}_i\big(v_{2i}(\mathfrak{t}) \otimes v_{2i+1}(\mathfrak{t})\big) \otimes \mathrm{gl}_i(\mathfrak{t}) \quad (0 \leq i \leq \varrho),$$

and for a finitely supported $\Psi \colon \mathcal{T} \to \mathbb{C}$ the glued tensor is $\Psi^{\mathrm{gl}} := \sum_{\mathfrak{t}} \Psi(\mathfrak{t})\,\mathrm{gl}(\mathfrak{t})$. The *restriction* res takes an algebraic form on X_m to one on Y_m by evaluating at $\mathrm{diag}(h, 1)$, applying a fixed branching map, and multiplying by $b_N := \prod_\tau \Phi_\tau(\bar\pi_N)^{m\Delta/2-a_\tau}$, where Φ_τ is the embedding of the CM type at τ, and $a_\tau = a$ for $\tau \in \Phi_a$, $a_\tau = 0$ otherwise; the same letter is used for the corresponding map of automorphic forms. The *composite lift* is

$$B_{\vartheta,\Psi}(\varphi) := \mathrm{res}\,\Theta_\vartheta^X\big(\Psi^{\mathrm{gl}}\big)\varphi \qquad (\varphi \in S).$$

Definition 43.4.4 (chain data)**.** A finitely supported $\Psi \colon \mathcal{T} \to \mathbb{C}$ is a *chain datum* for the twist ϑ if: (i) for $\mathfrak{t}$ in the support of Ψ, every entry of every $\mathfrak{t}_j$ becomes integral, after multiplication by $\bar\pi_M$, at every finite place w not above a prime dividing $\mathrm{Nm}\,Q_\vartheta$, and vanishes at every w not above a prime dividing $M\,\mathrm{Nm}\,Q_\vartheta$; (ii) every value $\Psi(\mathfrak{t})$ lies in the ring $\mathcal{O}^{[\mathrm{Nm}\,Q_\vartheta]}$ of numbers integral away from $\mathrm{Nm}\,Q_\vartheta$ (Chapter 34); (iii) if $Q_\vartheta = \emptyset$, then $\sum_{\mathfrak{t}} |\sigma(\Psi(\mathfrak{t}))| \leq M^{3fmn_m^2}$ for every field automorphism σ of $\mathbb{C}$; (iv) Ψ^{gl} is fixed by $\bigotimes_j \omega_j^X(b_j, b_{j+1})$, formed for the twist ϑ, for all $b_j \in K_j^X$ ($j < m$) and $b_m = 1$.

Theorem 43.4.1 (the seesaw identity)**.** *Let D be admissible data, λ a linear form on the values of the source forms, and g a point of the archimedean unitary group of Y_0. There is $c \in \mathbb{C}^\times$ such that for every twist ϑ there is a finitely supported $\Psi \colon \mathcal{T} \to \mathbb{C}$ which is a chain datum for ϑ and satisfies*

$$\Theta_\vartheta\big(\mathcal{P}_{g,\lambda}\varphi\big) = c\,B_{\vartheta,\Psi}(\varphi) \qquad \textit{for every } \varphi \in S_{\mathrm{ram}}.$$

For fixed D, λ, g, one scalar c works for all twists, and for each twist one Ψ works for all $\varphi \in S_{\mathrm{ram}}$; the equality is one of algebraic forms on Y_m.

Chapters 44–47 prove Theorem 43.4.1, along the lines of Section 43.2. Both sides are paired with a form on Y_m, and the lifts of the lower chain are moved onto that form by transposition, as in Problem 43.2.4; Theorem 44.4.1 then carries the remaining Bessel period through one lift of the lower chain. Theorem 45.5.1 takes the transfers two at a time: after each pair, the function left on the definite group

is a coefficient of the definite chain with evaluated pair data. Theorem 46.4.1 sums the finite variables over the cuts, with weights as in Problem 43.3.2: there is $c' \in \mathbb{C}$, possibly zero, such that for every tame character ξ and every $\varphi \in S_{\mathrm{ram}}$

$$\Theta_{\xi,m} \cdots \Theta_{\xi,1} \mathcal{P}_{g,\lambda} \varphi = c' \operatorname{res} \Theta_{\xi}^{X}(\mathrm{ss}_{\xi}) \varphi,$$

an equality of automorphic forms on Y_m, with the seesaw tensor ss_{ξ} of Definition 46.4.3. Theorem 47.5.1 writes ss_{ξ} as a scalar c_{gl}, independent of ξ, times a sum of glued vacuum tensors $\mathrm{gl}(\mathfrak{t})$ whose coefficients become integral away from $\operatorname{Nm} Q_{\xi}$ after multiplication by $c_{\mathrm{res}}^{2m} = M^{2fmn_m^2}$. Passing to algebraic forms on Y_m, and applying the choice of u in Problem 43.5.4 to $c' c_{\mathrm{gl}} / c_{\mathrm{res}}^{2m}$, gives for each twist a chain datum (Problem 47.6.3) and the theorem's scalar $c = u^{-1}$.
In the Lean formalization. Theorem 43.4.1 is `Data.seesaw_identity` in the Lean proof [GL]; the objects of Definitions 43.4.1–43.4.4 are `Data.liftY`, `Data.lowerChain`, `Data.levelX`, `Data.Translations`, `Data.gluedTensor`, `Data.restrictToY`, `Data.compositeLift` and `Data.IsChainDatum`. The passage to algebraic forms is `lowerChain_eq_of_lowerChainUpTo_eq`, and the image formula for S_{ram} is `ramifiedSourceForms_eq_range`. The declarations of the four steps are named in Chapters 44–47.

43.5. Ramified forms, and what is not claimed

Where does the proof use the hypothesis that φ is ramified?

Problem 43.5.1. Let $n \geq 1$ be an integer and let F be a linear endomorphism of a finite-dimensional complex vector space V with $F^n = 1$. Then $\ker\bigl(\sum_{i=0}^{n-1} F^i\bigr) = \operatorname{im}(1 - F)$, the sum of the eigenspaces of F for eigenvalues $\neq 1$. For the cyclic shift on $\mathbb{C}^n$ this space has dimension $n - 1$.

Problem 43.5.2. Let $n \geq 1$ be an integer, and let $F_1, \ldots, F_l$ be commuting linear endomorphisms of a finite-dimensional complex vector space V with $F_k^n = 1$ for every k. Then $\bigcap_k \ker\bigl(\sum_{i=0}^{n-1} F_k^i\bigr) = \operatorname{im} \prod_k (1 - F_k)$.

So S_{ram} is the image of $\prod_{w|\pi_N} (1 - T_w)$.

Problem 43.5.3. In the situation of Problem 43.5.2, let $\Lambda \colon V \to V'$ be linear with $\Lambda F_k = \Lambda$ for one k. Then Λ vanishes on $\bigcap_k \ker\bigl(\sum_{i=0}^{n-1} F_k^i\bigr)$.

The proof uses Problem 43.5.3 for chains of lifts: if the Weil action of $(1, z_w)$ on one lift factor alone fixes the tensor of data of a chain, the chain annihilates S_{ram}. With the initial finite point in K_M, this vanishing gives the lattice bounds of Problem 46.2.16 at every stage $1 \leq j < m$; the finite Bessel orbit of a point where the stage function is nonzero therefore meets the cut of that stage (Definition 46.3.2).

Theorem 43.4.1 asserts that $c \neq 0$, but not that either side is nonzero, for any φ or any twist.

Problem 43.5.4. Let V, V' be complex vector spaces, $A, A' \colon V \to V'$ linear maps, and $c' \in \mathbb{C}$ such that $A = c' A'$. Put $u := c'^{-1}$ if $c' \neq 0$ and $u := 1$ otherwise. Then $u \neq 0$ and $A = u^{-1}(u c' A')$, and $u c' A' = 0$ if and only if $c' = 0$ or $A' = 0$.

Problem 43.5.5. For $\lambda = 0$, Theorem 43.4.1 holds with $c = 1$ and $\Psi = 0$ for every twist: $\mathcal{P}_{g,0} = 0$, the function $\Psi = 0$ is a chain datum, and $B_{\vartheta,0} = 0$.

By Theorem 36.4.2 some A_s is nonzero on S_{ram}, so $\mathcal{P}$ is not zero there; Theorem B gives no nonvanishing after the lower chain.

Hints

§43.2.

43.2.1: $e_1^j e_2^{a-j}$ is the symmetrization of $e_1^{\otimes j} \otimes e_2^{\otimes(a-j)}$, and $\mathrm{Sym}^a(x)$ is the restriction of $x^{\otimes a}$.

43.2.2: Problems 23.1.4 and 43.2.1; $h(x,x) = h(x_1,x_1)+h(x_2,x_2)$, and $\Gamma_{e_2} = \{\mathrm{diag}(u,1) : u \in \mu_4\}$ has the order of Γ_X.

43.2.3: Substitute $v \mapsto \gamma v$. For the values use Problems 23.2.3, 23.2.4 and 23.2.1, and $c_k = 0$ for $4 \nmid k$.

43.2.4: Problems 23.1.5 and 43.2.2.

§43.3.

43.3.1: Apply the second lift to both sides of Problem 43.2.2; then Problems 43.2.3 and 23.2.4.

43.3.2: Exchange the two sums on the right and group by $y = \gamma c$.

43.3.3: Orthogonality of the characters of the finite group Λ_0/Λ. Characters of Λ_0 extend to $\mathbb{Q}_p^n$. For a general lattice Λ', use $\Lambda_0 \cap \Lambda'$.

§43.5.

43.5.1: F is diagonalizable; for Problem 43.5.2 use simultaneous eigenspaces.

43.5.5: The composite lift is linear in the glued tensor.

References

[GL] L. Sernau, *GRH for Dirichlet L-functions, in Lean 4*, a shorter rewriting of the Lean proof, text by Claude, `https://github.com/lsernau/grh-lean`, commit `72fead1`, readable edition `grh/`.

TRANSFERRING A BESSEL PERIOD THROUGH A THETA LIFT

Prerequisites. Hermitian forms over fields; Witt's extension theorem [Sch]. From Chapter 36: the Bessel subgroup $R = \mathcal{U} \rtimes U(X)$ and an example of its character (Section 36.1, Problems 36.1.1 and 36.1.2), and the finite unfolding of Problem 36.2.1. From Chapter 10: the unfolding of Problem 10.1.1. From Chapter 23: Problem 23.1.5 and Section 23.4. From Chapter 43: Theorem 43.4.1 and Problem 43.2.4. The Weil representation of a unitary dual pair and the Heisenberg representation under it, at the level of their definitions [We], [Ku, §1]. Matrices act on columns; the matrix of a map $V \to V'$ has its rows indexed by the basis of V'. In this sheet b, d, s are local letters (not the scale, the prime and the tower exponent).

The proof of Theorem 43.4.1 pairs both sides with a form on the last space of the lower chain and moves the lifts onto that form by transposition, as in Problem 43.2.4; what is left is a Bessel period of a theta function, integrated against the form. How does such a period pass through one theta lift? For the weights 0, the theta function expands in constant terms indexed by the classes of rational maps $V \to V'$ modulo maps of degree ≥ 0 (Section 44.2). In the period against a Bessel function only the $U(V')(F)$-translates of the set of classes agreeing with the string map contribute; the rational Bessel subgroup of the second space preserves this set, and each translate contributes one value of the transferred function. We first see the mechanism over $\mathbb{F}_3$ and $\mathbb{F}_9$.

44.1. Theta against a character on a plane over $\mathbb{F}_3$

Let $Q(v) = v_1^2 + v_2^2$ on $\mathbb{F}_3^2$, let $\zeta_3 := e^{2\pi \mathrm{i}/3}$, and for a function $\phi\colon \mathbb{F}_3^2 \to \mathbb{C}$ and $b \in \mathbb{F}_3$ put $(n(b)\phi)(v) := \zeta_3^{bQ(v)}\phi(v)$ and $\theta(\phi) := \sum_v \phi(v)$. The operators $n(b)$ commute with $(h\phi)(v) := \phi(h^{-1}v)$ for h in the orthogonal group $O(Q)$. In this section $\phi(v) := 1 + [v_1] + 2[v_2]$, with $[\,\cdot\,] \in \{0,1,2\}$ the least residue.

Problem 44.1.1. The sums $\sum_{Q(v)=1+j} \phi(v)$ are 13, 22, 1 for $j = 0, 1, 2$.

Problem 44.1.2. For every ϕ, $\frac{1}{3}\sum_{b\in\mathbb{F}_3} \zeta_3^{-b}\,\theta(n(b)\phi) = \sum_{Q(v)=1} \phi(v)$. For the ϕ above it is 13.

The left side is a period of $b \mapsto \theta(n(b)\phi)$ against a character; only the v with $Q(v) = 1$ survive it.

Problem 44.1.3. $O(Q)$ has 8 elements, the stabilizer of $v_0 := (1, 0)$ has 2, and the orbit of v_0 is $\{(\pm 1, 0), (0, \pm 1)\} = \{Q = 1\}$.

Problem 44.1.4. Let $\mathrm{cf}(\phi)$ be the coefficient of Problem 44.1.2 and Stab the stabilizer of v_0. For $h \in O(Q)$, $\mathrm{cf}(h\phi) = \sum_{q \in O(Q)/\,\mathrm{Stab}} \phi(h^{-1}qv_0)$; for $h = 1$ this is

Date: November 26, 2026.

$\frac12\sum_{\gamma\in O(Q)}\phi(\gamma v_0)=13$. For every function z on $O(Q)$,

$$\sum_{h\in O(Q)} z(h)\,\mathrm{cf}(h\phi)=\sum_{h\in O(Q)}\Big(\frac{1}{|\mathrm{Stab}|}\sum_{\gamma\in O(Q)} z(\gamma h)\Big)\phi(h^{-1}v_0).$$

This period is the finite model of the transfer: a sum over $O(Q)/\operatorname{Stab}$ of one function $h\mapsto\phi(h^{-1}v_0)$, evaluated at $q^{-1}h$. In the adelic period the unipotent group can be nonabelian, and the proof uses two choices of weights.

44.2. Strings, grades and the string map

For the matrix definitions and the finite examples, let E be a field with an involution $x\mapsto\bar x$ and fixed field F, and let $N\in F^\times$; all bases are finite.

Definition 44.2.1. A *space with a string* for N is a hermitian space V over E with a basis consisting of an orthonormal basis of a subspace X and vectors $f_0,\dots,f_{s-1}$ orthogonal to X, and with a constant $c_V\in F^\times$, such that f_i pairs only with f_{s-1-i}, to 1, or to $-N$ if $i=s-1-i$. We write J_V for the Gram matrix. X is the *definite part*, $f_0,\dots,f_{s-1}$ is the *string*, and $\operatorname{len}V:=s$ is its *length*.

Definition 44.2.2. The *grade* of a vector of the basis of X is 0, and that of f_i is $s-1-2i$. Let V' be a second space with a string, and let d be integer weights on the basis of V'. For basis vectors e of V and e' of V', the entry of a map $w\colon V\to V'$ in the row of e' and the column of e has *degree* $d(e')-\operatorname{grade}(e)$, and w has degree $\ge i$ if all its entries of degree $<i$ vanish. For maps $V\to V$ the weights are the grades.

For the shape of Section 36.1 the string is $v_1,\dots,v_\varrho,z,v'_\varrho,\dots,v'_1$; $\mathcal U$ is the group of unitary n with $n-1$ raising grades, and R that of the unitary g with gf_i-f_i in the span of the string vectors of larger grade for every f_i of grade ≥0. In the proof these descriptions define $\mathcal U$ and R for every space with a string.

Definition 44.2.3. Let $\operatorname{len}V'=\operatorname{len}V-1$, or $\operatorname{len}V=\operatorname{len}V'=0$. The *string map* $\mathrm{st}\colon V\to V'$ kills the definite part and sends f_i to f'_i times a scalar, and to 0 if V' has no vector f'_i. If $\operatorname{len}V$ is odd, the scalar is 1, $-Nc_V$, c_V for f_i of positive, zero, negative grade; if $\operatorname{len}V$ is even, it is c_V, 1 for positive, negative grade. For a map $w\colon V\to V'$ put $w^*:=J_V^{-1}\bar w^tJ_{V'}$.

For the grades of V and V' the string map has degree ≥-1; in the chain of the data it is $\mathrm{st}_j\colon Y_{j-1}\to Y_j$.

The hook. In the finite examples of this section and the next, $E=\mathbb F_9=\mathbb F_3[\mathrm i]$ with $\mathrm i^2=-1$ and $\bar{\mathrm i}=-\mathrm i$, $N=1$, and V, V' have no definite part, strings of lengths 3 and 2, and constants $c_V=c_{V'}=1$: $J_V=\operatorname{antidiag}(1,-1,1)$, $J_{V'}=\operatorname{antidiag}(1,1)$, the grades are $2,0,-2$ on V and $1,-1$ on V', and $\mathrm{st}=\left(\begin{smallmatrix}1&0&0\\0&-1&0\end{smallmatrix}\right)$.

Problem 44.2.1. The unitary upper unitriangular matrices for J_V are the 27 matrices $u=\left(\begin{smallmatrix}1&a&b\\0&1&\bar a\\0&0&1\end{smallmatrix}\right)$ with $b+\bar b=a\bar a$. They form $\mathcal U$, and $u-1$ has degree ≥2 for each of them.

Problem 44.2.2. $\operatorname{tr}(\mathrm{st}^*\mathrm{st}\,u)=a-\bar a$, and for $w=(v,0,0)$ with first column $v\in\mathbb F_9^2$, $\operatorname{tr}(w^*wu)=(\bar v^tJ_{V'}v)\,b$.

44.3. The survival test

Over the adeles, let E be a CM field with the CM type and Weil data of [GL], F its maximal totally real subfield and $\mathbb{A}_E$ its adeles; ψ_E is the standard additive character of $\mathbb{A}_E/E$, and $j_E \in E^\times$, with $\bar{j}_E = -j_E$, is the element given by the Weil data. In the proof the character used on the unitary n with $n-1$ of degree ≥ 2 is $\psi_{\mathcal{U}}(n) = \psi_E\big(\frac{1}{2} j_E \operatorname{tr}(\mathrm{st}^*\mathrm{st}\, n)\big)$; the matrix $\mathrm{st}^*\mathrm{st}$ is the shift of the string of V and depends on c_V, and $\psi_{\mathcal{U}}(nn') = \psi_{\mathcal{U}}(n)\psi_{\mathcal{U}}(n')$ for two such n, n'. Over $\mathbb{F}_9$ we use the same formulas with $\psi_E(x) = \zeta_3^{\operatorname{Tr}_{\mathbb{F}_9/\mathbb{F}_3} x}$ and $j_E = \mathrm{i}$ (and $\frac{1}{2} = -1$ in $\mathbb{F}_3$), and u runs over $\mathcal{U}(\mathbb{F}_3)$.

Definition 44.3.1. Let d be weights on the basis of V'. A rational map $w\colon V \to V'$ *survives* for d if

$$\psi_E\big(\tfrac{1}{2} j_E \operatorname{tr}(\mathrm{st}^*\mathrm{st}\, u)\big) = \psi_E\big(\tfrac{1}{2} j_E \operatorname{tr}(w^* w\, u)\big)$$

for every $u \in \mathcal{U}(\mathbb{A}_F)$ such that $u-1$ has degree ≥ 2 and $w(u-1)$ has degree ≥ 1 for the weights d. A map w *agrees with* st if w and st have the same entry in the row of e' and the column of e whenever $\operatorname{grade}(e) > 0$ and $\operatorname{grade}(e') < \operatorname{grade}(e)$.

The test is applied to classes of rational maps modulo the maps of degree ≥ 0, through a chosen representative of each class; a class is determined by the entries of negative degree. For the weights 0 these are the columns of positive grade.

Problem 44.3.1. In the hook, take the weights $(0,0)$. The classes are represented by the 81 maps $w = (v, 0, 0)$, and exactly 32 of them survive: the $v \neq 0$ with $\bar{v}^t J_{V'} v = 0$.

Problem 44.3.2. The unitary group $U(V')(\mathbb{F}_3) = \{g \in \mathrm{GL}_2(\mathbb{F}_9) : \bar{g}^t J_{V'} g = J_{V'}\}$ has 96 elements, and their first columns are the 32 surviving vectors of Problem 44.3.1. The stabilizer of $(1,0)^t$ has order 3 and is the Bessel subgroup R' of V'.

Problem 44.3.3. Take the weights $(1,-1)$, the grades of V'. The classes that agree with st are represented by the nine maps $\left(\begin{smallmatrix} 1 & 0 & 0 \\ 0 & c & 0 \end{smallmatrix}\right)$, $c \in \mathbb{F}_9$, and exactly $c = -1$ survives: the class of st.

The hook illustrates the two choices of weights in the proof. For the weights 0 the survivors are the translates by $U(V')(\mathbb{F}_3)$ of the one class that agrees with st, $v = (1,0)^t$, in bijection with $U(V')(\mathbb{F}_3)/R'$ ($96/3 = 32$); for the grades of V' only the class of st survives among the agreeing classes. Here is a finite model of how a failing map is killed.

Problem 44.3.4. Let H be a finite group and $\mathfrak{f}\colon H \to \mathbb{C}$ a function with $\mathfrak{f}(ux) = \zeta\mathfrak{f}(x)$ for all x, for one $u \in H$ and one $\zeta \neq 1$. Then $\sum_{x \in H} \mathfrak{f}(x) = 0$. If $\mathfrak{f}$ is also left invariant under a subgroup S, then $\sum_{x \in S\backslash H} \mathfrak{f}(x) = 0$.

44.4. Constant terms and the transfer

Let V, V' be spaces with strings for the same N over E, with $\operatorname{len} V' = \operatorname{len} V - 1$ or $\operatorname{len} V = \operatorname{len} V' = 0$, each with an adelic frame in which its Gram matrix is the same diagonal matrix of signs at every infinite place and the identity at the finite places; matrices are written in the bases of Definition 44.2.1. Let R, R' be the Bessel subgroups. Write $\mathbb{A} = \mathbb{A}_F$ for the groups and $\mathbb{A}_E$ for the matrices. Put $[R] := R(F)\backslash R(\mathbb{A})$ and $[U(V')] := U(V')(F)\backslash U(V')(\mathbb{A})$, with the quotient

measures of fixed Haar measures; $[R]$ is compact. Let $\mathbb{W} := \mathrm{Hom}(V, V')$, with the pairing $(y, y') \mapsto \mathrm{tr}(y'^{*}y)$. For each finite index set fix a continuous unitary character of the norm-one adeles of E trivial on the norm-one elements of E; for the index sets of the bases of V and V' these give the Weil representation ω of $U(V)(\mathbb{A})\times U(V')(\mathbb{A})$ on the Banach space $\mathcal{S}$ of data of [GL] (see [We], [Ku, §1]), with the Heisenberg operators $\mathrm{Heis}(y)$, $y \in \mathbb{W}(\mathbb{A}_E)$, and the theta functional $\theta\colon \mathcal{S} \to \mathbb{C}$. We use: $\omega(g,h)\mathrm{Heis}(y)\omega(g,h)^{-1} = \mathrm{Heis}(hyg^{-1})$; $\theta \circ \omega(\gamma, \gamma') = \theta$ for rational γ, γ'; $y \mapsto \theta(\mathrm{Heis}(y)\phi)$ is invariant under rational translations on every rational subspace of $\mathbb{W}$ on which the pairing vanishes. *Status*: classical.

Let d be weights on the basis of V' that change sign under the involution of the basis fixing the definite part and exchanging f'_i and $f'_{s'-1-i}$ ($s' = \mathrm{len}\, V'$), for instance $d = 0$ or the grading, and let $\mathbb{W}^d_{>0}$ be the maps whose entries of degree ≤ 0 vanish. The pairing vanishes on $\mathbb{W}^d_{>0}$. A map $V' \to V'$ has degree ≥ 0 for d if its entry in the row of e' and column of e'' vanishes whenever $d(e') < d(e'')$.

Definition 44.4.1. For a datum ϕ and a map $w \in \mathbb{W}(\mathbb{A}_E)$, the *constant term* of ϕ at w is the mean

$$\mathrm{CT}^d_w(\phi) := \int_{\mathbb{W}^d_{>0}(E)\backslash\mathbb{W}^d_{>0}(\mathbb{A}_E)} \theta\big(\mathrm{Heis}(y)\mathrm{Heis}(w)\phi\big)\, dy$$

for the probability Haar measure. We write $\mathrm{CT}_w := \mathrm{CT}^d_w$ when d is the grading of V'.

In the proof, for rational w, CT^d_w depends only on w modulo rational maps of degree ≥ 0. For the fixed spaces and weights d there is a constant $C_d \geq 0$ such that for every datum ϕ,

$$\theta(\phi) = \sum_w \mathrm{CT}^d_w(\phi), \qquad \sum_w |\mathrm{CT}^d_w(\phi)| \leq C_d \|\phi\|,$$

the sums over the classes of rational maps modulo maps of degree ≥ 0, with the norm of $\mathcal{S}$. This is the Fourier expansion along $\mathbb{W}^d_{>0}$ in a mixed model; compare [We]. *Status*: classical; the norm estimate is used in the form proved in the argument.

Definition 44.4.2. Let $\phi \in \mathcal{S}$, and let $\mathcal{W}$ be a continuous function on $R(\mathbb{A})$, left invariant under $R(F)$, with $\mathcal{W}(nr) = \psi_{\mathcal{U}}(n)\mathcal{W}(r)$ for all $n \in R(\mathbb{A})$ such that $n - 1$ has degree ≥ 2. The *transfer* of $\mathcal{W}$ is the function on $U(V')(\mathbb{A})$

$$\mathcal{W}'(h) := \int_{[R]} \mathcal{W}(r)\, \mathrm{CT}_{\mathrm{st}}\big(\omega(r,h)\phi\big)\, dr.$$

In the proof $\mathcal{W}'$ is continuous and left $R'(F)$-invariant. For each class w choose a rational representative $\tilde{w}$, and put $\mathcal{Q}^d_w(h,r) := \mathcal{W}(r)\, \mathrm{CT}^d_{\tilde{w}}(\omega(r,h)\phi)$; a class survives, or agrees with st, if $\tilde{w}$ does. In the proof, each $\mathcal{Q}^d_w$ is jointly continuous in (h,r), and for fixed h $\sum_w |\mathcal{Q}^d_w(h,r)|$ is bounded in r; and if $u \in R(\mathbb{A})$, $u - 1$ has degree ≥ 2 and $\tilde{w}(u-1)$ has degree ≥ 1, then

$$\mathcal{Q}^d_w(h, ur) = \frac{\psi_E\big(\frac{1}{2} j_E\, \mathrm{tr}(\mathrm{st}^*\mathrm{st}\, u)\big)}{\psi_E\big(\frac{1}{2} j_E\, \mathrm{tr}(\tilde{w}^*\tilde{w}\, u)\big)}\, \mathcal{Q}^d_w(h,r).$$

The ratio is 1 for all such u exactly when $\tilde{w}$ survives.

Problem 44.4.1. Let $\gamma \in R(F)$ and $\gamma' \in U(V')(F)$, and let γ' have degree ≥ 0 for the weights d (no condition when $d = 0$). Then $\mathcal{Q}^d_{\gamma' w \gamma^{-1}}(\gamma' h, \gamma r) = \mathcal{Q}^d_w(h, r)$.

We use special cases of two facts on discrete groups. Let G be a second-countable locally compact Hausdorff group with a left Haar measure, $\Gamma \subset G$ a discrete subgroup acting on a countable set $\mathcal{X}$, quotients by discrete subgroups carrying the induced measures, and $\mathfrak{k}_{\mathfrak{x}}$ ($\mathfrak{x} \in \mathcal{X}$) measurable functions on G with $\mathfrak{k}_{\gamma\mathfrak{x}}(\gamma g) = \mathfrak{k}_{\mathfrak{x}}(g)$. If $\sum_{\mathfrak{x}} |\mathfrak{k}_{\mathfrak{x}}|$ is integrable on $\Gamma\backslash G$, then $\mathfrak{k}_{\mathfrak{x}}$ is integrable on $\mathrm{Stab}_\Gamma(\mathfrak{x})\backslash G$ and $\int_{\Gamma\backslash G} \sum_{\mathfrak{x}' \in \Gamma\mathfrak{x}} \mathfrak{k}_{\mathfrak{x}'} = \int_{\mathrm{Stab}_\Gamma(\mathfrak{x})\backslash G} \mathfrak{k}_{\mathfrak{x}}$ [Bou]. And if $\mathfrak{f}$ is continuous, integrable on $\Gamma\backslash G$ and left Γ-invariant, with $\mathfrak{f}(ug) = \zeta\mathfrak{f}(g)$ for all g, one $u \in G$ and one $\zeta \neq 1$ of modulus one, then $\int_{\Gamma\backslash G} \mathfrak{f} = 0$; Problem 44.3.4 is the finite case. *Status*: the first is classical; the second is elementary, and is used in the form proved in the argument.

Problem 44.4.2. Let d be 0 or the grading of V', and let the class w fail the test for d. Then for every h, $\int_{[R]} \sum_{w' \in wR(F)} \mathcal{Q}^d_{w'}(h, r)\, dr = 0$.

Let w_+ and st_+ be the matrices of the columns of positive grade of w and of st. In the proof, if a rational w survives for $d = 0$, then w_+ has linearly independent columns and $\bar{w}^t_+ J_{V'} w_+ = \bar{\mathrm{st}}^t_+ J_{V'} \mathrm{st}_+$; Problem 44.3.1 illustrates this. Witt's theorem: if w_1, w_2 are matrices over E of the same shape, with linearly independent columns and $\bar{w}^t_1 J w_1 = \bar{w}^t_2 J w_2$ for a nondegenerate hermitian J, then $g w_1 = w_2$ for some invertible square g over E with $\bar{g}^t J g = J$ [Sch]. *Status*: classical.

Problem 44.4.3. Let w be a rational map with w_+ of linearly independent columns and $\bar{w}^t_+ J_{V'} w_+ = \bar{\mathrm{st}}^t_+ J_{V'} \mathrm{st}_+$. Then $\gamma' w$ agrees with st for some $\gamma' \in U(V')(F)$.

Let $\mathcal{C}$ be the set of classes for the weights 0 that agree with st. In the proof, if w agrees with st, $\gamma \in R(\mathbb{A})$ and $\gamma' \in U(V')(\mathbb{A})$, then $\gamma' w \gamma$ agrees with st if and only if $\gamma' \in R'(\mathbb{A})$; in particular $\mathcal{C}$ is stable under $w \mapsto w\gamma$, $\gamma \in R(F)$. Problem 44.3.2 illustrates this.

Problem 44.4.4. Let a group H act on a set $\mathcal{X}$, let $S \subseteq H$ be a subgroup and $\mathcal{C} \subseteq \mathcal{X}$ a subset such that for $\mathfrak{x} \in \mathcal{C}$, $g\mathfrak{x} \in \mathcal{C}$ if and only if $g \in S$. Then $(q, \mathfrak{x}) \mapsto q_{\mathrm{rep}}\mathfrak{x}$, for any choice of representatives q_{rep}, is a bijection from $(H/S) \times \mathcal{C}$ onto the union of the translates of $\mathcal{C}$.

The second selection takes place inside the period: in the proof, for every h,

$$\int_{[R]} \sum_{w \in \mathcal{C}} \mathcal{Q}^0_w(h, r)\, dr = \mathcal{W}'(h).$$

For each datum, the sum of the constant terms over $\mathcal{C}$ equals the sum over the classes agreeing with st for the grading of V'; every surviving representative of one of those lies in the class of st; st survives, and $R(F)$ fixes its class. Problem 44.3.3 illustrates this.

Problem 44.4.5. For every $h \in U(V')(\mathbb{A})$, the series on the right converges absolutely and

$$\int_{[R]} \mathcal{W}(r)\, \theta\big(\omega(r, h)\phi\big)\, dr = \sum_{q \in U(V')(F)/R'(F)} \mathcal{W}'(q^{-1}_{\mathrm{rep}} h).$$

Problem 44.4.6. Let $\Gamma' \subseteq \Gamma$ be discrete subgroups of G as above, $\mathfrak{f}$ a continuous left Γ'-invariant function and z a continuous left Γ-invariant function on G, with $\sum_{q\in\Gamma/\Gamma'}|\mathfrak{f}(q_{\mathrm{rep}}^{-1}h)z(h)|$ integrable on $\Gamma\backslash G$. Then $\mathfrak{f}z$ is integrable on $\Gamma'\backslash G$ and

$$\int_{\Gamma\backslash G}\sum_{q\in\Gamma/\Gamma'}\big(\mathfrak{f}(q_{\mathrm{rep}}^{-1}h)\,z(h)\big)\,dh=\int_{\Gamma'\backslash G}\mathfrak{f}(h)z(h)\,dh.$$

The height of $h\in U(V')(\mathbb{A})$ is the reciprocal of the first minimum, cut off at 1, of the lattice of the space moved by h. In the proof, for every g_0 and every large integer e, each h has a $\gamma'\in U(V')(F)$ with $\|\omega(g_0,\gamma'h)\|\le 2^e$ times the e-th power of the height of h; we use $g_0=1$. This growth estimate is proved by reduction theory; compare [KR]. A function z on $U(V')(\mathbb{A})$ is *automorphic* if it is continuous, left invariant under $U(V')(F)$ and invariant under right translation by a neighbourhood of 1 in the finite adelic group, and *rapidly decreasing* if for every integer $b\ge 0$, $|z(h)|$ times the b-th power of the height of h is bounded. For each rapidly decreasing z, in the proof, $\sum_{w\in\Sigma}|\mathcal{Q}_w^0(h,r)z(h)|\le C'$ for one constant C', every h, r and every set Σ of classes, and $\sum_q|\mathcal{W}'(q_{\mathrm{rep}}^{-1}h)z(h)|\le C'\,\mathrm{vol}[R]$, and $[U(V')]$ has finite volume. Problems 44.4.1–44.4.6, with the facts stated in this section, prove the following.

Theorem 44.4.1. *With E, the frames, ω and $\mathcal{S}$ as in this section, let V, V' be hermitian spaces over E, each the orthogonal sum of a definite part and a string for the same N, with* $\operatorname{len}V'=\operatorname{len}V-1$ *or* $\operatorname{len}V=\operatorname{len}V'=0$*; let R, R' be their Bessel subgroups and* st *the string map. Let $\phi\in\mathcal{S}$, $\mathcal{W}$ be as in Definition 44.4.2, and z be an automorphic, rapidly decreasing function on $U(V')(\mathbb{A})$. Then $\mathcal{W}'z$ is integrable on $R'(F)\backslash U(V')(\mathbb{A})$ and*

$$\int_{[R]}\mathcal{W}(r)\int_{[U(V')]}\theta\big(\omega(r,h)\phi\big)\,z(h)\,dh\,dr=\int_{R'(F)\backslash U(V')(\mathbb{A})}\mathcal{W}'(h)\,z(h)\,dh.$$

What has been proved. A Bessel period of a theta function, paired with a form on V', is the integral of the transfer against the form over $R'(F)\backslash U(V')(\mathbb{A})$. Used as given: the facts on ω, Heis and θ stated at the start of Section 44.4, the expansion of θ, the statements marked "in the proof", Witt's theorem and the facts on discrete groups. If $c_V=c_{V'}$, then in the proof, for each h, the function $r'\mapsto\mathcal{W}'(r'h)$ on $R'(\mathbb{A})$ satisfies the hypothesis on $\mathcal{W}$ for V': the transfer is again a Bessel function, on a string of length $\max(\operatorname{len}V-1,0)$. Along the lower chain $Y_0,\dots,Y_m$ the string of Y_j has length $m-1-j$ for $j<m$, and that of Y_m has length 0.

In the Lean formalization. Theorem 44.4.1 is `New.Grading.integral_besselGroup_unfold` in the Lean proof [GL]. The adelic definitions specialize `New.Grading`, `stringMap`, `constTerm`, `unfoldStep`, `Survives` and `HasDegreeGe`; the finite examples use the same matrix formulas. The expansion of θ is `hasSum_constTerm`, the matrix form of Witt's theorem is `New.witt`, and the growth estimate is `eventually_exists_norm_omega_le_mul_height_pow`. The statements marked "in the proof" are at these places of [GL], commit `72fead1`: the descriptions of $\mathcal{U}$ and R, compactness of $[R]$, the character $\psi_{\mathcal{U}}$ and st*st, the degree of st, class independence of CT_w^d, continuity and invariance of $\mathcal{W}'$, the terms $\mathcal{Q}_w^d$ and their phase law, the Gram condition, preservation of agreement, the second selection, the two estimates and the finite volume, the case $c_V=c_{V'}$, the chain gradings, the transposition, the orbit fact and the twisted integral.

Hints

§44.1.

44.1.2: Exchange the two sums and use $\sum_b \zeta_3^{b(Q(v)-1)}$.

44.1.3: -1 is not a square in $\mathbb{F}_3$, so Q is anisotropic.

44.1.4: Problems 44.1.2 and 44.1.3; substitute $h \mapsto \gamma h$, as in Problem 36.2.1.

§44.2.

44.2.1: Expand $\bar{u}^t J_V u = J_V$ entry by entry.

44.2.2: Compute the shift $\mathrm{st}^*\mathrm{st}$ on the string basis.

§44.3.

44.3.1: Which u are admissible for $v = 0$, and which for $v \neq 0$? Then Problem 44.2.2.

44.3.2: Count first, then second columns. The Bessel subgroup of a string of length two fixes f_0'.

44.3.3: Compare the entries used for agreement with those of negative degree; then compute the two phases.

§44.4.

44.4.1: Move $\omega(\gamma, \gamma')$ to the left through the Heisenberg operators, then substitute $y \mapsto \gamma' y \gamma^{-1}$ in the mean. An element of $R(\mathbb{A})$ preserves the span of the basis vectors of grade $\geq i$ for each i, so it does not lower grades (use unitarity for the grades < 0 and for the definite part).

44.4.2: Unfold the orbit with $\Gamma = R(F)$ and Problem 44.4.1; on the stabilizer quotient use the vanishing of twisted integrals.

44.4.3: Witt's theorem in V', for the columns of positive grade.

44.4.5: Expand θ for the weights 0, and sort the classes into the translates of $\mathcal{C}$ and the rest.

44.4.6: The orbit fact for Γ acting on Γ/Γ'; compare Problem 10.1.1.

References

[Bou] N. Bourbaki, *Intégration*, Chapitres 7 et 8, Hermann, Paris, 1963.

[GL] L. Sernau, *GRH for Dirichlet L-functions, in Lean 4*, a shorter rewriting of the Lean proof, text by Claude, `https://github.com/lsernau/grh-lean`, commit `72fead1`, readable edition `grh/`.

[KR] S. S. Kudla and S. Rallis, *A regularized Siegel–Weil formula: the first term identity*, Ann. of Math. **140** (1994), 1–80.

[Ku] S. S. Kudla, *Splitting metaplectic covers of dual reductive pairs*, Israel J. Math. **87** (1994), 361–401.

[Sch] W. Scharlau, *Quadratic and Hermitian Forms*, Grundlehren Math. Wiss. 270, Springer, 1985.

[We] A. Weil, *Sur certains groupes d'opérateurs unitaires*, Acta Math. **111** (1964), 143–211.

TWO LIFTS AT A TIME

Prerequisites. Chapter 44: spaces with a string, grades and degrees, string maps, constant terms, the transfer (Definitions 44.2.1–44.4.2), the Bessel groups $R = \mathcal{U} \rtimes U(X)$, ψ_E, j_E, $\psi_{\mathcal{U}}$, and Theorem 44.4.1, in its notation. Chapter 43, Definitions 43.4.1 and 43.4.2: the Bessel function $\mathcal{W}_{\lambda,\varphi}$; lift j of the lower chain $\Theta_{\xi,j}$, its Weil representation ω_j, its datum $\phi_j(\xi)$ (a harmonic at infinity times the finite datum $\mathbf{1}_j(\xi)$), the levels $K_j^Y(\xi) \subseteq K_j^{Y\circ}$; Heisenberg translations Heis; the definite lifts $\Theta^X_{\xi,j}(v)$. Chapter 23: Problems 23.2.3, 23.4.1, 23.5.1. Chapters 33, 34: X_j, Y_j, $\varrho = m/2 - 1$, tame characters (of weight zero), Problem 33.5.2.

In the proof of the seesaw identity (Chapter 43) the Bessel period of φ is transferred along the lower chain one lift at a time (Theorem 44.4.1). How does the function left on Y_j become a lift between the *definite* spaces X_j? The proof groups the transfers in pairs: the string maps of two consecutive lifts fit into one isotropic map. We compute it for strings of lengths $3, 2, 1$; then, after each pair, we identify the translated stage function on the definite group.

Lift j ($1 \le j \le m$) goes from Y_{j-1} to Y_j; pair i ($0 \le i \le \varrho$) consists of lifts $2i+1$, $2i+2$. For $j < m$, Y_j is X_j plus a string of length $m-1-j$, with Bessel group R_j; Y_m is definite, of rank $n_m - 1$, with string of length 0 and $R_m = U(Y_m)$ (Chapter 33).

45.1. Stage functions

Fix λ, archimedean points g_j of $U(Y_j)$, finite points $y_j \in U(Y_j)(\mathbb{A}_f)$ ($j \ge 0$), a tame character ξ and $\varphi \in S$.

Definition 45.1.1. Put $\mathcal{W}_0^{\mathrm{tr}} := \mathcal{W}_{\lambda,\varphi}$ on $R_0(\mathbb{A})$. For $0 \le j \le m-1$ let

$$\mathcal{W}_{j+1}(h) := \int_{[R_j]} \mathcal{W}_j^{\mathrm{tr}}(r)\, \mathrm{CT}_{\mathrm{st}_{j+1}}\big(\omega_{j+1}(r\,(g_j, y_j), h)\, \phi_{j+1}(\xi)\big)\, dr$$

on $U(Y_{j+1})(\mathbb{A})$, the transfer of $\mathcal{W}_j^{\mathrm{tr}}$ for $\omega_{j+1}((g_j, y_j), 1)\, \phi_{j+1}(\xi)$, and, for $j+1 < m$, $\mathcal{W}_{j+1}^{\mathrm{tr}}(r) := \mathcal{W}_{j+1}(r\,(g_{j+1}, y_{j+1}))$ on $R_{j+1}(\mathbb{A})$. These are the *stage functions*.

In the proof, for $0 \le j < m$, $\mathcal{W}_j^{\mathrm{tr}}$ satisfies the hypothesis of Definition 44.4.2 (continuous, left $R_j(F)$-invariant, $\mathcal{W}_j^{\mathrm{tr}}(nr) = \psi_{\mathcal{U}}(n)\mathcal{W}_j^{\mathrm{tr}}(r)$ when $n-1$ has degree ≥ 2); call such functions *equivariant*. A *form of the conjugate type* on Y_j is defined as a form of the lower chain on Y_j, with the type kernel replaced by its complex conjugate; these forms are paired with those of the lower chain. In the proof, for $0 \le j < m$ there is a linear map $\Theta^{\top}_{\xi,j+1}$, the *transpose* of lift $j+1$, from the forms of the conjugate type on Y_{j+1} to those on Y_j, with

$$\int_{[U(Y_{j+1})]} z\ \Theta_{\xi,j+1} f = \int_{[U(Y_j)]} (\Theta^{\top}_{\xi,j+1} z)\, f$$

Date: November 26, 2026.

for every form f of the lower chain on Y_j and every form z of the conjugate type on Y_{j+1}; and for such z,

$$(\Theta^{\top}_{\xi,j+1}z)(g) = [K_j^{Y\circ} : K_j^Y(\xi)] \int_{[U(Y_{j+1})]} \theta\big(\omega_{j+1}(g,h)\,\phi_{j+1}(\xi)\big)\, z(h)\, dh,$$

and z is automorphic and rapidly decreasing.

Problem 45.1.2. For $0 \le j \le m-1$ and every form z of the conjugate type on Y_{j+1}, the integral on the right converges absolutely and

$$\int_{[R_j]} \mathcal{W}_j^{\mathrm{tr}}(r)\,(\Theta^{\top}_{\xi,j+1}z)\big(r\,(g_j,y_j)\big)\,dr = [K_j^{Y\circ} : K_j^Y(\xi)] \int_{R_{j+1}(F)\backslash U(Y_{j+1})(\mathbb{A})} \mathcal{W}_{j+1}\, z.$$

Chapter 46 uses this identity in the recursion for paired periods.

45.2. Three strings

For adelic maps and data we use the CM field, Weil data and framed spaces of Chapter 44. Write V^- for V with its form negated.

Definition 45.2.1. Let V, V', V'' be spaces with strings for the same N, of lengths $\ell+1, \ell, \max(\ell-1,0)$ $(\ell \ge 0)$, with string maps $\mathrm{st}_1 \colon V \to V'$ and $\mathrm{st}_2 \colon V' \to V''$. The *stacked string map* is $A := \binom{\mathrm{st}_1^*}{\mathrm{st}_2} \colon V' \to V^- \oplus V''$.

In Problems 45.2.2–45.2.4 take $E = \mathbb{Q}(\mathrm{i})$, $N = 5$, $c_V = c_{V'} = c_{V''} = 1$, no definite parts, $J_V = \mathrm{antidiag}(1,-5,1)$, $J_{V'} = \mathrm{antidiag}(1,1)$, $J_{V''} = (-5)$.

Problem 45.2.2. $\mathrm{st}_1 = \left(\begin{smallmatrix} 1 & 0 & 0 \\ 0 & -5 & 0 \end{smallmatrix}\right)$, $\mathrm{st}_2 = (1,0)$, and $\mathrm{st}_1\mathrm{st}_1^* = \mathrm{st}_2^*\mathrm{st}_2 = \left(\begin{smallmatrix} 0 & 0 \\ -5 & 0 \end{smallmatrix}\right)$.

Problem 45.2.3. A has rows $(0,0)$, $(1,0)$, $(0,1)$, $(1,0)$, and $A^*A = 0$ for the form $-J_V \oplus J_{V''}$.

Problem 45.2.4. For the grades of V' and of V as weights, the maps $a \colon V \to V'$ of positive degree are the $a = \left(\begin{smallmatrix} 0 & \alpha_0 & \alpha_1 \\ 0 & 0 & \alpha_2 \end{smallmatrix}\right)$; then $a^* = \left(\begin{smallmatrix} \bar\alpha_2 & \bar\alpha_1 \\ 0 & -\bar\alpha_0/5 \\ 0 & 0 \end{smallmatrix}\right)$, and $a \mapsto a^*$ is a conjugate-linear bijection onto the maps $V' \to V$ of positive degree.

Problem 45.2.5. Over $\mathbb{Q}(\mathrm{i})$, for three spaces with no definite parts, string lengths $4,3,2$, $N = 5$ and $c_V = c_{V'} = c_{V''} = 2$: $\mathrm{st}_1 = \left(\begin{smallmatrix} 2 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{smallmatrix}\right)$, $\mathrm{st}_2 = \left(\begin{smallmatrix} 1 & 0 & 0 \\ 0 & -10 & 0 \end{smallmatrix}\right)$, and $\mathrm{st}_1\mathrm{st}_1^* = \mathrm{st}_2^*\mathrm{st}_2 = \left(\begin{smallmatrix} 0 & 0 & 0 \\ 2 & 0 & 0 \\ 0 & -10 & 0 \end{smallmatrix}\right)$.

Problem 45.2.6. Let $\ell \ge 1$ and $c_V = c_{V'}$. Then $\mathrm{st}_1\mathrm{st}_1^* = \mathrm{st}_2^*\mathrm{st}_2$; this map kills the definite part and $f'_{\ell-1}$ and sends f'_q to a multiple of f'_{q+1} for $q < \ell-1$. Also $A^*A = -\mathrm{st}_1\mathrm{st}_1^* + \mathrm{st}_2^*\mathrm{st}_2 = 0$.

In pair i the strings of $Y_{2i}, Y_{2i+1}, Y_{2i+2}$ have lengths $2(\varrho-i)+1$, $2(\varrho-i)$, $2(\varrho-i)-1$ if $i < \varrho$ (a *middle pair*) and $1,0,0$ if $i = \varrho$ (the *last pair*). The gradings of Y_j, $j < m$, have one common constant; that of Y_m has constant 1. In a middle pair the first string has odd length, so a map $V' \to V^- \oplus V''$ homogeneous of degree zero kills the string of V' and maps its definite part into the span of the definite parts and the middle vectors f_{mid} of V and f'_{mid} of V'', of norms N in V^- and $-N$ in V''.

Problem 45.2.7. For norms 5, -5, the basis $\frac{1}{10}(f_{\mathrm{mid}} - f'_{\mathrm{mid}})$, $f_{\mathrm{mid}} + f'_{\mathrm{mid}}$ of the plane they span has Gram matrix $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$; in general so has $(f_{\mathrm{mid}} - f'_{\mathrm{mid}})/2N$, $f_{\mathrm{mid}} + f'_{\mathrm{mid}}$.

So in a middle pair the part of grade zero of $Y_{2i}^- \oplus Y_{2i+2}$ is $X_{2i}^- \oplus X_{2i+2}$ plus one hyperbolic plane.

Problem 45.2.8. In the last pair, with f_{mid} the vector of the string of $Y_{2\varrho}$, f_{mid}/π_N has norm 1 in $Y_{2\varrho}^-$, for $N = 5$, $\pi_N = 2 + \mathrm{i}$ and in general. The part of grade zero of $Y_{2\varrho}^- \oplus Y_m$ is $X_{2\varrho}^- \oplus X_m$, no plane being left, with $X_m = Y_m \perp E\, f_{\mathrm{mid}}/\pi_N$, and $h \in U(Y_m)$ acts on X_m as $\mathrm{diag}(h, 1)$.

Problem 45.2.9. In the last pair $A = 0$.

In the proof, $\mathrm{Heis}(w)\mathrm{Heis}(w') = \psi_E\big(\frac{1}{2} j_E \,\mathrm{tr}(w'^* w)\big)\mathrm{Heis}(w + w')$ for adelic maps w, w' between two spaces, the adjoint taken for their forms; we use it for $\mathrm{Hom}(V', V^- \oplus V'')$.

Problem 45.2.10. Under the hypotheses of Problem 45.2.6, $(An')^*(An) = 0$ and $\mathrm{Heis}(An)\mathrm{Heis}(An') = \mathrm{Heis}(A(n + n'))$ for all adelic endomorphisms n, n' of V'.

45.3. Two constant terms at once

Let V, V', V'' be spaces with strings for the same N, of lengths $\ell + 1, \ell, \max(\ell - 1, 0)$, $\ell \geq 0$ even, $c_V = c_{V'}$. For the splitting into definite spaces and the two-period identity take $V = Y_{2i}$, $V' = Y_{2i+1}$, $V'' = Y_{2i+2}$ with the middle or last double-lift datum of pair i. Write X, X', X_0'' for the definite parts and R, R' for the Bessel groups of V, V'. For data ϕ on $\mathrm{Hom}(V, V')$ and ϕ' on $\mathrm{Hom}(V', V'')$, the *join* $\phi \boxtimes \phi'$ on $\mathrm{Hom}(V', V^- \oplus V'')$ is, in the proof, the product of ϕ' with ϕ carried to $\mathrm{Hom}(V', V^-)$ by a scaled adjoint change of coordinates; for all adelic w, w', with matrices in the rational bases, $\mathrm{Heis}\binom{w^*}{w'}(\phi \boxtimes \phi') = \mathrm{Heis}(w)\phi \boxtimes \mathrm{Heis}(w')\phi'$. We use:

(i) *Product formula*, in the proof: for framed spaces V, V', V'' (definite ones included) there is $z_\theta \neq 0$ with $\theta(\phi \boxtimes \phi') = z_\theta\, \theta(\phi)\theta(\phi')$ for all ϕ, ϕ'. Compare Problem 23.4.1; for the Weil representation see [We].

For data on $\mathrm{Hom}(V', V^- \oplus V'')$ let $\mathrm{zt}_{>0}(\cdot)(0)$ be the mean of $\theta(\mathrm{Heis}(b)\,\cdot\,)$ over the adelic maps $b\colon V' \to V^- \oplus V''$ of positive degree modulo the rational ones (the weights on $V^- \oplus V''$ are the grades); at a point v of the retained grade-zero space, $\mathrm{zt}_{>0}(\phi)(v)$ is the same mean of $\theta(\mathrm{Heis}(\iota v + b)\phi)$, ι the inclusion of that space.

Problem 45.3.1. For adelic maps $w\colon V \to V'$ and $w'\colon V' \to V''$,

$$\mathrm{CT}_w \phi \cdot \mathrm{CT}_{w'} \phi' = z_\theta^{-1}\, \mathrm{zt}_{>0}\big(\mathrm{Heis}(w)\phi \boxtimes \mathrm{Heis}(w')\phi'\big)(0).$$

Problem 45.3.2. If $\mathrm{len}\, V$ is odd, all grades of V are even, and $n - 1$ has degree ≥ 2 for every $n \in \mathcal{U}(\mathbb{A})$.

In the proof, for the first edge with the Weil action ω of the rank twists of an automorphic character of the norm-one torus, $\mathcal{W}(nr)\,\mathrm{CT}_{\mathrm{st}_1}(\omega(nr, h)\phi) = \mathcal{W}(r)\,\mathrm{CT}_{\mathrm{st}_1}(\omega(r, h)\phi)$ for every equivariant $\mathcal{W}$, $n \in \mathcal{U}(\mathbb{A})$, $r \in R(\mathbb{A})$, $h \in U(V')(\mathbb{A})$. Let zt be the zero term along the maps of positive degree followed, in a middle pair, by the mean over the adelic maps modulo the rational maps from X' into the line $E(f_{\mathrm{mid}} + f'_{\mathrm{mid}})$ of Problem 45.2.7 (no plane in the last pair). It lands in data on $\mathrm{Hom}(X', X^- \oplus X'')$, where $X'' = X_0''$ in a middle pair and $X'' = X_m$ in the last pair.

(iv) *Bessel groups*, in the proof. Let $R = \mathcal{U} \rtimes U(X)$ be the Bessel group of a space W with a string; $[R]$ is compact. Let $b_1, \ldots, b_e$ be distinct basis vectors of grade one ($e \geq 0$; none if $\mathrm{len}\, W$ is odd) and $n^{(1)} := (c_W(n - 1)_{b_p, x})_{p,x}$, x running over

the basis of X. There is c_R such that: if H is continuous and left $R(F)$-invariant on $R(\mathbb{A})$, $H(n\gamma) = G_\gamma(n^{(1)})$ for $n \in \mathcal{U}(\mathbb{A})$, $\gamma \in U(X)(\mathbb{A})$, each G_γ is continuous and periodic under rational matrices, and its mean $\langle G_\gamma \rangle$ is continuous and left $U(X)(F)$-invariant, then $\int_{[R]} H = c_R \int_{[U(X)]} \langle G_\gamma \rangle \, d\gamma$. See [Bo].

For a middle or last pair we use the following two-period identity from the proof. Let ω, ω' be the Weil representations of the two edges, with automorphic characters μ, μ' of the norm-one torus, each multiplied on a space of rank d by $v^{\lfloor d/2 \rfloor}$. For data ϕ, ϕ', an equivariant $\mathcal{W}$ on $R(\mathbb{A})$ and $h \in U(X_0'')(\mathbb{A})$, acting on V'' through X_0'',

$$\int_{[R']} \int_{[R]} \mathcal{W}(r) \, \mathrm{CT}_{\mathrm{st}_1}\big(\omega(r, r')\phi\big) \, \mathrm{CT}_{\mathrm{st}_2}\big(\omega'(r', h)\phi'\big) \, dr \, dr'$$
$$= \frac{c_R c_{R'}}{z_\theta} \int_{[U(X)]} \mathcal{W}(\gamma) \int_{[U(X')]} \theta\big(\omega^{\triangle}(\gamma, \gamma', \bar{h}) \, \mathrm{zt}\,\mathrm{Heis}(A)(\phi \boxtimes \phi')\big) \, d\gamma' \, d\gamma, \quad (1)$$

where $c_R, c_{R'}$ do not depend on $\mu, \mu', \phi, \phi', \mathcal{W}$ or h; $\omega^{\triangle}$ is the Weil representation of $U(X) \times U(X') \times U(X'')$ on $\mathrm{Hom}(X', X^- \oplus X'')$ normalized as in the proof (the characters μ, μ' and a flip character); and $\bar{h} = h$ in a middle pair, $\bar{h} = \mathrm{diag}(h, 1)$ in the last.

45.4. The definite double lift

The right side of (1) is a double theta integral between definite spaces. First the Gaussian case.

Problem 45.4.1. By machine, $c_4 = 0.143191337023821\ldots$, and the composite $\mathcal{A}_{(4)}(1) \to \mathcal{A}_{(4)}(1) \to \mathcal{A}_{(4)}(1)$ of two lifts $\Theta_{(4)}$ is multiplication by $c_4^2/16 = 0.00128148493741\ldots$.

In a model with several classes a form is a vector indexed by classes, a lift has a kernel matrix K, the class weights form a diagonal matrix D, the lift is $v \mapsto KDv$, and $\langle z, v \rangle := z^t D v$.

Problem 45.4.2. For $K_0 = \left(\begin{smallmatrix} 1 & 2 \\ 3 & -1 \end{smallmatrix}\right)$, $K_1 = \left(\begin{smallmatrix} 2 & 1 \\ 0 & -1 \end{smallmatrix}\right)$, $D_0 = \mathrm{diag}(1, \frac{1}{2})$, $D_1 = \mathrm{diag}(\frac{1}{3}, 1)$, $D_2 = \mathrm{diag}(1, \frac{1}{4})$, $v = (2, 1)^t$, $z = (1, -2)^t$: $K_1 D_1 K_0 D_0 v = (\frac{15}{2}, -\frac{11}{2})^t$, $z^t D_2 K_1 D_1 K_0 D_0 v = \frac{41}{4}$, and with both lifts transposed onto z, $K_0^t D_1 K_1^t D_2 z = (\frac{31}{6}, -\frac{1}{6})^t$, whose pairing $(\cdot)^t D_0 v$ with v is again $\frac{41}{4}$.

Each datum $\phi_j(\xi)$ is a pure tensor $\mathbf{u} \otimes \phi_f$ of a real Fock vector $\mathbf{u}$ and a finite datum ϕ_f (the integrated Heisenberg action of the proof). In the proof: the Weil actions, the join and $\mathrm{Heis}(w)$ respect this separation, a translate staying pure with any scalar absorbed in its real vector; on the real factor the characters act through their weights, which do not depend on the tame character; and the finite join $\boxtimes$ on tensors of finite data is injective, with a linear left inverse $\boxtimes^{-1}$.

(ii) *Archimedean zero term*, in the proof: for a translate $\mathrm{Heis}(w)$ and a real Fock vector $\mathbf{u}$ there is a real Fock vector $\mathbf{u}_0$ with $\mathrm{zt}(\mathrm{Heis}(w)(\mathbf{u} \otimes \phi_f)) = \mathbf{u}_0 \otimes \mathrm{zt}_f(\mathrm{Heis}_f(w_f)\phi_f)$ for every ϕ_f; here zt_f is the finite zero term and w_f the finite coordinate of the translation in the Weil model (the finite part of w, conjugated into the frames and divided by the finite idele of the Weil data). For the mixed model see [MVW], [We].

Definition 45.4.3. For $0 \le i \le \varrho$, with A and zt those of pair i, the *evaluated pair datum* is

$$\phi_i^{\mathrm{ev}}(\xi, y) := \boxtimes^{-1} \operatorname{zt}_f \operatorname{Heis}_f(A_f)\big(\mathbf{1}_{2i+1}(\xi)^y \boxtimes \mathbf{1}_{2i+2}(\xi)^y\big),$$
$$\text{where } \mathbf{1}_j(\xi)^y := \omega_j(y_{j-1}, y_j)\, \mathbf{1}_j(\xi),$$

with A_f as in (ii); it is a tensor of finite data on $\operatorname{Hom}(X_{2i}, X_{2i+1})$ and on $\operatorname{Hom}(X_{2i+1}, X_{2i+2})$.

In the proof, $\boxtimes\phi_i^{\mathrm{ev}}(\xi, y)$ is the finite zero term itself. Put $\phi_j(\xi)^{g,y} := \omega_j((g_{j-1}, y_{j-1}), (g_j, y_j))\, \phi_j(\xi)$.

Problem 45.4.4. For the fixed pair data and harmonics there is a real Fock vector $\mathbf{u}_i$, depending on the outer points only through $g_{2i}, g_{2i+1}, g_{2i+2}$, with $\operatorname{zt}\operatorname{Heis}(A)(\phi_{2i+1}(\xi)^{g,y} \boxtimes \phi_{2i+2}(\xi)^{g,y}) = \mathbf{u}_i \otimes \boxtimes\, \phi_i^{\mathrm{ev}}(\xi, y)$ for every tame ξ and all finite points y.

(iii) *Definite theta lifts*, in the proof. For a form ψ of the prescribed weight on X and a linear form l on its values put $\operatorname{coeff}_l \psi(\gamma) := l(\gamma_\infty^{-1}\psi(\gamma_f))$, γ_∞ acting on the values. For a family of definite lifts Θ_o^X, $o \in O$, between fixed spaces of algebraic forms of the prescribed source and target weights, with Weil actions ω_o, the coefficient property is: for every polynomial P on $\operatorname{Hom}(X, X')_\infty$, with Fock vector v_P, and every l there is l' such that for all o, finite data ϕ_f, forms ψ and $h \in U(X')(\mathbb{A})$,

$$\int_{[U(X)]} \theta\big(\omega_o(\gamma, h)(v_P \otimes \phi_f)\big)\, \operatorname{coeff}_l \psi(\gamma)\, d\gamma = \operatorname{coeff}_{l'}\big(\Theta_o^X(\phi_f)\psi\big)(h).$$

In the proof the lifts of the definite chain, O the tame characters, have it. See [Gr], [KV], [Ho].

Problem 45.4.5. Let $\Lambda\colon \mathsf{L} \to \mathsf{V}$ be $\mathbb{C}$-linear from a finite-dimensional complex vector space to a Hausdorff complex topological vector space, and $I\colon \mathsf{H} \to \mathsf{V}$ continuous on a topological space. If $I(u) \in \Lambda(\mathsf{L})$ for u in a dense subset of H, then for all $u \in \mathsf{H}$.

For polynomials P on $\operatorname{Hom}(X, X')_\infty$ and Q on $\operatorname{Hom}(X', X'')_\infty$, let PQ be their product after transposing the variables of P into the X-block and placing those of Q in the X''-block. In the proof, for finite data v, v' on the two edges, $(v_P \otimes v) \boxtimes (v_Q \otimes v') = v_{PQ} \otimes (v \boxtimes v')$, and on such joins the triple action at (γ, γ', h) acts on the two factors by the rank-twisted Weil actions of $X \to X'$ at (γ, γ') and of $X' \to X''$ at (γ', h).

Problem 45.4.6. Fix automorphic characters μ_o, μ_o' of the norm-one torus, $o \in O$, and families $\Theta_{1,o}^X\colon X \to X'$, $\Theta_{2,o}^X\colon X' \to X''$ with the same intermediate space of forms, having (iii) for the rank twists of μ_o and μ_o'; let $\omega_o^\triangle$ be their triple action. For P, Q as above and every l there is l'' such that for all o, finite data ϕ_f, ϕ_f', forms ψ on X and $h \in U(X'')(\mathbb{A})$,

$$\int_{[U(X)]} \operatorname{coeff}_l \psi(\gamma) \int_{[U(X')]} \theta\big(\omega_o^\triangle(\gamma, \gamma', h)(v_{PQ} \otimes (\phi_f \boxtimes \phi_f'))\big)\, d\gamma'\, d\gamma$$
$$= \operatorname{coeff}_{l''}\big(\Theta_{2,o}^X(\phi_f')\, \Theta_{1,o}^X(\phi_f)\, \psi\big)(h).$$

In the proof the polynomial vectors are dense in the real Fock model in its L^1 norm (for the Hilbert space see [Ba] and Problem 12.1.2); the families of double integrals, with pointwise topology in the other arguments, depend continuously on $\mathbf{u}$; and for fixed l the families $\mathrm{coeff}_{l''}(\cdots)$ form a finite-dimensional space as l'' varies. Every polynomial is a sum of products PQ, and both sides are linear in the finite tensor. For these same two families the proof gives the following coefficient formula: for every real Fock vector $\mathbf{u}$ and every l there is l'' with

$$\int_{[U(X)]} \mathrm{coeff}_l\,\psi(\gamma) \int_{[U(X')]} \theta\big(\omega_o^{\triangle}(\gamma,\gamma',h)(\mathbf{u}\otimes\boxtimes\Phi)\big)\,d\gamma'\,d\gamma = \mathrm{coeff}_{l''}\big(\Theta_o^X(\Phi)\psi\big)(h)$$

for all o, finite pair tensors Φ, forms ψ and h, where $\Theta_o^X(v\otimes v') := \Theta_{2,o}^X(v')\Theta_{1,o}^X(v)$, extended linearly. In the chain, l'' is chosen before the tame character. In the proof, for pair i the characters μ, μ' of (1) are those of lifts $2i+1$ and $2i+2$, the families are $\Theta_{1,\xi}^X = \Theta_{\xi,2i+1}^X$ and $\Theta_{2,\xi}^X = \Theta_{\xi,2i+2}^X$ with the rank twists of these characters, O the tame characters, and $\omega^{\triangle}$ of (1) is their triple action.

45.5. Induction on pairs

For $0 \le j < m$, a form ψ on X_j and a linear form l, let $\mathcal{W}_{l,\psi}$ on $R_j(\mathbb{A})$ be formed as $\mathcal{W}_{\lambda,\varphi}$ in Section 43.4: $\mathcal{W}_{l,\psi}(n\gamma) = \psi_{\mathcal{U}}(n)\,\mathrm{coeff}_l\,\psi(\gamma)$ for $n \in \mathcal{U}(\mathbb{A})$, $\gamma \in U(X_j)(\mathbb{A})$, with $\psi_{\mathcal{U}}(n) := \psi_E\big(\frac{1}{2} j_E \,\mathrm{tr}(\mathrm{st}_{j+1}^* \mathrm{st}_{j+1} n)\big)$ for every $n \in \mathcal{U}(\mathbb{A})$.

Problem 45.5.1. Let $\mathrm{len}\,Y_j$ be odd and $\mathcal{W}$ be equivariant on $R_j(\mathbb{A})$ with $\mathcal{W}(\gamma) = \mathrm{coeff}_l\,\psi(\gamma)$ for all $\gamma \in U(X_j)(\mathbb{A})$. Then $\mathcal{W} = \mathcal{W}_{l,\psi}$.

For finite pair tensors $\Phi_0,\dots,\Phi_i$, $\Theta_\xi^X(\Phi_i\otimes\cdots\otimes\Phi_0)$ is the composite of the first $i+1$ double lifts of the definite chain, pair j acting through $v\otimes v' \mapsto \Theta_{\xi,2j+2}^X(v')\circ\Theta_{\xi,2j+1}^X(v)$.

Theorem 45.5.1 (two lifts at a time)**.** *Fix λ, archimedean points g_k of $U(Y_k)$ $(k \ge 0)$ and $0 \le i \le \varrho$. There is a linear form l on the values of forms on X_{2i+2}, independent of the tame character, of φ and of the finite points, such that for every tame character ξ, every $\varphi \in S$, all finite points $y_k \in U(Y_k)(\mathbb{A}_f)$, and every h in $U(X_{2i+2})(\mathbb{A})$ if $i < \varrho$, in $U(Y_m)(\mathbb{A})$ if $i = \varrho$,*

$$\mathcal{W}_{2i+2}\big(h\,(g_{2i+2}, y_{2i+2})\big) = \mathrm{coeff}_l\Big(\Theta_\xi^X\big(\phi_i^{\mathrm{ev}}(\xi,y)\otimes\cdots\otimes\phi_0^{\mathrm{ev}}(\xi,y)\big)\varphi\Big)(\bar h).$$

Here h acts on Y_{2i+2} through its definite part, and $\bar h = h$ if $i < \varrho$, $\bar h = \mathrm{diag}(h,1) \in U(X_m)(\mathbb{A})$ if $i = \varrho$.

What has been proved. On the definite group the translated stage function after each pair is a coefficient of the definite chain, with one linear form for all tame characters, source forms and finite points. The problems prove: the isotropy of the stacked map (Problems 45.2.6 and 45.2.10), the product of two constant terms (Problem 45.3.1), the separation of the archimedean variables (Problem 45.4.4), the coefficient formula for polynomial vectors with its extension by density (Problems 45.4.6 and 45.4.5), and that an equivariant function on an odd string is determined by its values on the definite group (Problem 45.5.1). The hints indicate how Theorem 45.5.1 follows from these. Taken as given: the product formula (i), the archimedean zero term (ii), the coefficient property of the definite lifts (iii), the integration over a Bessel group (iv), the two-period identity (1) and the coefficient formula for all real Fock vectors (both stated from the proof; the problems give

their ingredients), and the statements marked "in the proof". Chapter 46 needs Definitions 45.1.1 and 45.4.3, Problem 45.1.2 and Theorem 45.5.1: for ramified source forms it applies support bounds and quotient integration to periods whose dependence on the archimedean points and the finite level classes separates.

In the Lean formalization. Theorem 45.5.1 specializes `Data.exists_unfoldStage_eq_algFormCoeff` [GL], which allows any double-lift data with the prescribed finite evaluation for pair i and an independent final archimedean point; here they are the middle or last pair and g_{2i+2}. The stage functions are `unfoldStageOn` and `unfoldStage`, the stacked map `stackedStringMap`, the evaluated pair datum `evaluatedDatum`. Identity (1) specializes `DoubleLiftData.exists_integral_constTermAtStringMap_mul_eq` (the action is `tripleWeil`); the display before Section 45.5 is `integral_theta_tripleWeil_eq_lift_comp`. Input (i) is `theta_arrowProduct`, (ii) specializes `exists_zeroTerm_rho_integrated_eq`, (iii) is `IsThetaLift`, proved for the chain by `isThetaLift_thetaKernel`, and (iv) is `isCocompact_ratBessel` with `integral_besselMeasure_eq_of_mean`. The other statements marked "in the proof" are:
`exists_unfoldStageOn_even_eq_sourceFn` and `formAdjoint_stackedStringMap_mul_stackedStringMap` (pairs, isotropy); `isEquivariant_unfoldStageOn` (equivariance of the stages); `transposedLiftY_apply`, `integral_mul_liftY` and `isRapid_conjFormY` (the transpose); `Heisenberg.Rep.mul` and `homBicharacter_eq` (the Heisenberg law); `arrowProduct` and `homHeisenbergOp_arrowProduct` (the join); `mul_constTermAtStringMap_unipotent_mul` (the first edge); `datumY`, `pairWeil_integrated_all`, `boxProd_integrated`, `CoordChange.map_integrated`, `exists_rho_integrated_eq`, `hasWeight_liftChar`, `injective_arrowTensor` and `leftInverse_arrowTensor` (the separation); `DoubleLiftData.arrowTensor_finEval` (the evaluated datum); `arrowProduct_integrated_polyVector` and `arrowProduct_twistedPairWeil` (polynomial joins); `Fock.denseRange_polyVector` (density), the remaining steps of the coefficient formula being in the proof of `integral_theta_tripleWeil_eq_lift_comp`; and `exists_unfoldStage_eq_algFormCoeff_of_sourceFn` (the order of l'' and ξ in the chain). Automorphy at stage $j+1$ is part of `ConjFormY`. In Problem 45.1.2 absolute convergence is `integrable_unfoldStage_mul` and the equality is `integral_unfoldStageOn_mul_transposedLiftY`.

Hints

§45.1.

45.1.2: Move (g_j, y_j) into the datum and apply Theorem 44.4.1 to $\mathcal{W}_j^{\mathrm{tr}}$.

§45.2.

45.2.3: The adjoint of $\binom{P}{Q}$ into $V^- \oplus V''$ is $(-P^*, Q^*)$.
45.2.4: The forms pair grades g and $-g$.
45.2.6: Compute both products on each f'_q, using $\bar{c}_V = c_V$.
45.2.8: Problem 33.5.2.

§45.3.

45.3.1: As in Problem 45.2.4, $a \mapsto a^*$ preserves positive degree; use (i) and Fubini on the compact groups.

§45.4.

45.4.1: Problem 23.2.3; keep track of the class weight in each lift; in Python, sum $\alpha^4 e^{-\pi|\alpha|^2}$ over $|\Re\alpha|, |\Im\alpha| \le 8$.

45.4.4: Split data and points into real and finite factors; apply (ii).

45.4.5: Finite-dimensional subspaces of a Hausdorff topological vector space are closed.

45.4.6: Apply (i) to the definite triple X, X', X'', with its own scalar z_θ^X; after Fubini use (iii) over γ, then over γ' for $z_\theta^X Q$.

§45.5.

45.5.1: Problem 45.3.2. For Theorem 45.5.1: apply the coefficient formula with $\mathbf{u} = (c_R c_{R'}/z_\theta)\mathbf{u}_i$, and Problem 45.5.1 at the intermediate even stages.

References

[Ba] V. Bargmann, *On a Hilbert space of analytic functions and an associated integral transform, Part I*, Comm. Pure Appl. Math. **14** (1961), 187–214.

[Bo] A. Borel, *Introduction aux groupes arithmétiques*, Hermann, Paris, 1969.

[GL] L. Sernau, *GRH for Dirichlet L-functions, in Lean 4*, a shorter rewriting of the Lean proof, text by Claude, `https://github.com/lsernau/grh-lean`, commit `72fead1`, readable edition `grh/`.

[Gr] B. H. Gross, *Algebraic modular forms*, Israel J. Math. **113** (1999), 61–93.

[Ho] R. Howe, *Transcending classical invariant theory*, J. Amer. Math. Soc. **2** (1989), 535–552.

[KV] M. Kashiwara and M. Vergne, *On the Segal–Shale–Weil representations and harmonic polynomials*, Invent. Math. **44** (1978), 1–47.

[MVW] C. Mœglin, M.-F. Vignéras and J.-L. Waldspurger, *Correspondances de Howe sur un corps p-adique*, Lecture Notes in Math. 1291, Springer, 1987.

[We] A. Weil, *Sur certains groupes d'opérateurs unitaires*, Acta Math. **111** (1964), 143–211.

LATTICES, CUTS AND THE RAMIFIED FORMS

Prerequisites. Lattices and their duals [OM]. From Chapter 45: stage functions $\mathcal{W}_j$ (Definition 45.1.1), the evaluated pair data $\phi_i^{\mathrm{ev}}(\xi, y)$ (Definition 45.4.3), the transposes $\Theta_{\xi,j}^{\top}$ with $\int z\,\Theta_{\xi,j} f = \int (\Theta_{\xi,j}^{\top} z) f$, the ordered pair tensors $\Phi_{\varrho} \otimes \cdots \otimes \Phi_0$, Problem 45.1.2 and Theorem 45.5.1; from Chapter 44, the grades (Definition 44.2.2) and the string maps $\mathrm{st}_j \colon Y_{j-1} \to Y_j$ (Definition 44.2.3). From Section 43.4: the lower and definite chains, their data, the definite lift $\Theta_{\xi}^{X}(\cdot)$ of a tensor, its Weil action ω^X, and the restriction res; from Chapter 43, Problems 43.3.2, 43.5.2 and 43.5.3. $K_j^{Y\circ}$ is the lattice stabilizer on Y_j, $K_j^Y(\xi)$ its subgroup reducing to 1 at the places dividing π_M and those of Q_ξ. K_M is the principal level of Y_0 (Sections 34.4 and 43.4); $K_0^Y(\xi) \subseteq K_M \subseteq K_0^{Y\circ}$. From Chapter 36: the Bessel subgroups (Section 36.1). The Poincaré map $\mathcal{P}_{g,\lambda}$ is that of Section 43.4. From Chapter 34: the spaces, $S \supseteq S_{\mathrm{ram}}$, T_w, z_w, tame characters ξ with Q_ξ and $\mathrm{Nm}\, Q_\xi$. R_j is the Bessel subgroup of Y_j, $[R_j] := R_j(F)\backslash R_j(\mathbb{A})$; for $0 \le j < m$ the string has length $m-1-j$, and $R_m = U(Y_m)$. $\varrho = m/2 - 1$. "The proof" is the one in [GL].

The seesaw identity (Theorem 43.4.1) is proved by pairing $\Theta_{\xi,m} \cdots \Theta_{\xi,1} \mathcal{P}_{g,\lambda}\varphi$ with a form on Y_m and transferring the Bessel period up the lower chain. Chapter 45 computes what is left after the transfers as a function of the outer variables $(g_k, y_k) \in U(Y_k)(\mathbb{A})$. At stage zero the finite sum is over classes in K_M. At the subsequent stages the Bessel periods must be integrated over the remaining outer variables. Which finite sets of level classes suffice to compute these integrals, and with which weights? The answer uses the lattices of the finite points and, at one place, the hypothesis $\varphi \in S_{\mathrm{ram}}$. The result is Theorem 46.4.1.

46.1. The first lift

Problem 46.1.1. Let y and z' be functions on $[U(Y_0)]$, fixed by right translation by K_M and by $K_0^Y(\xi)$ respectively, with yz' integrable. Then

$$\int_{[U(Y_0)]} y(h) \sum_{c \in K_M / K_0^Y(\xi)} z'(hc)\, dh = [K_M : K_0^Y(\xi)] \int_{[U(Y_0)]} y\, z'.$$

Hence, for every tame ξ, every $\varphi \in S$ and every form z on Y_1 as in Problem 45.1.2,

$$\int_{[U(Y_1)]} z\, \Theta_{\xi,1} \mathcal{P}_{g,\lambda}\varphi = [K_0^{Y\circ} : K_M] \sum_{c \in K_M / K_0^Y(\xi)} \int_{R_1(F)\backslash U(Y_1)(\mathbb{A})} \mathcal{W}_1\, z,$$

where the summand uses $(g, \tilde{c})$ in outer slot 0, with $\tilde{c} \in K_M$ any representative of c, and the identity in every other slot.

Date: November 26, 2026.

46.2. Lattices of finite points

The lattice of the finite point enters the support condition. The classes used for the evaluated data are taken modulo $K_j^Y(\xi)$. For $0 \le j \le m-1$ write X_j for the definite part of Y_j and $X_j^\perp$ for the span of its string, both in the rational frame of Chapter 34.

Definition 46.2.1. The *lattice* $\Lambda(x)$ of a point $x \in U(Y_j)(\mathbb{A}_f)$ is the set of finite adelic vectors whose coordinates in the frame of x (the frame of Chapter 34 followed by x) are integral, so that $\Lambda(x) = x\Lambda(1)$ when x acts in that frame. Its *string parts* are $\Lambda^-(x) := \Lambda(x) \cap X_j^\perp$ and $\Lambda^+(x) := \operatorname{pr}\Lambda(x)$, where pr is the orthogonal projection to $X_j^\perp$. We write $\Lambda_j^\pm$ when the stage must be named.

Definition 46.2.2. A lattice is *graded* if it contains the part of each grade of each of its vectors.

As the frame of x is orthonormal, $\Lambda(x)$ is self-dual. The standard lattice $\Lambda(1)$ is graded. At a place $w \mid \pi_N$, the standard lattice of an odd string is spanned, in the last definite coordinate and the middle string coordinate, by vectors $(1, \epsilon/N)$ and $(0, \epsilon')$ with units ϵ, ϵ'. In the toy $N = 5$, the place has degree one, $\epsilon = \epsilon' = 1$. In $\mathbb{Q}_5^2 = \mathbb{Q}_5 e_1 \oplus \mathbb{Q}_5 e_2$ call e_1 the definite coordinate and e_2 the string coordinate, and define $\Lambda^\pm$ as in Definition 46.2.1 with $X^\perp = \mathbb{Q}_5 e_2$; no form is fixed here.

Problem 46.2.3. For $\Lambda = B\mathbb{Z}_5^2$, $B = \left(\begin{smallmatrix} 1 & 0 \\ 1/5 & 1 \end{smallmatrix}\right)$: $\Lambda^- = \mathbb{Z}_5 e_2$, $\Lambda^+ = 5^{-1}\mathbb{Z}_5 e_2$ and $\#\Lambda^+/\Lambda^- = 5$. For $\Lambda = D'\mathbb{Z}_5^2$, $D' = \operatorname{diag}(5, 1/5)$: $\Lambda^- = \Lambda^+ = 5^{-1}\mathbb{Z}_5 e_2$.

Problem 46.2.4. Over a DVR, or a product of two exchanged by the involution, let Λ be a lattice, self-dual for a nondegenerate hermitian form, in a space $W \perp W'$. Then the dual of $\Lambda \cap W$ in W is the projection of Λ to W. Hence, for $x, x' \in U(Y_j)(\mathbb{A}_f)$ and a finite idele ϖ, $\varpi\Lambda^-(x) \subseteq \Lambda^-(x')$ implies $\bar\varpi\Lambda^+(x') \subseteq \Lambda^+(x)$.

Problem 46.2.5. A function on $\mathbb{Z}/25$ invariant under translation by $5\mathbb{Z}/25$ has Fourier transform supported on $5\mathbb{Z}/25$.

Definition 46.2.6. Let ϖ_ξ and ϖ_M be the generator ideles fixed in the proof for the ideals $(\pi_M)\prod_{w \in Q_\xi} w$ and (π_M); each has component 1 away from the places dividing its ideal. The *idele of the modulus* is $\mathfrak{u} := \varpi_\xi/\varpi_M$. It is a uniformizer at every $w \in Q_\xi$ and a unit at every other finite place.

In this sheet $\mathfrak{a} := \varpi_W/\bar\varpi_M$, where ϖ_W is the self-dual scale of the Weil data. Throughout this paragraph let $0 \le j \le m-2$. The finite datum of lift $j+1$ is fixed by the finite Heisenberg translations by $\varpi_\xi v$ for every integral vector v in the finite space of maps from Y_j to Y_{j+1}. The proof shows: let $\mathcal{W}_{j+1}(g_\infty, x') \ne 0$, so that the integrand defining it (Definitions 44.4.2 and 45.1.1) is nonzero at some $r \in R_j(\mathbb{A})$, and let x be the finite part of $r(g_j, y_j)$; if $r_1 \in R_j(\mathbb{A}_f)$ and $r_2 \in R_{j+1}(\mathbb{A}_f)$ make $\Lambda(r_1 x)$ and $\Lambda(r_2 x')$ graded, then

$$(\bar{\mathfrak{u}}/\mathfrak{a})\,\mathrm{st}_{j+1}\Lambda_j^+(r_1 x) \subseteq \Lambda_{j+1}^-(r_2 x').$$

For the standard lattices it shows $\mathrm{st}_{j+1}\Lambda_j^+(1) = \mathfrak{a}\,\Lambda_{j+1}^-(1)$.

Problem 46.2.7. Use the string matrices $J_3 = \left(\begin{smallmatrix} 0 & 0 & 1 \\ 0 & -5 & 0 \\ 1 & 0 & 0 \end{smallmatrix}\right)$, $J_2 = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$ and $\mathrm{st}_1 = \left(\begin{smallmatrix} 1 & 0 & 0 \\ 0 & -5 & 0 \end{smallmatrix}\right)$ of Chapter 45 ($N = 5$, string constant 1), and let $\hat{\mathcal{O}}$ be the integral finite adeles of $\mathbb{Q}(\mathrm{i})$. On the first string let $L^- = \hat{\mathcal{O}}^3$ and $L^+ = \operatorname{diag}(1, \frac{1}{5}, 1)\hat{\mathcal{O}}^3$, on the

second $L' = \hat{\mathcal{O}}^2$. Then L^- and L^+ are dual for J_3, L' is self-dual for J_2, and $\mathrm{st}_1 L^+ = L'$.

Definition 46.2.8. A point $x \in U(Y_j)(\mathbb{A}_f)$ has the *lattice bounds* at stage j if $\bar{\mathfrak{u}}^j \Lambda_j^-(1) \subseteq \Lambda_j^-(x)$ and $\mathfrak{u}^j \Lambda_j^-(x) \subseteq \Lambda_j^-(1)$.

Problem 46.2.9. Let $0 \le j \le m-2$, and suppose $\mathfrak{u}^j \Lambda_j^-(r_1 x) \subseteq \Lambda_j^-(1)$ and $(\bar{\mathfrak{u}}/\mathfrak{a})\,\mathrm{st}_{j+1}\Lambda_j^+(r_1 x) \subseteq \Lambda_{j+1}^-(r_2 x')$. Then $\bar{\mathfrak{u}}^{j+1}\Lambda_{j+1}^-(1) \subseteq \Lambda_{j+1}^-(r_2 x')$.

Definition 46.2.10. $\Lambda(x)$ is *split* at a finite place w if $1_w \Lambda^+(x) \subseteq \Lambda^-(x)$, where 1_w is the idempotent finite adele that is 1 at w and 0 elsewhere.

The proof shows that $\Lambda_j^+(1) = \Lambda_j^-(1)$ for an even string, and that for an odd string the two differ only in the middle coordinate, by a simple pole at the places above N: at each $w \mid N$ the quotient is the residue field k_w, as in Problem 46.2.3.

Problem 46.2.11. Let $1 \le j \le m-1$ and $\bar{\mathfrak{u}}^j \Lambda_j^-(1) \subseteq \Lambda_j^-(x)$, but $\mathfrak{u}^j \Lambda_j^-(x) \not\subseteq \Lambda_j^-(1)$. Then some $\mathfrak{u}^j v$, $v \in \Lambda_j^-(x)$, lies in $\Lambda_j^+(1)$ but not in $\Lambda_j^-(1)$. Moreover, the string of Y_j is odd, j is even, and $\Lambda(x)$ is split at a place w dividing π_N.

Problem 46.2.12. For $z = \mathrm{diag}(2,1)$, the scaling of the definite coordinate by a generator of $(\mathbb{Z}/5)^\times$: $B^{-1} z B = \left(\begin{smallmatrix} 2 & 0 \\ -1/5 & 1 \end{smallmatrix}\right)$ is not integral, and $D'^{-1} z D' = z$.

In general, if $\Lambda(x)$ is split at $w \mid \pi_N$, then $x^{-1} z_w x$, with z_w acting as a scalar on X_j and trivially on the string, is integral and 1 off $w, \bar{w}$. It belongs to $K_j^Y(\xi)$.

Problem 46.2.13. For $\mathrm{sh}\, e_k = e_{k+1 \bmod 4}$ on $\mathbb{C}^4$: $(1 - \mathrm{sh})e_0 = (1, -1, 0, 0)$ and $(1 + \mathrm{sh} + \mathrm{sh}^2 + \mathrm{sh}^3)(1 - \mathrm{sh})e_0 = 0$.

Problem 46.2.14. Suppose $\omega^X(z_w, z_w)$ acts trivially on the data of every lift $X_k \to X_{k+1}$, and $\omega^X(1, z_w)$, acting on one factor alone, fixes a tensor v of data. Then the (partial) chain $\Theta_\xi^X(v)$ satisfies $\Theta_\xi^X(v)\, T_w = \Theta_\xi^X(v)$, and it vanishes on S_{ram}.

For $w \mid \pi_N$, the diagonal scaling $\omega^X(z_w, z_w)$ is the identity on every lift: the base changes of the characters of the lifts are unramified at the places above N. For $0 \le i < \varrho$, embed $U(X_{2i+2})$ into $U(Y_{2i+2})$ by the identity on the string. If $y_{2i+2}^{-1} z_w y_{2i+2} \in K_{2i+2}^Y(\xi)$, then $\omega^X(1, z_w)$ on the second tensor factor fixes $\phi_i^{\mathrm{ev}}(\xi, y)$.

Problem 46.2.15. Let $\varphi \in S_{\mathrm{ram}}$, $2 \le j \le m-1$ even, and $\Lambda(x)$ split at some $w \mid \pi_N$. Then $\mathcal{W}_j(\gamma(g_\infty, x)) = 0$ for every $\gamma \in R_j(\mathbb{A})$ and every archimedean point g_∞.

Problem 46.2.16. Let $\varphi \in S_{\mathrm{ram}}$, $y_0 \in K_M$, $1 \le j \le m-1$, and $\mathcal{W}_j(g_\infty, x) \ne 0$. Then $r_2 x$ has the lattice bounds at stage j for every $r_2 \in R_j(\mathbb{A}_f)$ with $\Lambda(r_2 x)$ graded.

This is where the hypothesis $\varphi \in S_{\mathrm{ram}}$ enters. We use two facts for the field E of the data, which contains a primitive 5040th root of unity. (i) Every finite point x has a translate ux with u in the unipotent subgroup of $R_j(\mathbb{A}_f)$ and $\Lambda(ux)$ graded. This is the lattice form of the Iwasawa decomposition [Ti, 3.3.2]. (ii) There is a finite set $\mathcal{Z}_j$ of finite points equal to 1 outside $Q_\xi \cup \bar{Q}_\xi$ such that, if the $R_j(\mathbb{A}_f)$-orbit of x contains a graded point satisfying the bounds, then $rx \in \mathcal{Z}_j K_j^{Y\circ}$ for some $r \in R_j(\mathbb{A}_f)$. We use (ii) as proved in [GL]. Two classical lattice facts used there are that only finitely many lattices lie between two fixed full lattices, and that a lattice is determined by its local components [OM].

46.3. Cuts and multiplicities

In this sheet let a group G_0 act on a set, let $G_1 \subseteq G_0$ be a subgroup and Cut a finite G_1-stable subset, and put $\mathrm{mult}(t) := \#\{rG_1 \in G_0/G_1 : r^{-1}t \in \mathrm{Cut}\}$, with the value 0 for an infinite count. For a finite group acting on a finite set, if the cut meets every orbit, this is the setting of Problem 43.3.2 with translates counted modulo G_1.

Problem 46.3.1. Let $G_0 = H = S_3$ act on H/H_0, $G_1 = H_0 := \langle(1\,2)\rangle$, $x = (1\,2\,3)$, $\mathrm{Cut} := \{hxH_0 : h \in H_0\} \subset H/H_0$. Then $\#\mathrm{Cut} = 2$, the multiplicities of the three cosets are $2, 2, 2$, and for $f_1(hH_0) := h(3)$,

$$\sum_{t\in H/H_0} f_1(t) = 6 = \sum_{rH_0\in H/H_0}\ \sum_{c\in\mathrm{Cut}} \frac{f_1(rc)}{\mathrm{mult}(rc)}.$$

Definition 46.3.2. $\mathrm{Cut}_0(\xi)$ is the set of classes modulo $K_0^Y(\xi)$ of the elements of K_M, with $\mathrm{mult}_0 := 1$. For $1 \le j \le m-1$, let $G_0 = R_j(\mathbb{A}_f)$ and $G_1 = R_j(\mathbb{A}_f) \cap K_j^{Y\circ}$ act on $U(Y_j)(\mathbb{A}_f)/K_j^Y(\xi)$; write mult_j for the multiplicity above. A *cut* at stage j is a finite set $\mathrm{Cut}_j(\xi)$ of classes such that: (a) it is G_1-stable; (b) its points are integral at every place not above a prime dividing $\mathrm{Nm}\, Q_\xi$; (c) on it mult_j divides a power of $\mathrm{Nm}\, Q_\xi$; (d) $\mathrm{mult}_j(x) \neq 0$ whenever the G_0-orbit of x contains a point with graded lattice and the lattice bounds at stage j. The proof fixes one cut at each stage.

For $1 \le j < m$ the proof shows that a cut exists by choosing, inside the image of $\mathcal{Z}_j K_j^{Y\circ}$ modulo $K_j^Y(\xi)$, one class in each G_0-orbit meeting that image, and taking the G_1-saturation. For x integral off $Q_\xi \cup \bar{Q}_\xi$, such as the points of $\mathcal{Z}_j K_j^{Y\circ}$, it shows that there is n with $(xux^{-1})^{(\mathrm{Nm}\, Q_\xi)^n} \in K_j^{Y\circ}$ for all $u \in K_j^Y(\xi)$.

Problem 46.3.3. Let C meet each G_0-orbit in at most one point, and $\mathrm{Cut} = G_1 \cdot C$. For $c \in C$, $\mathrm{mult}(c) = [\mathrm{Stab}_c : \mathrm{Stab}_c \cap G_1]$ with $\mathrm{Stab}_c := \mathrm{Stab}_{G_0}(c)$ (index 0 if infinite); and $\mathrm{mult}(st) = \mathrm{mult}(t)$ for $s \in G_0$.

Problem 46.3.4. (a) A finite group in which every element has order dividing q^n has order dividing a power of q. (b) For $u \equiv 1 \pmod p$ in $\mathrm{GL}_2(\mathbb{Z}_p)$ and $x = \mathrm{diag}(p^{-2}, 1)$, $xu^p x^{-1}$ is integral; for $p = 3$, $u = \left(\begin{smallmatrix} 4 & 3 \\ 3 & 1 \end{smallmatrix}\right)$, xux^{-1} is not. (c) For the G_1-saturation of the classes chosen in the construction above, every c has $\mathrm{mult}_j(c) \mid (\mathrm{Nm}\, Q_\xi)^n$ for some $n \ge 0$.

Problem 46.3.5. For $0 \le j < m$, if $Q_\xi = \varnothing$, every finite point representing a class of $\mathrm{Cut}_j(\xi)$ lies in $K_j^{Y\circ}$, and $\#\mathrm{Cut}_j(\xi) \le \#\mathrm{GL}_{r+jt}(\mathcal{O}_E/\pi_M) \le M^{f(r+jt)^2} \le M^{fn_m^2}$.

46.4. Summing over the cuts

Fix $1 \le j \le m-1$, and let G_0, G_1 be as in Definition 46.3.2. A level K' here means a subgroup of $K_j^{Y\circ}$ containing a neighbourhood of the identity.

Problem 46.4.1. Let F_∞ be a function on $U(Y_j)_\infty$. There is $k(F_\infty) \in \mathbb{C}$ with the following property, for every level K', every finite G_1-stable set Cut of classes modulo K', every complex function h_1 on $U(Y_j)(\mathbb{A}_f)/K'$ and every continuous left $R_j(F)$-invariant function f_1 on $U(Y_j)(\mathbb{A})$, integrable on $R_j(F)\backslash U(Y_j)(\mathbb{A})$, with

$\mathrm{mult}(x_f) \neq 0$ wherever $f_1(x) \neq 0$. If $\int_{[R_j]} f_1(rx)\,dr = [K_j^{Y\circ} : K']\, F_\infty(x_\infty)\, h_1(x_f K')$ whenever $x_f K' \in \mathrm{Cut}$, then

$$\int_{R_j(F)\backslash U(Y_j)(\mathbb{A})} f_1 = k(F_\infty) \sum_{c \in \mathrm{Cut}} \frac{h_1(c)}{\mathrm{mult}(c)}.$$

Problem 46.4.1 uses quotient integration in stages [Bou, Ch. VII, §2]; *Status*: classical. Problems 46.1.1 and 46.4.1, with Problem 45.1.2 and Problem 46.2.16 for the support, give the following by induction. Fix g, λ, a stage $0 \leq j \leq m-1$, and the grading of Y_{j+1} used in the stage function. For every complex function F_∞ of the tuple of archimedean outer points there is $c_j(F_\infty) \in \mathbb{C}$ with the following property. Let ξ be tame, $\varphi \in S_{\mathrm{ram}}$, z a form on Y_{j+1} as in Problem 45.1.2, and S_1 a complex function of the tuple of finite level classes. Suppose that for every tuple $(g_k, y_k)_k$ with $y_0 \in K_M$ and $y_m = 1$, the integral of $\mathcal{W}_{j+1} z$ over $R_{j+1}(F)\backslash U(Y_{j+1})(\mathbb{A})$ equals $F_\infty((g_k)_k)\, S_1((y_k K_k^Y(\xi))_k)$. Then the integral of $z\,\Theta_{\xi,j+1} \cdots \Theta_{\xi,1} \mathcal{P}_{g,\lambda}\varphi$ over $[U(Y_{j+1})]$ equals

$$c_j(F_\infty) \sum_{c_0 \in \mathrm{Cut}_0(\xi), \ldots, c_j \in \mathrm{Cut}_j(\xi)} \frac{S_1(c_0, \ldots, c_j, 1, 1, \ldots)}{\prod_{k=0}^{j} \mathrm{mult}_k(c_k)},$$

where each 1 denotes the identity class at its stage.

For interlacing highest weights, restriction from $U(n+1)$ to $U(n)$ has multiplicity one [GW, Thm. 8.1.1]; *Status*: classical. For the weights and integral Weyl modules of X_m, Y_m, the proof fixes an integer matrix whose complex span is the space of intertwiners for the block embedding.

Problem 46.4.2. Let l be a linear form on the value space of the algebraic forms on X_m of the prescribed weight. There is $c(l) \in \mathbb{C}$ with the following property, for every such form ψ and every h' with $h'(g_\infty, x) = \langle v^+, \rho(g_\infty^{-1}) P'(x) \rangle$ for an algebraic form P' on Y_m of the weight of the lower chain. Identify Y_m with the complement of the last basis vector of X_m. If $F'(k)$ is the coefficient of ψ at l, evaluated at $\mathrm{diag}(k, 1)$, for every $k \in U(Y_m)(\mathbb{A})$, then

$$\int_{[U(Y_m)]} F'\, \overline{h'} = c(l) \int_{[U(Y_m)]} (\mathrm{res}\psi)\, \overline{h'},$$

where v^+ is the highest-weight vector, ρ the action on the value space, the product is conjugate-linear in the first variable, and on the right $\mathrm{res}\psi$ is read in the same way.

Definition 46.4.3. The *seesaw tensor* of a tame character ξ is

$$\mathrm{ss}_\xi := \sum_{c_0 \in \mathrm{Cut}_0(\xi), \ldots, c_{m-1} \in \mathrm{Cut}_{m-1}(\xi)} \Big(\prod_{j=0}^{m-1} \frac{1}{\mathrm{mult}_j(c_j)} \Big) \big(\phi_\varrho^{\mathrm{ev}}(\xi, c) \otimes \cdots \otimes \phi_0^{\mathrm{ev}}(\xi, c) \big),$$

with $c_m := 1$, in the order of Chapter 45; the evaluated data do not depend on the representatives of the classes.

In the proof $\Theta_{\xi,j+1}^{\top}$ preserves the forms of Problem 45.1.2, and both sides below have the shape of h' in Problem 46.4.2, where pairing with such h' is nondegenerate. So Problems 46.1.1, 46.2.16, 46.4.1 and 46.4.2, with Theorem 45.5.1 and the facts quoted, prove the following.

Theorem 46.4.1. *Let λ be a linear form on the values of source forms and g a point of the archimedean unitary group of Y_0. There is $c' \in \mathbb{C}$, possibly zero, such that for every tame character ξ and every $\varphi \in S_{\mathrm{ram}}$*

$$\Theta_{\xi,m} \cdots \Theta_{\xi,1} \mathcal{P}_{g,\lambda} \varphi = c' \operatorname{res} \Theta_{\xi}^{X}(\mathrm{ss}_{\xi})\varphi,$$

an equality of automorphic forms on Y_m, with res *read in automorphic forms.*

In the Lean formalization. Theorem 46.4.1 is `exists_lowerChainUpTo_poincareAt_eq` in the Lean proof [GL]; the string parts Λ^-, Λ^+ are `latticeMinus`, `latticePlus`; $\mathfrak{u}$ is `twistIdele`; the lattice bounds are `HasLatticeBounds`; a split lattice is `LatticeSplitsAt`; the cuts and multiplicities are `cutPoints` and `cutMultiplicity`; and ss_{ξ} is `seesawDatum`. Problem 46.2.16 is `hasLatticeBounds_of_unfoldStage_ne_zero`. Other assertions attributed to the proof: the one-lift inclusion (in general), the standard image, the string parts of the standard lattice, fact (ii), the construction of a cut, the common conjugate power, the integer branching matrix, the transpose on conjugate-type forms and the comparison by pairing.

We have proved Theorem 46.4.1. Taken as given: the one-lift inclusion and the image of the standard lattice, the string parts of the standard lattice, facts (i) and (ii), the existence of a cut, quotient integration in stages, the branching rule with its integer matrix, and the statements marked "in the proof". c' may vanish, and ss_{ξ} is not yet a combination of translated vacua. The next step needs Definitions 46.3.2 and 46.4.3 and Problems 46.3.4 and 46.3.5.

Hints

§46.1.

46.1.1: Then the transpose relation, the definition of $\mathcal{P}_{g,\lambda}$ and Problem 45.1.2; $\Theta_{\xi,1}^{\top} z$ is $K_0^Y(\xi)$-fixed and the K_M-trace of its conjugate lies in $H(Y_0)$.

§46.2.

46.2.3: Λ is spanned by $(1, \frac{1}{5})$ and $(0, 1)$.
46.2.4: A vector of W pairs with $v \in \Lambda$ as with the projection of v.
46.2.5: Translation invariance of the function.
46.2.9: Apply Problem 46.2.4 to the upper bound at stage j.
46.2.11: Dualize the lower bound; work at a place above N (where $\mathfrak{u}$ is a unit) at which $\mathfrak{u}^j v$ is nonzero in the local quotient; the quotients at w and $\bar{w}$ are dual (Problem 46.2.4). m is even.
46.2.14: Problems 43.5.2 and 43.5.3, and the equivariance $\Theta(\omega^X(g,h)f) = h \circ \Theta(f) \circ g^{-1}$ of each lift. Note $T_w^{N-1} = 1$ on S.
46.2.15: With (g_∞, x) as outer variable of stage j, Theorem 45.5.1 and its proof give $\mathcal{W}_j$ on $R_j(\mathbb{A})(g_\infty, x)$ via the first $j/2$ double lifts.
46.2.16: Strong induction. At stage zero the point $\gamma_f y_0$ has the translate y_0, with lattice $\Lambda(1)$. Later, use (i) and the earlier bounds where the integrand is nonzero, then Problems 46.2.9, 46.2.11 and 46.2.15.

§46.3.

46.3.1: H is transitive on H/H_0.

46.3.3: The classes counted at c form a Stab_c-orbit in G_0/G_1.

46.3.4: (a) Cauchy's theorem. (b) $u^p \equiv 1 \pmod{p^2}$. (c) At a selected class c, $[\mathrm{Stab}_c : \mathrm{Stab}_c \cap G_1] < \infty$; let Stab_c act on $\mathrm{Stab}_c/(\mathrm{Stab}_c \cap G_1)$; Problem 46.3.3.

46.3.5: Reduce integral representatives modulo π_M; $\#\mathcal{O}_E/(\pi_M) = M^f$.

§46.4.

46.4.1: A cutoff $\mathfrak{k} \geq 0$ of $R_j(\mathbb{A})$-orbit integral 1; the Haar measure du on G_0 giving G_1 measure 1; weight $\int_{G_0} \mathfrak{k}(x_\infty, u)\, du$ times $1/\mathrm{mult}(x_f K')$ on the cut, 0 off it. Compare Problem 43.3.2.

46.4.2: Average $v \mapsto l(v)v^+$ over $U(Y_m)_\infty$ (a model: $\frac{1}{4}\sum_{u \in \mu_4} u^{-1}(2+3u) = 3$ extracts one weight), then use branching and Schur orthogonality; $R_m = U(Y_m)$.

References

[Bou] N. Bourbaki, *Intégration*, Ch. VII–VIII, Hermann, Paris, 1963.

[GL] L. Sernau, *GRH for Dirichlet L-functions, in Lean 4*, a shorter rewriting of the Lean proof, text by Claude, `https://github.com/lsernau/grh-lean`, commit `72fead1`, readable edition `grh/`.

[GW] R. Goodman, N. R. Wallach, *Symmetry, Representations, and Invariants*, Grad. Texts in Math. 255, Springer, 2009.

[OM] O. T. O'Meara, *Introduction to Quadratic Forms*, Grundlehren Math. Wiss. 117, Springer, 1963.

[Ti] J. Tits, Reductive groups over local fields, in *Automorphic Forms, Representations and L-Functions*, Proc. Sympos. Pure Math. 33, Part 1, Amer. Math. Soc., 1979, 29–69.

THE SEESAW TENSOR: TRANSLATED VACUA, GLUING AND THE UNIT

Prerequisites. From Chapter 46: the cuts $\mathrm{Cut}_j(\xi)$, their multiplicities mult_j and the seesaw tensor ss_ξ (Definitions 46.3.2 and 46.4.3), the generator ideles ϖ_ξ, ϖ_M (Definition 46.2.6), Problems 46.3.4 and 46.3.5, and Theorem 46.4.1. From Chapter 45: the join $\boxtimes$, the zero term zt, the stacked map A and the evaluated pair datum $\phi_i^{\mathrm{ev}}(\xi, y)$ (Definition 45.4.3). From Chapter 43: the translations $\mathfrak{t} \in \mathcal{T}$, the translated vacua $v_j(\mathfrak{t})$, the data $\mathbf{1}_j(\xi)$ of the lower chain, the levels K_j^X, the restriction res, chain data and the composite lift $B_{\vartheta,\Psi}$ (Section 43.4), and Problems 43.3.3, 43.5.4, 43.5.5. In a tensor over pairs, later pairs stand on the left. From Chapter 12: theta lines and intertwiners (Problems 12.2.1, 12.3.4, 12.5.2, Theorem 12.4.1). From Chapter 34: the frames of the spaces, Q_ξ, $\mathrm{Nm}\, Q_\xi$, the integral vacuum and c_{vac} (Sections 34.3, 34.6, 34.8), and the ring $\mathcal{O}^{[q]}$ of the $z \in \mathbb{C}$ with $|\eta(z)|_\ell \le 1$ for every prime $\ell \nmid q$ and every ring map $\eta\colon \mathbb{C} \to \mathbb{C}_\ell$. The Weil representation over the finite adeles in its Schrödinger and lattice models [We], [MVW, Ch. 2]. As in Chapter 45, $\mathbf{1}_j(\xi)$ is the finite datum of the lift $Y_{j-1} \to Y_j$; ω_j^X is the finite Weil action on the data of the lift $X_j \to X_{j+1}$.

This chapter is the last of the four that prove the seesaw identity, Theorem 43.4.1, which Theorem A uses. Theorem 46.4.1 gives it on automorphic forms, for ramified source forms, with the tensor ss_ξ, a weighted sum over the cuts of evaluated pair data, in place of a chain datum. Which scalar and which common denominator suffice to express ss_ξ in glued vacuum tensors $\mathrm{gl}(\mathfrak{t})$? Three local facts answer this: Fourier inversion on a residue module, the lattice model of the vacuum, and a neighbour lattice at N. One complex unit then works for all twists.

Throughout, ξ is a tame character and $q := \mathrm{Nm}\, Q_\xi$. A finite adelic vector is *integral away from* q if its entries are integral at every finite place not above a prime dividing q.

47.1. Residue modules and Fourier inversion

Definition 47.1.1. Let $(w_\gamma)_{\gamma \in \mathcal{Z}}$ be vectors of a complex vector space, $\mathfrak{d} \ge 1$ an integer and $\mathfrak{s} \ge 0$ real. A vector z is a *combination of the* w_γ, $\gamma \in \mathcal{Z}$, *with denominator* $\mathfrak{d}$ *and size* $\mathfrak{s}$ if $z = \sum_{\gamma \in \mathcal{Z}} r_\gamma w_\gamma$ with finitely many nonzero $r_\gamma \in \mathbb{C}$, $\mathfrak{d}\, r_\gamma \in \mathcal{O}^{[q]}$ for every γ and, if $Q_\xi = \varnothing$, $\sum_\gamma |\sigma(r_\gamma)| \le \mathfrak{s}$ for every $\sigma \in \mathrm{Aut}\,\mathbb{C}$.

Let $\mathfrak{m} \subseteq \mathcal{O}_E$ be a nonzero ideal, $\mathsf{A}_\mathfrak{m} := (\mathcal{O}_E/\mathfrak{m})^n$, $\psi_\mathfrak{m}$ a primitive additive character of $\mathcal{O}_E/\mathfrak{m}$, $\mathfrak{y} \cdot \mathfrak{b} := \sum_k \mathfrak{y}_k \mathfrak{b}_k$, and $\chi_\mathfrak{b}(\mathfrak{y}) := \psi_\mathfrak{m}(\mathfrak{y} \cdot \mathfrak{b})$. For the next problem alone, take the additive group $\mathbb{Z}/5\mathbb{Z}$ and characters with values in the fifth roots of unity of $\mathbb{F}_{11}$.

Problem 47.1.1. The class of 3 in $\mathbb{F}_{11}$ has order 5, and $\sum_{l=0}^{4} 3^{\,l(j-2)}$ is $0, 0, 5, 0, 0$ in $\mathbb{F}_{11}$ for $j = 0, \dots, 4$.

Date: November 26, 2026.

At the places of $\mathfrak{m} := (\pi_M)\prod_{w\in Q_\xi} w$ (a modulus prime to its conjugate) the datum $\mathbf{1}_j(\xi)$ is the operator of the Schrödinger model attached to the point mass at the class $\mathfrak{i}\in \mathsf{A}_\mathfrak{m}$ of the inclusion matrix, $n=\dim Y_{j-1}\dim Y_j$, applied to the vacuum vac; at the other finite places it is the vacuum. Here $\psi_\mathfrak{m}(u \bmod \mathfrak{m})=\psi_0(\varpi_\xi^{-1}u)$ for integral finite adeles u, with ϖ_ξ the generator idele of $\mathfrak{m}$ of Definition 46.2.6 and ψ_0 the self-dual character of the finite adeles; a residue function is read on the reduction at the places of $\mathfrak{m}$, and is zero off the integral box there. The operator of $\chi_\mathfrak{b}$, on vectors fixed by the integral translations at the places of $\mathfrak{m}$ and their conjugates (as vac is), is the Heisenberg translation $\mathrm{Heis}(t_\mathfrak{b})$, where $t_\mathfrak{b}$ is the complex conjugate of the part at the places of $\mathfrak{m}$ of $\varpi_\xi^{-1}\tilde{u}_\mathfrak{b}$, $\tilde{u}_\mathfrak{b}$ any integral lift of $\mathfrak{b}$.

Problem 47.1.2. The point mass at $\mathfrak{i}$ is $|\mathsf{A}_\mathfrak{m}|^{-1}\sum_\mathfrak{b}\psi_\mathfrak{m}(-\mathfrak{i}\cdot\mathfrak{b})\,\chi_\mathfrak{b}$. Hence $\mathbf{1}_j(\xi)=|\mathsf{A}_\mathfrak{m}|^{-1}\sum_\mathfrak{b}\psi_\mathfrak{m}(-\mathfrak{i}\cdot\mathfrak{b})\,\mathrm{Heis}(t_\mathfrak{b})\mathrm{vac}$, and for every $\sigma\in\mathrm{Aut}\,\mathbb{C}$ the absolute values of the σ-conjugates of these coefficients sum to 1.

Problem 47.1.3. Each $\bar\pi_M t_\mathfrak{b}$ is integral away from q, and $\#(\mathcal{O}_E/\pi_M\mathcal{O}_E)^n$ divided by $|\mathsf{A}_\mathfrak{m}|$ is $q^{-n}\in\mathcal{O}^{[q]}$. So $\mathbf{1}_j(\xi)$ is a combination of the $\mathrm{Heis}(\mathfrak{z})\mathrm{vac}$, over the $\mathfrak{z}$ with $\bar\pi_M\mathfrak{z}$ integral away from q, with denominator $\#(\mathcal{O}_E/\pi_M\mathcal{O}_E)^n$ and size 1.

47.2. The lattice model

Let V be $\mathrm{Hom}(Y_{j-1},Y_j)$ or $\mathrm{Hom}(X_j,X_{j+1})$, with its standard lattice Λ in the finite adelic frame of Section 34.3, finite Heisenberg translations $\mathrm{Heis}(\mathfrak{z})$, Weil representation ω and vacuum vac. For background on the Weil representation and its models see [We], [MVW, Ch. 2]; we use the following, in the normalization of [GL]. (L1) $\mathrm{Heis}(\mathfrak{z})\mathrm{vac}=\mathrm{vac}$ for $\mathfrak{z}\in\Lambda$, and the vectors of the finite part fixed by all these translations are the multiples of vac (compare Problem 12.2.1). (L2) $\mathrm{Heis}(\mathfrak{z})\mathrm{Heis}(\mathfrak{z}')=\zeta\,\mathrm{Heis}(\mathfrak{z}+\mathfrak{z}')$, where ζ is a root of unity depending only on $\sum_k\bar{\mathfrak{z}}'_k\mathfrak{z}_k$ and equal to 1 when this sum is 0. (L3) $\omega(h)\mathrm{Heis}(\mathfrak{z})=\mathrm{Heis}(h\mathfrak{z})\,\omega(h)$ for $h\in U(V)(\mathbb{A}_f)$. (L4) $\omega(h)\mathrm{vac}=c_h\sum_{\mathfrak{z}\in\Lambda/(\Lambda\cap h^{-1}\Lambda)}\mathrm{Heis}(h\mathfrak{z})\mathrm{vac}$ with $c_h\neq 0$; compare the intertwiner defined in Section 12.3 and evaluated in Problem 12.3.4. The scalar c_h is the Weil multiplier divided by its squared absolute value. If h is integral away from q, then $|\eta(c_h)|_\ell=1$ for every prime $\ell\nmid q$ and every ring map $\eta\colon\mathbb{C}\to\mathbb{C}_\ell$; if h is integral at every finite place, then $c_h=1$. *Status*: we use the classical lattice model in the normalization of [GL], which proves (L1)–(L4) and the multiplier bounds.

Problem 47.2.1. Let $h\in U(V)(\mathbb{A}_f)$. A vector f of the finite part with $\mathrm{Heis}(h\mathfrak{z})f=f$ for all $\mathfrak{z}\in\Lambda$ is a multiple of $\omega(h)\mathrm{vac}$.

Problem 47.2.2. Let $h\in U(V)(\mathbb{A}_f)$ be integral away from q, and let $\bar\pi_M\mathfrak{z}_0$ be integral away from q. Then $\omega(h)\mathrm{Heis}(\mathfrak{z}_0)\mathrm{vac}$ is a combination of the $\mathrm{Heis}(\mathfrak{z})\mathrm{vac}$, over the $\mathfrak{z}$ with $\bar\pi_M\mathfrak{z}$ integral away from q, with denominator 1 and size 1.

The action ω_j on the data of the lower chain is that of Problem 47.2.2 times a determinant-character factor, which at points integral away from q has ℓ-adic norm 1 for $\ell\nmid q$ and absolute value 1 under every $\sigma\in\mathrm{Aut}\,\mathbb{C}$. So the moved data $\mathbf{1}_j(\xi)^y$ at points integral away from q keep the denominators of Problem 47.1.3 and size 1. If the two translations become integral away from q after multiplication by $\bar\pi_M$, the join of their translated vacua is a root of unity times a translated vacuum on $\mathrm{Hom}(Y_{2i+1},Y_{2i}^-\oplus Y_{2i+2})$, whose translation becomes integral away from q after multiplication by π_M on the first block and by $\bar\pi_M$ on the second. Evaluation

translates the joined datum by A_f, takes its finite zero term along the isotropic part I of the splitting, and applies $\boxtimes^{-1}$ on the definite spaces.

Problem 47.2.3. Let F be a nonarchimedean local field with integers $\mathcal{O}_F$, W a finite-dimensional F-vector space with a nondegenerate symmetric or alternating bilinear form, $L \subset W$ a lattice with $L = \{x : \langle x, L\rangle \subseteq \mathcal{O}_F\}$, and $I \subseteq W$ an isotropic subspace. Then the image of $L \cap I^{\perp}$ in $I^{\perp}/I$ is a lattice equal to its own dual.

Let L be the standard lattice of $\mathrm{Hom}(Y_{2i+1}, Y_{2i}^{-} \oplus Y_{2i+2})$ in its finite adelic frame. The proof identifies the reduced lattice with a finite adelic unitary image of the standard lattice in the quotient and deduces its self-duality for the pairing $(x, w) \mapsto \psi_0(\bar{x}^t w)$; Problem 47.2.3 is the analogue at one place. The image of $L \cap I^{\perp}$ in $I^{\perp}/I$, identified by the splitting with the finite adelic space of $\mathrm{Hom}(X_{2i+1}, X_{2i}^{-} \oplus X_{2i+2})$, is the *zero-term lattice* of pair i. The zero term of the vacuum on the first Hom space is a number $c_i' \neq 0$ times the sum of the translates of the vacuum on the second by representatives of the zero-term lattice modulo its intersection with the standard lattice there.

47.3. The neighbour at N

Which lattice is the zero-term lattice? Let P be the set of places $w \mid \pi_N$ and $\bar{P}$ the set of their conjugates; they are disjoint, with union the set of places above N. Let $\mathbf{1}_P$ be the finite adele equal to 1 on P and 0 elsewhere, π_P the finite idele equal to π_N on P, to $\bar{\pi}_N^{-1}$ on $\bar{P}$ and to 1 elsewhere, and u_{-1} a fixed unit of the integral finite adeles with $u_{-1}\bar{u}_{-1} = -1$. For a pair i let e, e'' be the last basis vectors of X_{2i} and X_{2i+2} in $X_{2i}^{-} \oplus X_{2i+2}$, and put $e_P := e + \bar{u}_{-1}\bar{\mathbf{1}}_P e''$. For columns write $z^* := \bar{z}^t$.

Problem 47.3.1. Over a commutative ring with involution, let z be a column with $z^*z = 1$, δ a scalar and $\gamma := 1 + (\delta - 1)zz^*$. Then $\gamma z = \delta z$, $\gamma z' = z'$ when $z^*z' = 0$, and $\gamma^*\gamma = 1$ if and only if $\delta\bar{\delta} = 1$. Moreover $e_P^* e_P = 1$ and $\pi_P \bar{\pi}_P = 1$.

Definition 47.3.1. The *neighbour lattice* of pair i is the image of the standard lattice of $\mathrm{Hom}(X_{2i+1}, X_{2i}^{-} \oplus X_{2i+2})$ under the matrix acting on the target as $\gamma_P := 1 + (\pi_P - 1)e_P e_P^*$ at the places above N, and at the other finite places as the identity for $i < \varrho$; for $i = \varrho$, at these places it scales the last row of X_m by $\varpi_M/\bar{\varpi}_M$ and fixes the other rows, ϖ_M the generator idele of (π_M) of Definition 46.2.6.

For a local example take $N = 5$ and the split algebra $\mathbb{Q}_5 \times \mathbb{Q}_5$, with factors indexed by $w \in P$ and $\bar{w}$ and conjugation exchanging them; take $\pi_N = (5, 1)$, $u_{-1} = (1, -1)$, $\mathbf{1}_P = (1, 0)$, and keep the rows e, e''.

Problem 47.3.2. In this model $e_P = \big((1,1),(0,1)\big)$, $\pi_P = (5, \frac{1}{5})$, and the components of γ_P at w and $\bar{w}$ are $G = \left(\begin{smallmatrix} 5 & 4 \\ 0 & 1 \end{smallmatrix}\right)$ and $G' = \left(\begin{smallmatrix} 1/5 & 0 \\ -4/5 & 1 \end{smallmatrix}\right)$, with $G^t G' = 1$.

To a residue modulo N at w, with representative $y \in \{0, \ldots, N-1\}$, the proof attaches the translation supported at $\bar{w}$ with entries $u_{-1}\bar{y}/N$ in row e and $-\bar{y}/N$ in row e'', where $\bar{y}/N$ is the conjugate of the adele equal to y/N at w and 0 elsewhere.

Problem 47.3.3. G is integral, and $G'\mathbb{Z}_5^2 + \mathbb{Z}_5^2 = \mathbb{Z}_5^2 + \mathbb{Z}_5 \cdot \frac{1}{5}(1,1)^t$; the five classes modulo $\mathbb{Z}_5^2$ are those of $\frac{1}{5}(y,y)^t$, $y = 0, \ldots, 4$. The translation attached to y is $-\frac{1}{5}(y,y)^t$ at $\bar{w}$, so one residue labels both rows.

Black box. For every pair i of the proof the zero-term lattice is the neighbour lattice; the lift of its columns is integral and orthogonal to the finite stacked map. We take the lattice equality and the two properties of the lift from [GL].

A representative of the neighbour lattice modulo its integral points is indexed by one residue modulo N for each basis vector of X_{2i+1} and each $w \in P$, specifying both rows e, e'', and one class away from N. Under the join on the definite spaces, Gl_i corresponds to the sum of the Heisenberg operators of these residue translations. Let C_i be c_i' times the number of classes away from N; it depends only on the data. The proof obtains: for n prime to N and $\mathfrak{z}$ on $\mathrm{Hom}(Y_{2i+1}, Y_{2i}^{-} \oplus Y_{2i+2})$ with π_M times its first block and $\bar{\pi}_M$ times its second integral away from n, the evaluation of $\mathrm{Heis}(\mathfrak{z})\mathrm{vac}$ is a finite sum of the vectors $C_i\,\mathrm{Gl}_i(\mathrm{Heis}(t_1)\mathrm{vac} \otimes \mathrm{Heis}(t_2)\mathrm{vac})$, with $\bar{\pi}_M t_1$, $\bar{\pi}_M t_2$ integral away from n, whose coefficients become integral away from n after multiplication by $\#(\mathcal{O}_E/\pi_M\mathcal{O}_E)^{(n_{2i}+n_{2i+2})n_{2i+1}}$ and have σ-conjugates of absolute sum at most 1 for every $\sigma \in \mathrm{Aut}\,\mathbb{C}$.

47.4. Invariance

Problem 47.4.1. Let sw exchange the coordinates of $\mathbb{Q}^2$. For $v = (1,2)^t$ and $v' = (3,-1)^t$, the sum of the matrices in the orbit of vv'^t under $X \mapsto \mathrm{sw}\,X\,\mathrm{sw}^t$ is $\left(\begin{smallmatrix} 1 & 5 \\ 5 & 1 \end{smallmatrix}\right)$ and is fixed by this action.

Problem 47.4.2. Let a group H act on finite sets $\mathcal{X}_0, \dots, \mathcal{X}_{m-1}$ and linearly on a complex vector space; let $\mathrm{mult}_j \colon \mathcal{X}_j \to \mathbb{Z}_{>0}$ be H-invariant and $\mathcal{E}$ a function on $\mathcal{X}_0 \times \cdots \times \mathcal{X}_{m-1}$ with $\mathcal{E}(bc) = b\,\mathcal{E}(c)$ for $b \in H$. Then $\sum_c \prod_j \mathrm{mult}_j(c_j)^{-1}\mathcal{E}(c)$ is fixed by H.

In the proof, let $b_j \in K_j^X$ for $j < m$ and $b_m := 1$. For $j < m$ the image of b_j in $U(Y_j)(\mathbb{A}_f)$ lies in the finite Bessel subgroup, permutes $\mathrm{Cut}_j(\xi)$ and keeps the multiplicities; and evaluation is equivariant: the evaluated pair datum at the translated points is $\omega_{2i}^X(b_{2i}, b_{2i+1}) \otimes \omega_{2i+1}^X(b_{2i+1}, b_{2i+2})$ applied to $\phi_i^{\mathrm{ev}}(\xi, y)$. By Problem 47.4.2, ss_ξ is fixed by $\bigotimes_j \omega_j^X(b_j, b_{j+1})$ for all such b.

47.5. Denominators and sizes

Definition 47.5.1. The *residue count* is $c_{\mathrm{res}} := M^{f n_m^2}$.

Since q is prime to N, the pair evaluation applies with $n = q$. Thus for $0 \le i \le \varrho$ and points y integral away from q, $\phi_i^{\mathrm{ev}}(\xi, y)$ is a combination of the vectors $C_i\,\mathrm{Gl}_i(\mathrm{Heis}(t_1)\mathrm{vac} \otimes \mathrm{Heis}(t_2)\mathrm{vac})$, over t_1, t_2 with $\bar{\pi}_M t_1$, $\bar{\pi}_M t_2$ integral away from q, with denominator $\#(\mathcal{O}_E/\pi_M\mathcal{O}_E)^{\mathfrak{e}_i}$ and size 1, where $\mathfrak{e}_i := \dim Y_{2i} \dim Y_{2i+1} + \dim Y_{2i+1} \dim Y_{2i+2} + (n_{2i} + n_{2i+2})n_{2i+1}$. The proof states this with the uniform denominator c_{res}^4.

Problem 47.5.1. Substituting $1, 2, 3$ for the three Y-dimensions and for the three X-ranks in $\mathfrak{e}_i$ gives $16 \le 4 \cdot 3^2$. For the ranks of the proof, $\mathfrak{e}_i \le 4n_m^2$, so $\#(\mathcal{O}_E/\pi_M\mathcal{O}_E)^{\mathfrak{e}_i}$ divides c_{res}^4.

Problem 47.5.2. Let z be a combination of the w_γ, $\gamma \in \mathcal{Z}$, with denominator $\mathfrak{d}$ and size $\mathfrak{s}$, and let each w_γ be a combination of the $w'_{\gamma'}$, $\gamma' \in \mathcal{Z}'$, with denominator $\mathfrak{d}'$ and size $\mathfrak{s}'$. Then z is a combination of the $w'_{\gamma'}$ with denominator $\mathfrak{d}\mathfrak{d}'$ and size $\mathfrak{s}\mathfrak{s}'$. If z_k is a combination of the $w_{k,\gamma}$ with denominator $\mathfrak{d}_k$ and size $\mathfrak{s}_k$ $(k < l)$, then $z_{l-1} \otimes \cdots \otimes z_0$ is a combination of the $w_{l-1,\gamma_{l-1}} \otimes \cdots \otimes w_{0,\gamma_0}$ with denominator $\prod_k \mathfrak{d}_k$ and size $\prod_k \mathfrak{s}_k$.

The integral vacuum of $\mathrm{Hom}(X_j, X_{j+1})$ is $c_{\mathrm{vac}}^{n_j n_{j+1}}\mathrm{vac}$ (Section 34.8). Put

$$c_{\mathrm{gl}} := \prod_{i=0}^{\varrho} \frac{C_i}{c_{\mathrm{vac}}^{n_{2i}n_{2i+1}}\, c_{\mathrm{vac}}^{n_{2i+1}n_{2i+2}}},$$

a nonzero number. By Problems 47.5.1 and 47.5.2, for points y integral away from q the tensor $\bigotimes_{i=0}^{\varrho}\phi_i^{\mathrm{ev}}(\xi, y)$ is a combination of the $c_{\mathrm{gl}}\,\mathrm{gl}(\mathfrak{t})$, over the $\mathfrak{t}$ with every $\bar\pi_M\mathfrak{t}_j$ integral away from q, with denominator c_{res}^{2m} and size 1.

Problem 47.5.3. Each $\mathrm{mult}_j(c)^{-1}$, $c \in \mathrm{Cut}_j(\xi)$, lies in $\mathcal{O}^{[q]}$, and if $Q_\xi = \varnothing$, then $\sum_{c_0,\dots,c_{m-1}}\prod_j \mathrm{mult}_j(c_j)^{-1} \le c_{\mathrm{res}}^m$. Hence ss_ξ is a combination of the $\bigotimes_i \phi_i^{\mathrm{ev}}(\xi, c)$, over tuples c of cut points with representatives integral away from q, with denominator 1 and size c_{res}^m.

The pair evaluation, the tensor bound above and Problem 47.5.3, followed by substitution (Problem 47.5.2), give the following theorem.

Theorem 47.5.1. *There is $c_{\mathrm{gl}} \in \mathbb{C}$, depending only on the data, such that for every tame character ξ, with $q = \mathrm{Nm}\,Q_\xi$, the tensor ss_ξ is a combination of the $c_{\mathrm{gl}}\,\mathrm{gl}(\mathfrak{t})$, over the $\mathfrak{t} \in \mathcal{T}$ with every $\bar\pi_M\mathfrak{t}_j$ integral away from q, with denominator c_{res}^{2m} and size c_{res}^m: there are $r_{\xi,\mathfrak{t}} \in \mathbb{C}$, finitely many nonzero, with*

$$\mathrm{ss}_\xi = \sum_{\mathfrak{t}} r_{\xi,\mathfrak{t}}\, c_{\mathrm{gl}}\,\mathrm{gl}(\mathfrak{t}), \qquad c_{\mathrm{res}}^{2m} r_{\xi,\mathfrak{t}} \in \mathcal{O}^{[q]},$$

$$Q_\xi = \varnothing \implies \sum_{\mathfrak{t}} |\sigma(r_{\xi,\mathfrak{t}})| \le c_{\mathrm{res}}^m \text{ for all } \sigma \in \mathrm{Aut}\,\mathbb{C}.$$

47.6. The unit and the seesaw identity

By Theorem 46.4.1 and Theorem 47.5.1, for every ramified source form φ the composite of the lower lifts on automorphic forms applied to $\mathcal{P}_{g,\lambda}\varphi$ is $c'c_{\mathrm{gl}}/c_{\mathrm{res}}^{2m}$ times $\mathrm{res}\,\Theta_\xi^X\big(\sum_{\mathfrak{t}} c_{\mathrm{res}}^{2m} r_{\xi,\mathfrak{t}}\mathrm{gl}(\mathfrak{t})\big)\varphi$, and these coefficients lie in $\mathcal{O}^{[q]}$. The scalar may be 0.

Problem 47.6.1. Let $c' = 2$, $c_{\mathrm{gl}} = 3$, denominator 4 and $r = (\frac14, -\frac12)$. Applying Problem 43.5.4 to the scalar $c'c_{\mathrm{gl}}/4$ gives $u = \frac23$ and $c = u^{-1} = \frac32$. The cleared vector $\Psi = 4r$ is $(1, -2)$ and satisfies $c\Psi = c'c_{\mathrm{gl}}r = (\frac32, -3)$. If $c' = 0$, the same identity holds with $c = 1$ and $\Psi = 0$.

Problem 47.6.2. Let $\mathcal{V}$ be the set of finite places above the primes dividing Mq, and $\mathbf{1}_{\mathcal{V}}\mathfrak{t} := (\mathbf{1}_{\mathcal{V}}\mathfrak{t}_j)_j$. If every $\bar\pi_M\mathfrak{t}_j$ is integral away from q, then $v_j(\mathbf{1}_{\mathcal{V}}\mathfrak{t}) = v_j(\mathfrak{t})$ for every j, so $\mathrm{gl}(\mathbf{1}_{\mathcal{V}}\mathfrak{t}) = \mathrm{gl}(\mathfrak{t})$.

Problem 47.6.3. Let the tame character ξ be a twist ϑ, with the nonzero c_{gl} chosen above, coefficients $r_{\vartheta,\mathfrak{t}}$ for this choice in Theorem 47.5.1, and $\mathcal{V}$ as in Problem 47.6.2 for $q = \mathrm{Nm}\,Q_\vartheta$. If $c' \neq 0$, put $\Psi(\mathfrak{t}) := c_{\mathrm{res}}^{2m}\sum r_{\vartheta,\mathfrak{t}'}$ over the $\mathfrak{t}'$ with $\mathbf{1}_{\mathcal{V}}\mathfrak{t}' = \mathfrak{t}$; otherwise $\Psi := 0$. Then Ψ is a chain datum for ϑ; for $Q_\vartheta = \varnothing$ its size is at most $c_{\mathrm{res}}^{2m}c_{\mathrm{res}}^m = M^{3fmn_m^2}$.

Theorem 46.4.1, Theorem 47.5.1, the invariance of ss_ξ, Problems 43.5.4, 47.6.2 and 47.6.3, and the passage from automorphic to algebraic forms on Y_m prove Theorem 43.4.1, with $c = c'c_{\mathrm{gl}}/c_{\mathrm{res}}^{2m}$ if $c' \neq 0$ and $c = 1$, $\Psi = 0$ otherwise (compare Problem 43.5.5). Passage to algebraic forms on Y_m carries the restriction on the right of the automorphic identity to the restriction in $B_{\vartheta,\Psi}$. Nothing is said about the size of c.

Definition 47.6.1. For $\mathfrak{t} \in \mathcal{T}$ let $\mathrm{pl}_0(\mathfrak{t}) := 1 \in \mathbb{C}$ and $\mathrm{pl}_{i+1}(\mathfrak{t}) := \big(v_{2i}(\mathfrak{t}) \otimes v_{2i+1}(\mathfrak{t})\big) \otimes \mathrm{pl}_i(\mathfrak{t})$ for $0 \le i \le \varrho$. The *plain vacuum tensor* is $\mathrm{pl}(\mathfrak{t}) := \mathrm{pl}_{\varrho+1}(\mathfrak{t})$.

If every $\mathfrak{t}_j$ vanishes at the places above N, then $\mathrm{gl}(\mathfrak{t})$ is the sum of the $\mathrm{pl}(\mathfrak{t} + \mathfrak{g}_y)$ over the residues y of the gluings, $\mathfrak{g}_y$ the tuple of their translations; Chapter 48 uses this expansion of the composite lift.

We have proved Theorem 47.5.1 and with it the seesaw identity. Taken as given: the Schrödinger and lattice models with the multiplier bounds, and the zero-term lattice, its lift and the pair evaluation quoted above.
In the Lean formalization. Declaration names omit the prefix `New.`.
Theorem 47.5.1 is `Data.exists_isAdmissibleCombination_seesawDatum` in the Lean proof [GL]. Definition 47.1.1 specializes `Seesaw.IsAdmissibleCombination` to $q = \mathrm{Nm}\, Q_\xi$, the size condition $Q_\xi = \varnothing$, positive denominators and nonnegative bounds. Definition 47.5.1 is `Data.residueMatrixCount`; Definition 47.6.1 and $\mathrm{gl}(\mathfrak{t})$ are `Data.ungluedVacuum` and `Data.gluedVacuum`. The uniform bound for one evaluated pair is `Data.exists_isAdmissibleCombination_evaluatedDatum`, the bound for their tensor
`Data.exists_isAdmissibleCombination_gluedVacuum`, and joint invariance `Data.isInvariant_seesawDatum`. The zero-term lattice equality is `Seesaw.DoubleLiftData.zeroTermLattice_splitting_eq`. Theorem 43.4.1 is `Data.seesaw_identity`. The other statements read from the proof are, in [GL] (paths relative to `grh/src/`): for the residue operator
`Lib/Weil/DualPair/Defs.lean` (587, 625) and
`New/UpperBound/Objects/Rows.lean` (377); for (L1)–(L4)
`Lib/Weil/Construction/VacuumProjections.lean` (102, 203, 450, 755, 928), with the multiplier bounds in
`New/UpperBound/Seesaw/AdmissibleCombinations.lean` (451) and
`Lib/Weil/Construction/FiniteMultiplier.lean` (948, 979). In
`New/UpperBound/Seesaw/`: the moved and joined data `GoodDatum.lean` (267, 370); the evaluation, the reduced lattice and the equivariance `EdgePairEvaluation.lean` (487, 514, 853, 988); the zero term of the vacuum, the lift and the pair evaluation `AdmissibleEvaluation.lean` (248, 329, 565, 596); the residue translations and representatives `NeighbourLattice.lean` (171, 996); the gluing `NeighbourVacuum.lean` (241); the rank bound `GoodDatum.lean` (421); the inputs to invariance `Cut.lean` (173, 182, 199). The plain expansion is in `New/UpperBound/Divisibility/ChainDatumExpansion.lean` (233).

Hints

§47.1.

47.1.2: Orthogonality of the characters of $\mathsf{A}_{\mathfrak{m}}$; the operator depends linearly on the function. Compare Problem 43.3.3.

47.1.3: $\mathfrak{m}$ is the product of the coprime ideals (π_M) and $\prod_{w \in Q_\xi} w$.

§47.2.

47.2.1: Move the problem to the standard lattice.

47.2.2: (L2)–(L4). If $Q_\xi = \varnothing$, then $h\Lambda = \Lambda$.

47.2.3: Compute the annihilator of $L \cap I^\perp$ in W; $L \cap I^\perp$ is a direct summand of L.

§47.3.

47.3.1: Expand $\gamma^*\gamma$. $\mathbf{1}_P\bar{\mathbf{1}}_P = 0$.

§47.4.

47.4.2: Substitute $c \mapsto bc$.

§47.5.

47.5.1: All ranks are at most n_m, and $\#(\mathcal{O}_E/\pi_M\mathcal{O}_E) = M^f$.

47.5.2: $\mathcal{O}^{[q]}$ is a ring; the triangle inequality gives the sizes.

47.5.3: Problems 46.3.4 and 46.3.5.

§47.6.

47.6.2: Split $\mathfrak{t}_j$ into its parts on $\mathcal{V}$ and off $\mathcal{V}$. Which part fixes the vacuum, and what is their Heisenberg phase?

47.6.3: Problems 47.6.2 and 47.4.2; regroup equal indices.

References

[GL] L. Sernau, *GRH for Dirichlet L-functions, in Lean 4*, a shorter rewriting of the Lean proof, text by Claude, `https://github.com/lsernau/grh-lean`, commit `72fead1`, readable edition `grh/`.

[MVW] C. Mœglin, M.-F. Vignéras and J.-L. Waldspurger, *Correspondances de Howe sur un corps p-adique*, Lecture Notes in Math. 1291, Springer, 1987.

[We] A. Weil, *Sur certains groupes d'opérateurs unitaires*, Acta Math. **111** (1964), 143–211.

DIVISIBILITY OF THE COMPOSITE LIFT

Prerequisites. Chapter 33: the parameters, the field E and its places (Section 33.2), the scales and ranks (Section 33.3), the weights κ and the prime sums s_{fin} (Section 33.4), and the source forms, twists and integral vacuum (Chapter 34). Chapter 43: chain data and the composite lift $B_{\vartheta,\Psi}$. The stage bound of one lift, Theorem 50.4.4, is used here and proved in Chapter 50, which follows; its shape in the plane is Theorem 16.3.1. The colength of Chapter 5, Section 5.4, in the form of Chapter 18, Section 18.6; the elementary divisor theorem, Theorem 48.5.1, is stated in Section 48.5. The step at a full mark, Theorem 53.4.1, and the case of the level prime, Theorem 52.4.1, are used here and proved in Chapters 53 and 52, which follow. Modules over a valuation ring; $\mathbb{C}_p$, with $|p|_p = p^{-1}$.

Theorem A needs a valuation bound for the composite lift $B_{\vartheta,\Psi}$ at every prime p. The divisibility predicted at p is a number $\mathrm{gain}(p)$. It holds up to an error, on a submodule of colength at most the error times $D_X = \dim_{\mathbb{C}} S$, and the errors, weighted by $\log p$, add up to at most $U = fa\log^3 b$. We follow the four cases of the proof.

- Read from the proof: the expansion of a chain datum into a weak one (Theorem 48.3.4), inputs (i) and (ii) of Section 48.3, and the colength estimate for one marked prime (from Theorem 48.5.1, itself read from the proof).
- Developed in the chapters that follow: the bound for one lift at a prime $p < x_1$ with $\chi_K(p) \neq 1$, input (iii) of Section 48.3, is Theorem 50.4.4, and Chapter 49 treats the count behind it; the primes above an exceptional prime, the existence of a full mark and the valuation bound at a full mark are in Chapter 53 (Theorem 53.4.1); the level prime is Chapter 52 (Theorem 52.4.1).
- Derived here from these: Theorems 48.7.1 and 48.7.2.

48.1. The gain at a prime

We use q_0, d, K, χ_K, q_1, E, Φ, f, $[\nu]$, Φ_a, Φ_b, the weight κ and s_{fin} as in Chapter 33; recall that $a/x_1 \le \kappa(\sigma) \le b \le a$ and that q_1 is q_0 times a product of powers of 2 and 3. For a natural number p, let $c_p = 1/2$ if $p = d$ and $c_p = 1$ otherwise, and let I_p be the set of integers $e \ge 1$ such that $p = d$, or $\chi_K(p) = -1$ and e is odd. For $y \in \mathbb{R}$ and $\sigma \in \Phi$, with $z_+ = \max(z, 0)$, the *local prime sum* and the *gain* are

$$s_{\mathrm{fin},p}(y,\sigma) = c_p \sum_{e\in I_p} \Big(\frac{y}{p^e} - \kappa([-p^e]\sigma)\Big)_+, \qquad \mathrm{gain}(p) = m\Big(\sum_{\tau\in\Phi_a} s_{\mathrm{fin},p}(a,\tau) + k\sum_{\sigma\in\Phi} s_{\mathrm{fin},p}(\kappa(\sigma),\sigma)\Big).$$

The first sum records the a columns of height one at each a-place; the second counts the local term at $\kappa(\sigma)$ with multiplicity k at every place.

Problem 48.1.1. Every prime dividing q_1 splits in K. Hence a prime $p \neq d$ with $\chi_K(p) \neq 1$ is prime to q_1, and $[-p^e]$ is the place of the class of $-p^e$.

Date: November 26, 2026.

Problem 48.1.2. Let $p \neq d$ be inert in K, $\tau \in \Phi_a$, and suppose that $\kappa([-p^e]\tau) = w$ for every positive odd integer e. Then $s_{\mathrm{fin},p}(a,\tau) = \sum_{e\geq 1,\ e\ \mathrm{odd}} (a/p^e - w)_+$, the first sum of Theorem 16.3.1 without the integer parts. Evaluated at $p = 13$, $a = 13^4$ and $w = 1$, the sum is 2208.

Problem 48.1.3. $\mathrm{gain}(p) = 0$ if $\chi_K(p) = 1$ or $p \geq x_1$.

Problem 48.1.4. Let p be prime and $y \leq a$. The terms of $s_{\mathrm{fin}}(y,\sigma)$ with ν a power of p add up to $2\, s_{\mathrm{fin},p}(y,\sigma)\log p$.

Let Π be the set of primes $p < x_1$ with $\chi_K(p) \neq 1$. Summing over primes, $2\sum_{p\in\Pi} \mathrm{gain}(p)\log p = m\sum_{\tau\in\Phi_a} s_{\mathrm{fin}}(a,\tau) + mk\sum_{\tau\in\Phi} s_{\mathrm{fin}}(\kappa(\tau),\tau)$; the contribution of the powers of p to the right-hand side is $2\,\mathrm{gain}(p)\log p$.

48.2. Collisions

In this section p is a prime. For a set $\Phi' \subseteq \Phi$, a *collision outside* Φ' is a pair (τ, e) with $e \in I_p$ and $\tau, [-p^e]\tau \in \Phi_a \smallsetminus \Phi'$; the *collision sum* is

$$C_p(\Phi') = \sum_{(\tau,e)\ \text{collision outside}\ \Phi'} \frac{a}{p^e}.$$

Let o_p be the order of the image of $[-p]$ in $(\mathbb{Z}/q_0)^\times$, and r_p the least integer $h \geq 0$ with $m \leq p^h$. The prime p is *exceptional* if $\chi_K(p) = -1$, $p \not\equiv \pm 1 \pmod m$, and o_p is odd with $o_p \leq r_p$. The *unit of loss* at p is

$$L_p = f(\log b)^2\, \frac{a}{p} \cdot \begin{cases} m & \text{if } m \mid p-1 \text{ or } m \mid p+1, \\ 1 & \text{otherwise.} \end{cases}$$

Problem 48.2.1. Let $\chi_K(p) \neq 1$ and let (τ, e) be a collision outside some Φ'. Then $p \neq d$, e is odd, and $o_p \mid e$; in particular o_p is odd.

Problem 48.2.2. Let $q_0 = 18480$ and let p be a prime not dividing q_0. If o_p is odd, then $p \equiv -1 \pmod{240}$ and $o_p \in \{1,3,5,15\}$. For $d = 138599$, the inert prime 13 has $o_{13} = 20$. Among the primes inert in $\mathbb{Q}(\sqrt{-138599})$, the least with o_p odd is 479, with $o_{479} = 15$, and the least with $o_p = 1$ is 55439.

Problem 48.2.3. Let $o \geq 0$ be an integer. If every collision (τ, e) outside Φ' has $e \geq o$, then $C_p(\Phi') \leq 2fa/p^o$.

From Chapter 33 we use $(\log b)^2 \geq 15$ and $m \geq 2$.

Problem 48.2.4. Let $p < x_1$ be a prime with $\chi_K(p) \neq 1$ that is not exceptional. Then $m\, C_p(\varnothing) \leq L_p$.

Problem 48.2.5. Let p be exceptional with $o_p = 1$, and let $h_0 = \#(\mathbb{Z}/q_0)^\times$. Then $\#\Phi_a = f/h_0$ and $m\, C_p(\varnothing) \geq mfa/(h_0 p)$, which exceeds L_p when $m > h_0(\log b)^2$.

So at an exceptional prime the unit of loss need not pay for the collisions; Section 48.4 obtains the valuation bound there on a submodule.

48.3. The chain of lifts

Fix a prime p and a ring map $\eta\colon \mathbb{C} \to \mathbb{C}_p$; $\mathcal{O}_\eta$ is the ring of Chapter 34.

Definition 48.3.1. At a point g of the finite adelic group, the *gauge* $\|\omega\|_g$ of a Weyl vector ω is the largest absolute value of a coordinate of $g^{-1} \cdot \eta(\omega)$, where at τ the adelic matrix acts in the Weyl representation through the extension to finite adeles of $u \mapsto \eta(\Phi_\tau(\bar{u}))$, and Φ_τ is the embedding of E selected by the CM type. A form φ *has valuation at least* c, for a real number c, if $\|\varphi(g)\|_g \le p^{-c}$ for every g; it is *integral* if it has valuation at least 0.

With $S \supseteq S_{\mathrm{ram}}$ the source forms and the ramified ones (Chapter 34), let $S_\eta \subseteq S$ be the $\mathcal{O}_\eta$-module of integral source forms and $S_{\mathrm{ram},\eta} = S_\eta \cap S_{\mathrm{ram}}$.

The translations $\mathfrak{t} = (\mathfrak{t}_j)_{j\ge 0} \in \mathcal{T}$ and the translated vacua $v_j(\mathfrak{t})$ are those of Definition 43.4.2.

Definition 48.3.2. For a twist ϑ, a finitely supported $\Psi\colon \mathcal{T} \to \mathbb{C}$ is a *weak chain datum* for ϑ if: for every $\mathfrak{t}$ in its support and every j, the entries of $\alpha\mathfrak{t}_j$ are integral at every finite place not dividing $N\mathrm{Nm}\, Q_\vartheta$ (with α as in Chapter 33); every value $\Psi(\mathfrak{t})$ is integral under every ring map $\mathbb{C} \to \mathbb{C}_\ell$ for every prime $\ell \nmid \mathrm{Nm}\, Q_\vartheta$; if $Q_\vartheta = \varnothing$, then $\sum_{\mathfrak{t}} |\sigma(\Psi(\mathfrak{t}))| \le \exp(x^{60})$ for every automorphism σ of $\mathbb{C}$; and $\sum_{\mathfrak{t}} \Psi(\mathfrak{t}) \bigotimes_{j<m} v_j(\mathfrak{t})$ is fixed by the levels of $X_0, \dots, X_{m-1}$.

Definition 48.3.3. The *restricted chain* of a weak chain datum Ψ for ϑ is $R_{\vartheta,\Psi} := \sum_{\mathfrak{t}} \Psi(\mathfrak{t})\, \Theta^{\mathfrak{t}}_{m-1} \cdots \Theta^{\mathfrak{t}}_0$, followed by restriction to Y_m, where the jth lift $\Theta^{\mathfrak{t}}_j$ is built from ϑ and has the datum $v_j(\mathfrak{t})$.

Away from N the proof uses the following expansion, which we take from it [GL].

Theorem 48.3.4. *For every twist ϑ and every chain datum Ψ for ϑ there is a weak chain datum Ψ' for ϑ with $B_{\vartheta,\Psi}\varphi = R_{\vartheta,\Psi'}\varphi$ for all $\varphi \in S$.*

We use three inputs. In (i) and (ii), let Ψ' be a weak chain datum for ϑ and suppose $p \nmid \mathrm{Nm}\, Q_\vartheta$.

(i) If $p \ne N$ and $p \ne d$, then $R_{\vartheta,\Psi'}$ maps S_η to integral forms.

(ii) Let $p \ne N$. If $p \nmid M$, then for every $\mathfrak{t}$ in the support of Ψ' and every $j \ge 0$ the datum $v_j(\mathfrak{t})$ is a standard datum of denominator 1 (Definition 50.4.1). If $\rho_0, \rho_1, \dots$ are real numbers such that, for every $\mathfrak{t}$ in the support of Ψ' and every $j \ge 0$, the datum $v_j(\mathfrak{t})$ multiplies gauges by at most $p^{-\rho_j}$ (Definition 50.4.2, for the lift j built from ϑ), then $R_{\vartheta,\Psi'}$ maps S_η to forms of valuation at least $\sum_{j<m} \rho_j$.

(iii) Let $\mathcal{D}_j(\Phi')$, for $j \ge 0$ and $\Phi' \subseteq \Phi$, be the stage bound of Definition 50.1.1. By Theorem 50.4.4: if $\chi_K(p) \ne 1$, then for every twist, every $j \ge 0$ and every standard datum φ of denominator 1 on $\mathrm{Hom}(X_j, X_{j+1})$, φ multiplies gauges by at most $p^{-\mathcal{D}_j(\varnothing)}$; and if $p < x_1$ and $\chi_K(p) \ne 1$, then for every $0 \le j < m$ and every $\Phi' \subseteq \Phi$,

$$\mathcal{D}_j(\Phi') \ge \frac{\mathrm{gain}(p)}{m} - C_p(\Phi') + c_p\, \#(\Phi_a \cap \Phi')\, \frac{a}{x_1} - \frac{fa(\log b)^2}{mp}.$$

Inputs (i) and (ii) are read from the proof. Input (iii) is proved in Chapter 50: its first part from the bound on jets along products of minors, Theorem 17.5.1, applied to the theta series of a standard datum, with four statements read from the proof; its second part by comparing the predicted divisibility of the diagram of the lift

with the prime sums that define gain(p). Here $\gamma_p = 1/(p-1) - \rho(d,p)$, which is $p/(p^2-1)$ at an inert prime and $1/(2d-2)$ at $p=d$ (Problem 49.1.1), is the credit of one box in the stage bound. A prime $p < x_1$ divides neither M nor N, since $p_0, p_1 \geq b^{10}$ and $N > M$ (Chapter 33).

Problem 48.3.1. Let $\mathcal{V}_0, \dots, \mathcal{V}_m$ be finite-dimensional $\mathbb{C}_p$-spaces with sup norms in fixed bases, let $\Theta_j^{\mathfrak{t}} \colon \mathcal{V}_j \to \mathcal{V}_{j+1}$ satisfy $\|\Theta_j^{\mathfrak{t}} u\| \leq p^{\rho_j}\|u\|$ for $\mathfrak{t}$ in a finite set, and let $\Psi(\mathfrak{t}) \in \mathbb{C}_p$ have $|\Psi(\mathfrak{t})|_p \leq 1$. Then $\big\|\sum_{\mathfrak{t}} \Psi(\mathfrak{t})\Theta_{m-1}^{\mathfrak{t}} \cdots \Theta_0^{\mathfrak{t}} u\big\| \leq p^{\rho_0+\cdots+\rho_{m-1}}\|u\|$.

Problem 48.3.2. Let $p < x_1$ be prime with $\chi_K(p) \neq 1$, $p \nmid \operatorname{Nm} Q_\vartheta$, and Ψ a chain datum for ϑ. For $\varphi \in S_\eta$, $B_{\vartheta,\Psi}\varphi$ has valuation at least gain$(p) - L_p - m\,C_p(\varnothing)$.

Let $p \nmid \operatorname{Nm} Q_\vartheta$ and let Ψ be a chain datum for ϑ. If $p < x_1$ is non-split and not exceptional, then by Problems 48.2.4 and 48.3.2, $B_{\vartheta,\Psi}$ has valuation at least gain$(p) - 2L_p$ on S_η. If $p \neq N$ and either $\chi_K(p) = 1$ or $p \geq x_1$, then $p \neq d$, as $d < x_1$ by Chapter 33; by (i), $B_{\vartheta,\Psi}$ maps S_η to integral forms, and gain$(p) = 0$.

48.4. Exceptional primes

Let p be inert in K. Each place σ, represented by the embedding Φ_σ, gives through η a prime v_σ of E above p; for every positive odd integer e, $v_{[-p^e]\sigma} = \bar{v}_\sigma$, the complex conjugate prime (Problem 53.1.1). Let $p < x_1$ be exceptional. A *mark* is a set $\mathfrak{M}$ of primes of E above p, each of the form v_τ with $\tau \in \Phi_a$, such that $\bar{v} \notin \mathfrak{M}$ for $v \in \mathfrak{M}$. It is *full* if it contains v_τ or $\bar{v}_\tau$ for each $\tau \in \Phi_a$; a full mark exists for every exceptional $p < x_1$ (Problem 53.1.5). Let $\Phi_{\mathfrak{M}} = \{\sigma \in \Phi : v_\sigma \in \mathfrak{M}\}$.

Problem 48.4.1. If $\mathfrak{M}$ is a full mark, then $C_p(\Phi_{\mathfrak{M}}) = 0$.

For $v \in \mathfrak{M}$ let $a_v = a \cdot \#\{\tau \in \Phi_a : v_\tau = v\}$, let T_v be the Hecke operator at the split pair $v, \bar{v}$ of the double coset of $\operatorname{diag}(p1_{r_p}, 1)$ (p is a uniformizer at v, as p is unramified in E), and let $Y_v = p^{a_v} T_v$ on S. Let $Y_{\mathfrak{M}}$ be the product of the Y_v, $v \in \mathfrak{M}$, in a fixed order. By Theorem 53.4.1, for a full mark $\mathfrak{M}$, a weak chain datum Ψ' for ϑ with $p \nmid \operatorname{Nm} Q_\vartheta$, and $\varphi \in S_\eta$, the form $R_{\vartheta,\Psi'}(Y_{\mathfrak{M}}^m \varphi)$ has valuation at least gain$(p) - 2L_p$. Let $j_p = \lceil 2mfa/p \rceil$.

Problem 48.4.2. Under the hypotheses of Problem 48.3.2, $B_{\vartheta,\Psi}(p^{j_p}\varphi)$ has valuation at least gain$(p) - L_p$ for $\varphi \in S_\eta$.

Problem 48.4.3. Let $p < x_1$ be exceptional, $\mathfrak{M}$ a full mark, $p \nmid \operatorname{Nm} Q_\vartheta$, and Ψ a chain datum for ϑ. On $S' = Y_{\mathfrak{M}}^m S_\eta + p^{j_p} S_\eta$, $B_{\vartheta,\Psi}$ has valuation at least gain$(p) - 2L_p$.

How large is S' in S_η? We use the colength of Chapter 5 and the phrase "onto modulo p^u up to colength c" as defined in Chapter 18. The proof applies Theorem 48.5.1 (Section 48.5) at the marked primes and obtains: for a mark $\mathfrak{M}$, $v \in \mathfrak{M}$ and every integer $u \geq 0$, Y_v is onto S_η modulo p^u up to colength $\big(12a_v/(mp) + u/(m^2 f)\big) D_X$.

Problem 48.4.4. Let $\mathcal{O}$ be a commutative ring, $p \in \mathcal{O}$, $\mathcal{L}$ a submodule of an $\mathcal{O}$-module $\mathcal{W}$, and Y_1, Y_2 $\mathcal{O}$-linear endomorphisms of $\mathcal{W}$ that are onto $\mathcal{L}$ modulo p^u up to colengths c_1 and c_2. Then $Y_1 Y_2$ is onto $\mathcal{L}$ modulo p^u up to colength $c_1 + c_2$.

Problem 48.4.5. For a mark $\mathfrak{M}$, $\sum_{v \in \mathfrak{M}} a_v \leq af$ and $\#\mathfrak{M} \leq f$, and

$$m \sum_{v \in \mathfrak{M}} \Big(\frac{12 a_v}{mp} + \frac{j_p}{m^2 f} \Big) \leq \frac{14fa + p/m}{p} \leq L_p.$$

So $Y^m_{\mathfrak{M}}$ is onto S_η modulo p^{j_P} up to colength L_pD_X: there is an integer $0 \le l \le L_pD_X$ such that the colength of S' in S_η divides p^l.

48.5. The theorem on elementary divisors

This section states the theorem that Section 48.4 applies at the marked primes. It is read from the proof [GL] and is not proved here; Chapter 18 computes its model at one vertex of the tree (Theorem 18.5.1), and "onto modulo p^u up to colength" is defined in Section 18.6. The letters of this section are its own and are used in no other section: here X, Z and I are finite sets, U is an endomorphism, η, η' are elements of $X \times \mathcal{C}$, ω is a coset, $\rho(\gamma)$ and D are matrices, and β is a family of exponents, not the diagram of the data.

In this chapter N_0, n, r_0, D and θ are local to the following theorem. Let $N_0 \ge 1$, let W' be a commutative local ring with maximal ideal $\mathfrak{m}$, and let O be a valuation domain of characteristic 0. In the setting of the theorem, a *Frobenius cycle* of length N_0 from W' to O consists of a prime p, a power $P \ge 5$ of p, ring homomorphisms $\iota_s\colon W' \to O$ for $s \in \mathbb{Z}/N_0$, a parity, even or odd, for each s, and an element $\varpi \in O$, such that $\varpi^2 = p$; p divides $\iota_{s+1}(w) - \iota_s(w)^P$ in O for all s and all $w \in W'$; the parities of s and $s+1$ differ for every s; and $W'/\mathfrak{m}$ has $q := P^{N_0}$ elements. Fix integers $n \ge 1$ (the rank), $\mu \ge 0$ (the degree in each letter s) and $r_0 \ge 0$. Let $\mathcal{B}$ be the set of families $\beta = (\beta_s)_{s\in\mathbb{Z}/N_0}$ of maps $\beta_s\colon \{0,\dots,n-1\} \to \mathbb{Z}_{\ge 0}$ with $\sum_i \beta_s(i) = \mu$ for each s. For $\gamma \in \mathrm{GL}_n(W')$ put $\gamma_s = \iota_s(\gamma)$ if s is even and $\gamma_s = \iota_s((\gamma^{-1})^{\mathsf{T}})$ if s is odd, and let $\rho(\gamma)$ be the $\mathcal{B}\times\mathcal{B}$ matrix whose (β,β') entry is the product over s of the coefficients of z^{β_s} in $\prod_i \bigl(\sum_j (\gamma_s)_{ji} z_j\bigr)^{\beta'_s(i)}$. The *depth* $\mathrm{dp}(\beta)$ is the sum of $\beta_s(i)$ over the pairs (i,s) with s even and $i \ge r_0$, or s odd and $i < r_0$; and D is the diagonal matrix with entries $p^{\mathrm{dp}(\beta)}$. Let $\mathcal{K}_{r_0} \subseteq \mathrm{GL}_n(W')$ consist of the matrices whose (i,j) entry lies in $\mathfrak{m}$ whenever $i < r_0 \le j$, and let $\mathcal{C} = \mathrm{GL}_n(W')/\mathcal{K}_{r_0}$, the set of left cosets.

For the theorem take finite sets X and Z. *Edge coordinates* on (X,Z) are maps $\pi\colon X\times\mathcal{C} \to X$, $\gamma\colon X\times\mathcal{C} \to \mathrm{GL}_n(W')$, $\gamma'\colon \mathcal{C} \to \mathrm{GL}_n(W')$ and $\upsilon\colon X\times\mathcal{C} \to \mathrm{GL}_Z(O)$, such that $\gamma'(\omega)^{-1}\mathcal{K}_{r_0} = \omega$ for every $\omega \in \mathcal{C}$, and $\eta = \eta'$ whenever $\eta,\eta' \in X\times\mathcal{C}$ satisfy $\pi(\eta) = \pi(\eta')$ and $\gamma(\eta)^{\mathsf{T}}(\gamma(\eta')^{\mathsf{T}})^{-1} \in \mathcal{K}_{r_0}$. For a finite set I and a bijection $J = (J_1, J_2)\colon I \to \mathcal{B}\times Z$, the *edge Hecke operator* $\mathcal{A}$ is the O-linear endomorphism of $(O^I)^X$ given by

$$(\mathcal{A}F)(\lambda)_i = \sum_{\omega\in\mathcal{C}} \sum_{i'\in I} \upsilon(\lambda,\omega)_{J_2 i,\, J_2 i'} \bigl(\rho(\gamma(\lambda,\omega))\, D\, \rho(\gamma'(\omega))\bigr)_{J_1 i',\, J_1 i}\, F(\pi(\lambda,\omega))_{i'}.$$

For $n = 2$ and $r_0 = 1$ the cosets $\mathcal{C}$ correspond to the lines of the residue plane, as the sources of Problem 18.1.1 do.

Theorem 48.5.1. *Let a Frobenius cycle of length $N_0 \ge 1$ from a commutative local ring W' to a valuation domain O of characteristic 0 be given, with prime p, power P and $q = P^{N_0}$ as above, and suppose that p is not a unit in O. Let n, μ, r_0 be integers and θ a real number with, for the natural logarithm,*

$$0 < r_0, \quad 2r_0 \le n, \quad 0 < \theta \le 1, \quad \mu^4 \le q, \quad \Bigl(\frac{N_0 n \log q}{\theta}\Bigr)^5 P^{3r_0} \le \mu.$$

Let X, Z and I be finite sets ($\mathcal{C}$ is finite), $J\colon I \to \mathcal{B}\times Z$ a bijection, edge coordinates on (X,Z) with edge Hecke operator $\mathcal{A}$, $\mathcal{M}$ an O-module, $\psi\colon (O^I)^X \to \mathcal{M}$ an O-linear map and U an endomorphism of $\mathcal{M}$ with $U\psi = \psi\mathcal{A}$. Then for every integer

$u \ge 0$, U is onto $\mathcal{L} = \psi\big((O^I)^X\big)$ modulo p^u up to colength

$$\big(3\,c_{\mathrm{div}} + \theta u\big)\,\#X\,\#I, \qquad c_{\mathrm{div}} = N_0\mu\Big(\frac{1}{P^{2r_0}} + \frac{r_0^2}{nP}\Big).$$

The bound has a part $\theta u\,\#X\,\#I$, a share θ of the bound $u\,\#X\,\#I$ that every endomorphism keeping $\mathcal{L}$ satisfies, as $\mathcal{L}$ is generated by $\#X\,\#I$ elements, and a part $3c_{\mathrm{div}}\#X\,\#I$ that does not depend on u. It bounds a colength, not the individual elementary divisors. Theorem 18.5.1 is its model, not a case of it:

Problem 48.5.1. A Frobenius cycle has even length N_0. Under the hypotheses on n, μ, r_0, θ of Theorem 48.5.1, $\mu > P^{3r_0}$ and $N_0 > 12r_0$. For $N_0 = 14$, $n = 2$, $r_0 = 1$, $\theta = 1/2$, $P = 5^{100}$ and $\mu = 5^{350}$ these hypotheses hold.

48.6. The level prime and the sum of the errors

At the level prime N, which is at least x_1, the gain is 0. Let S_N be the module of Definition 52.3.1. By Theorem 52.4.1 there is an integer $0 \le l \le mfb\,D_X$ such that the colength of S_N in S_η divides N^l, and for every twist ϑ, every chain datum Ψ for ϑ and every $\varphi \in S_{\mathrm{ram}} \cap S_N$, the form $B_{\vartheta,\Psi}\varphi$ has valuation at least $-2mfb$. The elements of S_N are forms on X_0, not all of them source forms; at $p = N$ the module of Theorem 48.7.1 is $S' = S_N \cap S_\eta$.

The *allowed loss* is

$$\mathrm{loss}(p) = \begin{cases} 2L_p & \text{if } p < x_1 \text{ is prime and } \chi_K(p) \ne 1, \\ 2mfb & \text{if } p = N, \\ 0 & \text{otherwise.} \end{cases}$$

Problem 48.6.1. Let $m \ge 2$, $p \ge 2$, and $p \equiv \pm 1 \pmod m$. Then $p = mc - 1$ or $p = mc + 1$ for an integer c with $1 \le c \le p$ and $m \le 2p/c$.

Let $T_0 = 4fa(\log b)^2 \log x_1$.

Problem 48.6.2. For a prime $p < x_1$ with $\chi_K(p) \ne 1$ there is an integer $1 \le c \le p$ with $p \in \{mc - 1, c, mc + 1\}$ and $\mathrm{loss}(p)\log p \le T_0/c$.

The term of N is also at most T_0: the scale inequalities of Chapter 33 give $2mfb\log N \le T_0$ (they give $\log N \le 30\,m\log b$ and $m \le 2\sqrt{x}$, and imply $(\log b)\log x_1 \ge 60$). In sums over natural numbers we set $\log 0 = 0$.

Problem 48.6.3. For every finite set A of natural numbers, $\sum_{p\in A}\mathrm{loss}(p)\log p \le 4T_0(1 + \log x_1)$.

Problem 48.6.4. If $(\log x_1)^6 \le \log b$ and $\log x_1 \ge 3$, then $4T_0(1 + \log x_1) \le U$.

Both hypotheses of Problem 48.6.4 hold for the data of Chapter 33.

48.7. The theorem

The four kinds of primes are: $p \ne N$ split or at least x_1, with S_η and $l = 0$ (Section 48.3); $p < x_1$ non-split and not exceptional, with S_η and $l = 0$ (Section 48.3); $p < x_1$ exceptional, with S' (Section 48.4); and $p = N$, with $S' = S_N \cap S_\eta$ and the integer l of Theorem 52.4.1 (Section 48.6). These four cases give the following theorem for ramified inputs.

Theorem 48.7.1. *Let p be prime and $\eta\colon \mathbb{C} \to \mathbb{C}_p$ a ring map. There are an integer $l \geq 0$ with $l \leq \operatorname{loss}(p)\, D_X$ and an $\mathcal{O}_\eta$-submodule $S' \subseteq S$ whose colength in S_η divides p^l, such that, for every twist ϑ, every chain datum Ψ for ϑ with $p \nmid \operatorname{Nm} Q_\vartheta$, and every $\varphi \in S' \cap S_{\mathrm{ram}}$, the form $B_{\vartheta,\Psi}\varphi$ has valuation at least* $\operatorname{gain}(p) - \operatorname{loss}(p)$.

Intersecting S' with $S_{\mathrm{ram},\eta}$ keeps the bound on its colength, now in $S_{\mathrm{ram},\eta}$. The definition of loss gives its nonnegativity and vanishing, and Problems 48.6.3 and 48.6.4 bound its weighted sum. This gives the theorem of this chapter.

Theorem 48.7.2. *There are real numbers* $\operatorname{err}(p)$, $p \in \mathbb{N}$, *with the following properties.*

(a) $\operatorname{err}(p) \geq 0$ *for every p.*
(b) *If $p \neq N$, and $\chi_K(p) = 1$ or $x_1 \leq p$, then* $\operatorname{err}(p) = 0$.
(c) $\sum_{p \in A} \operatorname{err}(p) \log p \leq U$ *for every finite set A of natural numbers.*
(d) *For every prime p and every ring map $\eta\colon \mathbb{C} \to \mathbb{C}_p$ there are an integer $l \geq 0$ with $l \leq \operatorname{err}(p)\, D_X$ and an $\mathcal{O}_\eta$-submodule $S' \subseteq S_{\mathrm{ram},\eta}$ whose colength in $S_{\mathrm{ram},\eta}$ divides p^l, such that for every twist ϑ, every chain datum Ψ for ϑ with $p \nmid \operatorname{Nm} Q_\vartheta$, and every $\varphi \in S'$, the form $B_{\vartheta,\Psi}\varphi$ has valuation at least* $\operatorname{gain}(p) - \operatorname{err}(p)$.

Its proof takes err = loss. The dimension in (d) is that of all source forms, while the colength is measured in the integral ramified ones; the module S' depends on p and η and serves every twist of level prime to p and every chain datum for that twist.

Theorem 48.7.2 is the divisibility input to Theorem A: Chapter 42 combines (c) and (d) with the seesaw identity of Chapter 43 and further inputs to bound the index of finite families in the images $A_s(S^{\mathrm{int}}_{\mathrm{ram}})$ of the integral ramified source forms under the normalized translates. Chapters 49 and 50 prove input (iii), Chapter 52 treats the level prime and Chapter 53 the exceptional primes; Chapter 51 bounds the size of the composite lift, against which Theorem A sets this divisibility.

In the Lean formalization. In the Lean proof [GL], Theorem 48.7.2 is `New.Data.exists_err_gaugeLe_compositeLift` and Theorem 48.7.1 is `New.Data.exists_colengthDvd_gaugeLe_compositeLift`, in `New/UpperBound/Divisibility/LocalDivisibility.lean`. The definitions are `Data.gain`, `Data.localPrimeSum`, `Data.loss` (L_p), `Data.allowedLoss` (loss), `Data.IsExceptional`, `Data.IsMarked`, `Data.IsFullMark`, `Data.IsWeakChainDatum` and `Data.restrictedChain`. The inputs read in the text are `Data.IsChainDatum.exists_isWeakChainDatum_compositeLift_eq` (Theorem 48.3.4), `Data.IsWeakChainDatum.gaugeLe_restrictedChain_one` (i), `Data.IsWeakChainDatum.translateDatum_mem_standardData` and `Data.IsWeakChainDatum.gaugeLe_restrictedChain_of_mem_raises` (ii), and `Data.IsMarked.isOntoUpToColength_scaledHeckeOperator`. Theorem 48.5.1 is `FrobeniusCycle.elementary_divisors`, with the hypotheses `IsLargeDegree`, in `New/UpperBound/ElementaryDivisors/ElementaryDivisorTheorem.lean`.

Hints

§48.1.

48.1.1: Show $d \equiv q_0/2 - 1 \pmod{q_0}$, so $d \equiv -1$ modulo 8 and modulo each odd prime dividing q_0. Then quadratic reciprocity.

48.1.2: I_p is the set of odd $e \geq 1$, and $c_p = 1$.
48.1.3: If $\chi_K(p) = 1$, I_p is empty. If $p \geq x_1$, compare y/p^e with a/x_1.
48.1.4: Compute $1 - \chi_K(p^e)$ in the three cases inert, ramified, split. For $p^e > a$ the term of $s_{\mathrm{fin},p}$ vanishes.

§48.2.

48.2.1: τ and $[-p^e]\tau$ have class 1 modulo q_0. For $p = d$, compute $-d^e$ modulo q_0 separately for even and odd e, using $4 \mid q_0$ and the congruence for d in the hint to Problem 48.1.1.
48.2.2: Decompose $(\mathbb{Z}/18480)^\times$ by the Chinese remainder theorem and find its elements of odd order. Use a prime search for the two minima.
48.2.3: At each of the f places, a geometric series of ratio at most $1/2$.
48.2.4: Two cases, according as $p \equiv \pm 1 \pmod m$ (Problem 48.2.3 with $o = 1$) or not; in the second, Problem 48.2.1 and $m \leq p^{r_p}$.
48.2.5: Every $(\tau, 1)$ with $\tau \in \Phi_a$ is a collision.

§48.3.

48.3.1: The sup norm is ultrametric.
48.3.2: Theorem 48.3.4; then (ii) and (iii) with $\Phi' = \varnothing$.

§48.4.

48.4.1: The relation $v_{[-p^e]\sigma} = \bar{v}_\sigma$.
48.4.2: Problem 48.2.3 with $o = 1$.
48.4.3: The ultrametric inequality.
48.4.4: A product of two matrices.
48.4.5: Each $\tau \in \Phi_a$ induces one prime. Bound j_p by $2mfa/p + 1$.

§48.5.

48.5.1: Go once around $\mathbb{Z}/N_0$. For the size, $N_0 n \log q/\theta > 1$; for the example, $\log 5 < 2$.

§48.6.

48.6.1: $mc \leq p + 1 \leq 2p$.
48.6.2: Problem 48.6.1, or $c = p$.
48.6.3: Each $c \leq x_1$ serves at most the four numbers N, $mc - 1$, c, $mc + 1$; give N the value $c = 1$.
48.6.4: Compare $16\,t(1 + t)$ with t^6.

References

[GL] L. Sernau, *GRH for Dirichlet L-functions, in Lean 4*, a shorter rewriting of the Lean proof, text by Claude, `https://github.com/lsernau/grh-lean`, commit `72fead1`, readable edition `grh/`.

THE COUNT: CONGRUENCES, DIRECTIONS AND FACTORIALS

Prerequisites. Chapter 17, *Pairings on a formal group of height two*: Problems 17.3.1 and 17.3.3, and Section 17.5 entire; Problem 17.4.4. Legendre's formula $\operatorname{val}(n!) = (n - s_p(n))/(p-1)$, with $s_p(n)$ the sum of the base-p digits of n. Determinants over a commutative ring; the field $\mathbb{C}_p$, its ring of integers $\mathcal{O}_{\mathbb{C}_p}$, and the valuation val with $\operatorname{val}(p) = 1$ (Chapter 34).

In Chapter 48 the kernel bound (ii) of Section 48.3 rests on a bound for the jets of a series in the normal form along products of minors, stated in Theorem 17.5.1. For the marks at exceptional primes $p < x_1$ (Section 48.4) the proof [GL] needs it in a stronger form, in which the columns of height one at some places are removed from the prediction and paid for by powers of p on the rows. This sheet proves the bound for two places and states the general count with charges. How much of the credit $\gamma_p n$ of a jet of order n, from the factorials and the rescaling by ϖ, survives the couplings between a place and its partners?

Throughout, $d \equiv 7 \pmod 8$ is a prime, $K = \mathbb{Q}(\sqrt{-d})$, p is a prime with $\chi_K(p) = (\frac{p}{d}) \neq 1$, and c_p, I_p, I_p°, $\rho(d,p)$ are as in Section 17.5: $c_p = 1/2$ if $p = d$ and 1 otherwise, I_p° is the set of $e \geq 0$ with $p = d$, or $\chi_K(p) = -1$ and e odd, $I_p = I_p^\circ \smallsetminus \{0\}$, and $\rho(d,p) = c_p/(p^2-1)$ for p inert, $c_p/(p-1)$ for $p = d$. As in Chapter 48, $\gamma_p := 1/(p-1) - \rho(d,p)$. Let $\pi_p := p$ if $p \neq d$, and $\pi_p := \eta(\sqrt{-d})$ if $p = d$, for a fixed ring map $\eta\colon \mathbb{C} \to \mathbb{C}_p$; so $\operatorname{val}\pi_p = c_p$. Integral series and jets $(Q(\partial)G)(0)$ are as in Section 17.5.

49.1. Two places and one row

Problem 49.1.1. $\gamma_p = c_p \sum_{e \in I_p} p^{-e}$. If $\varpi \in \mathbb{C}_p$ has $\operatorname{val}\varpi = \rho(d,p)$, then $\operatorname{val}(\varpi^{p+1}\pi_p/p) = 1/(p-1)$, both for p inert and for $p = d$. [Check: $\gamma_3 = 3/8$ at an inert prime 3.]

For the rest of this section $\chi_K(p) = -1$, so that $c_p = 1$, $I_p^\circ = I_p$ is the set of odd $e \geq 1$, and $\operatorname{val}\varpi = \rho := 1/(p^2-1)$. The *two-place model* has two places $1, 2$, one row and one input coordinate, hence two variables z_1, z_2; the partner of each place, for every e, is the other place. So the couplings are $\Gamma_e = z_1^{p^e} z_2 + z_2^{p^e} z_1$, and $F \in \mathbb{C}_p[[z_1, z_2]]$ has the normal form for (I_p, ϖ) if

$$F(\varpi z_1, \varpi z_2) = W(z_1, z_2)\, \exp\Big(\frac{\varpi^{p+1}}{p}\, \mathcal{E}(z_1, z_2)\Big),$$

with W integral and $\mathcal{E}$ a sum of the powers $\Gamma_e^{p^j}$ ($e \in I_p$, $j \geq 0$) with coefficients in $\mathcal{O}_{\mathbb{C}_p}$. In this sheet a and w are the orders of a jet $\partial_1^a \partial_2^w$, with $\partial_i := \partial/\partial z_i$.

Problem 49.1.2. Let $p = 3$. The series $F_0 := \exp\big((z_1^3 z_2 + z_1 z_2^3)/3\big)$ has the normal form with $W = 1$ and $\mathcal{E} = \Gamma_1$. Its jets at $(a, w) = (3k, k)$ are $(3k)!/3^k$, that is $2, 80, 13440$ for $k = 1, 2, 3$, of valuations $0, 0, 1$.

Date: November 26, 2026.

The credit comes from the factorials.

Problem 49.1.3. For integers $\nu_1, \dots, \nu_q \geq 0$ with $\nu_1 + \cdots + \nu_q = n$, and $\nu! := \nu_1! \cdots \nu_q!$,

$$\operatorname{val}(\nu!) \;\geq\; \frac{n}{p-1} - q\big(1 + \lfloor \log_p n \rfloor\big),$$

with $\lfloor \log_p 0 \rfloor := 0$. [Check: $p = 3$, $\nu = (27, 1)$: $13 \geq 14 - 8$.]

Problem 49.1.4. Let G be a power series over $\mathbb{C}_p$ in q variables whose coefficients of degree n are integral, and let Q be a homogeneous polynomial of degree n with coefficients in $\mathcal{O}_{\mathbb{C}_p}$. Then $\operatorname{val}\big((Q(\partial)G)(0)\big)$ is at least the bound of Problem 49.1.3.

The debit comes from the couplings. One differentiates along scaled directions.

Problem 49.1.5. For $y_1, y_2 \in \mathbb{C}_p$ and $G(u_1, u_2) := F(\varpi y_1 u_1, \varpi y_2 u_2)$, $(\partial_{u_1}^a \partial_{u_2}^w G)(0) = \varpi^{a+w} y_1^a y_2^w \, (\partial_1^a \partial_2^w F)(0)$.

Problem 49.1.6. Let F have the normal form, $n \geq 0$, and $y_1, y_2 \in \mathcal{O}_{\mathbb{C}_p}$ with $y_1^{p^e} y_2 \equiv y_2^{p^e} y_1 \equiv 0 \pmod{p}$ for every $e \in I_p$ with $p^e \leq n$. Then the coefficients of degree at most n of $F(\varpi y_1 u_1, \varpi y_2 u_2)$ are integral.

Problem 49.1.7. Fix $e \in I_p$, and let $p^{1/p^e} \in \mathcal{O}_{\mathbb{C}_p}$ be a root of $X^{p^e} = p$. The pairs $(y_1, y_2) = (1, p)$, $(p, 1)$, $(p^{1/p^e}, p^{1/p^e})$ satisfy both congruences of Problem 49.1.6 at e, at the costs $a \operatorname{val} y_1 + w \operatorname{val} y_2 = w$, a, $(a + w)/p^e$. There is also an integral pair satisfying both congruences at the cost

$$\min(a/p^e, w) + \min(w/p^e, a).$$

[Check: $p = 3$, $(a, w) = (27, 1)$: $4/3$ at $e = 1$, $28/27$ at $e = 3$.]

Problem 49.1.8. If F has the normal form, then for all $a, w \geq 0$,

$$\operatorname{val}\big((\partial_1^a \partial_2^w F)(0)\big) \;\geq\; \gamma_p(a + w) - \sum_{e \in I_p,\ p^e \leq a+w} \Big[\min\Big(\frac{a}{p^e}, w\Big) + \min\Big(\frac{w}{p^e}, a\Big)\Big] - 2\big(1 + \lfloor \log_p(a + w) \rfloor\big).$$

Problem 49.1.9. For $a + w \geq 1$, the right side of Problem 49.1.8 is at least $\mathcal{D}(a, w) - 2(1 + \log_p(a + w))$, where

$$\mathcal{D}(a, w) := \sum_{e \in I_p} \Big[\Big(\frac{a}{p^e} - w\Big)_+ + \Big(\frac{w}{p^e} - a\Big)_+\Big]$$

is the predicted divisibility of Problem 17.5.3. [Check: $p = 3$: $\mathcal{D}(27, 1) = 8$, $\mathcal{D}(54, 2) = 16$, $\mathcal{D}(243, 1) = 88$.]

Problem 49.1.10. Let $p = 3$ and $F_1 := F_0/(1 - z_1)$. Then F_1 has the normal form, and $(\partial_1^a \partial_2 F_1)(0) = a!/3$ for $a \geq 3$, of valuation 12 at $a = 27$ and 120 at $a = 243$. Problem 17.4.4 gives valuations 11 at $(27, 1)$ and 22 at $(54, 2)$ for $\exp(-Q_{c,\sigma c})$, c a unit. All four exceed $\mathcal{D}(a, w)$.

Problems 49.1.3–49.1.9 prove the count for two places, one row and one input coordinate, with the error $2(1 + \log_p \max(a + w, 1))$. The model is not an instance of Theorem 17.5.1: there the partners are the places $[-p^e]\tau$, and only columns of height less than the number n of rows count, so height-one columns need $n \geq 2$; with $n = 2$ and all boxes in row 0 the error is $8f(1 + \log_p \max(a + w, 1))$. In general a direction has one component per input coordinate, and at height h the proof takes integral combinations of the first h directions by an $h \times h$ matrix.

49.2. Diagrams, directions and the cost

From now on we are in the setting of Theorem 17.5.1: q_0, d, s, the set Φ of infinite places of $\mathbb{Q}(\sqrt{-d},\zeta_{q_1})$ and $f=\#\Phi$ are as there, p is a prime with $\chi_K(p)\neq 1$, and the partner of τ at e is $[-p^e]\tau$. There are n rows $0\le i<n$ and n' input coordinates $0\le l<n'$, and the variables are $z_{\tau il}$. The couplings are $\Gamma_e=\sum_{\tau,i,l} z_{\tau il}^{\,p^e} z_{[-p^e]\tau,il}$, and $\varpi\in\mathbb{C}_p$ has $\operatorname{val}\varpi=\rho(d,p)$. We say that $F\in\mathbb{C}_p[[z]]$ has the normal form if it has the normal form of Section 17.5 for $(I_p^\circ,[-p^e]\cdot\,,\varpi)$ and some family of integral coefficients.

Definition 49.2.1. A *diagram* is a function $\beta\colon \Phi\times\{1,2,\dots\}\to\mathbb{N}$; $\beta(\tau,h)$ is the number of columns of height h at τ. Only the heights $h<n$ count:

$$\beta_1(\tau):=\beta(\tau,1),\qquad \beta_{>1}(\tau):=\sum_{1<h<n}\beta(\tau,h),\qquad \|\beta\|_{>1}(\tau):=\sum_{1<h<n}h\,\beta(\tau,h),$$

(with $\beta_1:=0$ if $n\le 1$), and the number of boxes is $|\beta|:=\sum_\tau\big(\beta_1(\tau)+\|\beta\|_{>1}(\tau)\big)$.

Definition 49.2.2. For $\Phi'\subseteq\Phi$, the *erasure* $\beta\smallsetminus\Phi'$ is the diagram equal to 0 at $(\tau,1)$ for $\tau\in\Phi'$ and to β elsewhere.

Definition 49.2.3. With $\tau':=[-p^e]\tau$ and $\tau_0:=[-1]\tau$, the *predicted divisibility* of β is

$$\begin{aligned}\mathcal{D}(\beta):=c_p\sum_{e\in I_p}\sum_{\tau\in\Phi}\Big[&\Big(\frac{\beta_1(\tau)}{p^e}-\beta_1(\tau')-\beta_{>1}(\tau')\Big)_+\\ &+\Big(\frac{\|\beta\|_{>1}(\tau)}{p^e}-\|\beta\|_{>1}(\tau')\Big)_+-\frac{\beta_{>1}(\tau)}{p^e}\Big]\\ -[p=d]\,\frac12\sum_{\tau\in\Phi}\Big[&\min\big(\beta_1(\tau),\beta_1(\tau_0)+\beta_{>1}(\tau_0)\big)+\beta_{>1}(\tau)\\ &+\min\big(\|\beta\|_{>1}(\tau),\|\beta\|_{>1}(\tau_0)\big)\Big],\end{aligned}$$

where $[p=d]$ is 1 if $p=d$ and 0 otherwise.

For the shape κ with $\kappa(\tau,0)=0$ and $\kappa=\beta$ at heights $h\ge 1$ this is the number $\Delta(\kappa)$ of Section 17.5, and a_τ,a'_τ,l_τ there are $\beta_1(\tau),\beta_{>1}(\tau),\|\beta\|_{>1}(\tau)$. For a standard filling $\mathbf{i}$, which puts the row $\mathbf{i}(\tau,h,c,j)$ into box $j<h$ of the cth column $(1\le c\le\beta(\tau,h))$ of height h at τ, $1\le h<n$, and integral directions $y=(y_{\tau lk})$ $(k\ge 0)$, the product of minors of Section 17.5, written P_μ there for the family $\mu=y$, is

$$P_y(z)=\prod_{\tau\in\Phi}\prod_{h<n}\prod_{1\le c\le\beta(\tau,h)}\det\Big(\sum_l y_{\tau lk}\,z_{\tau,\mathbf{i}(\tau,h,c,j),l}\Big)_{0\le j,k<h}.$$

Three facts of the general step are read from the proof (see the remark). The proof replaces the given directions by new ones, $y'_{\tau hk}:=\sum_{k'<h}(g_{\tau h})_{kk'}\,y_{\tau\cdot k'}$, with one integral $h\times h$ matrix $g_{\tau h}$ for each place and height, shared by the $\beta(\tau,h)$ columns.

Problem 49.2.1. Let $v_1,\dots,v_h\in\mathcal{O}_{\mathbb{C}_p}$ be the values of a linear form on the h rows of a matrix, and $\varpi'\in\mathcal{O}_{\mathbb{C}_p}$. Some $g\in M_h(\mathcal{O}_{\mathbb{C}_p})$ with $\det g\mid\varpi'$ has $\varpi'\mid(gv)_k$ for every k. For finitely many forms and moduli there is one g, with $\det g$ dividing the product of the moduli, that works for all of them. [Over $\mathbb{Z}_3$, for $v=(1,2)^t$ and $\varpi'=3$, there is such a g with $gv=(3,0)^t$ and $\det g=3$.]

Problem 49.2.2. Take one place (dropped from indices), $n = 3$, $n' = 2$, two columns of height 2 filled with the rows $0, 1$, and the coordinate vectors as directions. Then $P_y = (z_{00}z_{11} - z_{01}z_{10})^2$ and $(P_y(\partial)P_y)(0) = 12$. With the first direction scaled by 3, $y = \mathrm{diag}(3, 1)$, the jet of $(z_{00}z_{11} - z_{01}z_{10})^2$ along P_y is 108.

In general put $z_{\tau il} = \varpi \sum_{h<n,\ k<h} u_{\tau hki}\, y'_{\tau hk,l}$ in new variables $u_{\tau hki}$, and let Q be the product, over the columns, of $\det(u_{\tau hk\,\mathbf{i}(\tau,h,c,j)})_{0\le j,k<h}$. First, by multilinearity of the determinants and the chain rule,

$$\big(Q(\partial_u)\, F(z(u))\big)(0) = \varpi^{|\beta|} \prod_{\tau\in\Phi} \prod_{h<n} (\det g_{\tau h})^{\beta(\tau,h)}\ \big(P_y(\partial)F\big)(0),$$

the case of Problem 49.1.5 with matrices in place of scalars. Second, for a shift e, a place τ and its partner $\tau' = [-p^e]\tau$, let

$$\mathrm{ded}_{e,\tau}(\beta) := \min\Big(\frac{\beta_1(\tau)}{p^e},\ \beta_1(\tau') + \beta_{>1}(\tau')\Big) + \frac{\beta_{>1}(\tau)}{p^e} + \min\Big(\frac{\|\beta\|_{>1}(\tau)}{p^e},\ \|\beta\|_{>1}(\tau')\Big).$$

The proof chooses the $g_{\tau h}$ so that π_p divides $\sum_l y'^{\,p^e}_{\tau hk,l}\, y'_{\tau' h'k',l}$ for all $e \in I_p^\circ$ with $e \le \lfloor \log_p|\beta|\rfloor$, all places, heights and directions, and so that

$$\sum_{\tau\in\Phi}\sum_{h<n} \beta(\tau,h)\,\mathrm{val}(\det g_{\tau h}) \ \le\ c_p \sum_{e\in I_p^\circ,\ e\le\lfloor\log_p|\beta|\rfloor} \ \sum_{\tau\in\Phi} \mathrm{ded}_{e,\tau}(\beta).$$

At the source the modulus is π_p^{1/p^e}, at the partner π_p, as in Problem 49.1.7; a source condition $\sum_l y_l^{p^e} v_l \equiv 0 \pmod{\pi_p}$ follows from the linear condition $\sum_l v_l^{1/p^e} y_l \equiv 0 \pmod{\pi_p^{1/p^e}}$, so Problem 49.2.1 applies. Each height is weighted by its number of columns: the first minimum compares entry conditions at height one on the source with pairing conditions at the partner, the middle term counts source pairing conditions at the higher heights, and the last minimum compares entry conditions at those heights on the two sides. Third, π_p divides $\Gamma_e(z(u)/\varpi)$ for these e, the series $F(z(u))$ is integral through degree $|\beta|$, and Q is homogeneous of degree $|\beta|$.

Problem 49.2.3. $c_p \sum_{e\in I_p^\circ} \sum_{\tau\in\Phi} \mathrm{ded}_{e,\tau}(\beta) = \gamma_p|\beta| - \mathcal{D}(\beta)$, the series converging. The variables $u_{\tau hki}$ number at most fn^3.

As $\mathrm{ded}_{e,\tau} \ge 0$, the truncated sum is at most the full one. So Problems 49.1.3, 49.1.4 and 49.2.3, with the three facts read from the proof, give Theorem 17.5.1 for diagrams (with $\lfloor \log_p 0\rfloor := 0$).

Problem 49.2.4. Let $p = d$ and $n \ge 2$, let σ_1 and $\sigma_2 = [-1]\sigma_1$ be two places, and let $\beta(\sigma_1, 1) = 12$, $\beta(\sigma_2, 1) = 4$ and $\beta = 0$ otherwise. The shift $e = 0$ debits $c_p\big(\mathrm{ded}_{0,\sigma_1}(\beta) + \mathrm{ded}_{0,\sigma_2}(\beta)\big) = 4$, and the half sum in $\mathcal{D}(\beta)$ contributes -4.

49.3. Charges

At an exceptional prime $p < x_1$ the loss allowed in Section 48.2 need not cover the collisions between a-places. The proof then removes the columns of height one at a set Φ' of places from the prediction and pays for their pairings with factors p on rows.

Definition 49.3.1. Let β be a diagram and $\Phi' \subseteq \Phi$. *Charges* for (β, Φ') are numbers $\mathfrak{c}(\tau, h, i) \in \mathbb{N}$ ($\tau \in \Phi$, $h \ge 1$, $0 \le i < n$) such that, for all $e \in I_p^\circ$, $\tau \in \Phi$, $h \ge 1$ and rows i, with $\tau' = [-p^e]\tau$: if both $\beta(\tau, 1) \ne 0$ and $\beta(\tau', h) \ne 0$, and if

either $\tau \in \Phi'$ or both $h = 1$ and $\tau' \in \Phi'$, then $\mathfrak{c}(\tau,1,i) + \mathfrak{c}(\tau',h,i) > 0$. Here h runs over all heights, including $h \geq n$. For a filling $\mathbf{i}$, the sum of the charges over the boxes is $\sum_{\text{boxes}} \mathfrak{c} := \sum_\tau \sum_{h<n} \sum_{1\leq c\leq \beta(\tau,h)} \sum_{j<h} \mathfrak{c}\big(\tau,h,\mathbf{i}(\tau,h,c,j)\big)$.

Problem 49.3.1. In the two-place model let F have the normal form. (i) $\operatorname{val}\big((\partial_1^a\partial_2^w F)(0)\big) \geq \gamma_p(a+w) - w - 2(1+\lfloor \log_p(a+w)\rfloor)$. (ii) With a second, empty row ($n = 2$), $\beta(1,1) = a$, $\beta(2,1) = w$, $\beta = 0$ otherwise, $\Phi' = \{1\}$, $\mathfrak{c}(2,1,i) = 1$ for both rows i and $\mathfrak{c} = 0$ otherwise, the numbers $\mathfrak{c}$ are charges for (β,Φ') for the partner rule of the model, and for the filling with all boxes in row 0 the main term $\mathcal{D}(\beta \smallsetminus \Phi') + \gamma_p(|\beta| - |\beta \smallsetminus \Phi'|) - \sum_{\text{boxes}} \mathfrak{c}$ equals $\gamma_p(a+w) - w$. [Check the main term in (ii) at $p = 3$: 719/8 at $(243,2)$, against $\mathcal{D}(243,2) = 86$; 2177/8 at $(729,2)$, against $\mathcal{D}(729,2) = 267$.]

In general the substitution becomes $z_{\tau il} = \varpi \sum_{h,k} p^{\mathfrak{c}(\tau,h,i)}\, u_{\tau hki}\, y'_{\tau hk,l}$, and the multiplier gains the factor $p^{\sum_{\text{boxes}} \mathfrak{c}}$. The pairings of height one at τ with height h at τ', where $\tau \in \Phi'$ or both $h = 1$ and $\tau' \in \Phi'$, are *exempt*: no congruence is imposed on them, and the charge condition gives a factor p on one side of each row (after setting the charges to 1 where $\beta(\tau,h) = 0$, which changes no box). With S the set of $e \in I_p^\circ$, $e \leq \lfloor \log_p|\beta|\rfloor$, the remaining congruences give $\sum_\tau \sum_{h<n} \beta(\tau,h) \operatorname{val}(\det g_{\tau h}) \leq c_p \sum_{e\in S} \sum_\tau \operatorname{ded}_{e,\tau}(\beta \smallsetminus \Phi')$, the cut-off using $|\beta|$.

Problem 49.3.2. (m) Let $q_0 = 18480$, $d = 138599$, $s = 0$, $p = 13$. By machine: d is prime, $q_0 \mid 2(d+1)$, $(d+1) \bmod q_0 = 9240$, $\chi_K(13) = -1$, $f = \varphi(4490640) = 933120$, and $[-13^e] \neq 1$ for odd e. Take $n = 2$ rows, one input coordinate, $A := 13^{12}$ columns of height one at the identity place, all in row 0, the direction 1 at that place, and $F := (z/\varpi)^A$ in the coordinate z of that row. Then F has the normal form, $\operatorname{val}\big(F^{(A)}(0)\big) = (A-1)/12 - A/168 = 302875106592239/168$, and the bound of Theorem 17.5.1 is $13A/168 - 933120 \cdot 2^3 \cdot 13 = 302858803119613/168$.

We take the following theorem from the proof. The construction of the directions uses the simultaneous elimination of Problem 49.2.1; the proof uses both conclusions of Problem 49.2.3, applying the identity to the erased diagram; Problem 49.3.1 treats one marking in the two-place model.

Theorem 49.3.2. *Let q_0, d, s, Φ, f, p with $\chi_K(p) \neq 1$, η, the n rows and the n' input coordinates be as above, let $\varpi \in \mathbb{C}_p$ with $\operatorname{val}\varpi = 1/(p-1) - \gamma_p$, and let $F \in \mathbb{C}_p[[z]]$ have the normal form. Let β be a diagram, $\Phi' \subseteq \Phi$, and $\mathfrak{c}$ charges for (β,Φ'). Then for every standard filling $\mathbf{i}$ of β and all integral directions y,*

$$\operatorname{val}\big((P_y(\partial)F)(0)\big) + \sum_{boxes} \mathfrak{c} \;\geq\; \mathcal{D}(\beta\smallsetminus\Phi') + \gamma_p\big(|\beta| - |\beta\smallsetminus\Phi'|\big) - fn^3\big(1+\log_p \max(|\beta|,1)\big).$$

For $\Phi' = \varnothing$ and $\mathfrak{c} = 0$ it gives Theorem 17.5.1 for shapes with $\kappa(\tau,0) = 0$; that theorem keeps its place in Chapter 17. The theorem is read from the proof; which series have the normal form is a separate statement.

In the Lean formalization. In the Lean proof [GL], Theorem 49.3.2 is `New.Parameters.norm_jet_minorProd_le_of_charges` in `grh/src/New/Derivatives/Divisibility/Count.lean`, stated as an upper bound for the norm of the jet, for diagrams κ on $\Phi \times \mathbb{N}$; this sheet takes $\kappa(\tau,0) = 0$ (when $n > 0$, columns of height 0 would count among the low columns). In the same file, erasure, the predicted divisibility and the sum of the charges over the boxes are `eraseHeightOne`, `predictedDivisibility` and

`fillingCharge`; the multiplier is `jet_columnDetProd_subst`; the divisibility of the substituted couplings, exempt pairs included, is `dvd_subst_coupling_directionSubst_of_charges`; and the identity of Problem 49.2.3 is `mul_tsum_deductionAt`. In `NullFrames.lean`, $\mathrm{ded}_{e,\tau}$ is `deductionTerm` with no marked places, and the change of directions with its determinant bound is `exists_newDirection_dvd`. The integrality through degree $|\beta|$ is `HasNormalForm.norm_coeff_subst_le_one` in `NormalForm.lean`.

This sheet has proved the two-place bounds, without marking and with place 1 marked (Problems 49.1.9 and 49.3.1); Theorem 49.3.2 is read from the proof. Chapter 50 uses the normal form of the jet series of a standard datum and the uncharged count to bound the kernel of one lift; the charged count enters the estimate at a mark of an exceptional prime $p < x_1$ [GL].

Hints

§49.1.

49.1.1: A geometric series; then $\mathrm{val}(\varpi^{p+1}) + c_p - 1$.
49.1.2: Only $(z_1^3 z_2)^k$ contributes to the monomial $z_1^{3k} z_2^k$.
49.1.3: Legendre's formula; $s_p(\nu_i) \le (p-1)(1 + \lfloor \log_p n \rfloor)$.
49.1.4: The jet of G along u^ν is $\nu!\,[u^\nu]G$.
49.1.6: Couplings with $p^e > n$ have degree $> n$. In degrees $\le n$ the exponent has coefficients of valuation $\ge 1/(p-1)$ (Problem 49.1.1); argue as in Problem 17.3.3.
49.1.7: For each congruence compare a source scaling by p^{1/p^e} with a partner scaling by p, and multiply the two choices.
49.1.8: Take the product of the pairs of Problem 49.1.7 over $e \in I_p$, $p^e \le a + w$; then Problems 49.1.5, 49.1.6 and 49.1.4, and $\gamma_p + \rho = 1/(p-1)$.
49.1.9: Compare $z - \min(z, z')$ with $(z - z')_+$, and expand $\gamma_p(a + w)$ by Problem 49.1.1.
49.1.10: Rescale the denominator of F_1. For the mixed jets, compare the valuations of Problem 17.4.4 directly with $\mathcal{D}(a, w)$.

§49.2.

49.2.1: Treat $h = 0$ separately; otherwise look at an entry of least valuation. For several forms, take the next form on the current rows.
49.2.3: Problem 49.1.9 for each term, $\sum_\tau (\beta_1(\tau) + \|\beta\|_{>1}(\tau)) = |\beta|$, and Problem 49.1.1; treat $e = 0$ separately. For the variables, $\sum_{h<n} h \le n^2$.

§49.3.

49.3.1: (i) Use $y_1 = 1$, $y_2 = p$ in Problems 49.1.5, 49.1.6 and 49.1.4. (ii) $\mathcal{D}(\beta \smallsetminus \Phi')$ has only the terms $(w/p^e)_+$.
49.3.2: Sage. No odd shift returns to the identity place, so $\mathcal{D} = \gamma_{13} A$.

References

[GL] L. Sernau, *GRH for Dirichlet L-functions, in Lean 4*, a shorter rewriting of the Lean proof, text by Claude, `https://github.com/lsernau/grh-lean`, commit `72fead1`, readable edition `grh/`.

ONE LIFT AT A SMALL NON-SPLIT PRIME

Prerequisites. Chapter 33: the scales, ranks and weights, in particular $x_1 \mid a$ and $a/x_1 \le \kappa(\tau) \le b$ (Problem 33.4.1), and that x is very large. Chapter 34: the gap Δ, the weights κ_j (Section 34.2), the integral vacuum (Section 34.8), the diagram of the data (Definition 34.2.1), and the valuation val and the ring $\mathcal{O}_\eta$ of its opening paragraph. Chapter 48: c_p, I_p, $s_{\mathrm{fin},p}$, $\mathrm{gain}(p)$ (Section 48.1), collisions and $C_p(\Phi')$ (Section 48.2), the gauge $\|\omega\|_g$ of a Weyl vector and $\gamma_p = 1/(p-1) - \rho(d,p)$ (Section 48.3). Chapter 49: diagrams, β_1, $\beta_{>1}$, $\|\beta\|_{>1}$, $|\beta|$ (Definition 49.2.1), the erased diagram $\beta \smallsetminus \Phi'$ (Definition 49.2.2) and the predicted divisibility $\mathcal{D}(\beta)$ (Definition 49.2.3). Chapter 17, Section 17.5: the exponent set I_p°, couplings, the normal form, standard fillings, products of minors P_μ, and Theorem 17.5.1. Chapter 43: the definite chain with its data (Section 43.4); we write $\mathrm{Heis}(y)$ for the finite Heisenberg translation by y. The residue field $\bar{\mathbb{F}}_p$ of $\mathcal{O}_{\mathbb{C}_p}$, which is infinite.

How divisible by p is a single lift of the chain, and where does it fall short of $\mathrm{gain}(p)/m$? Chapter 48 composes m lifts and needs, at each stage, a bound for the kernel of the lift at a prime $p < x_1$ with $\chi_K(p) \neq 1$ (its inputs (ii) and (iii) in Section 48.3). The stage bound deducts a logarithmic counting term from the predicted divisibility of the diagram of the lift and credits each erased box; we compare it with $\mathrm{gain}(p)/m$, allowing a uniform error and the collision sum. We work it out first on a model of the places, then for the data, and finally state how the bound reaches the kernel.

50.1. The stage bound

Recall (Definitions 49.2.1 and 49.2.2) that a diagram β is read at heights below a fixed bound, the number of rows; $\beta_1(\tau)$ is its number of columns of height one at τ, $\beta_{>1}(\tau)$ the number of its other columns, $\|\beta\|_{>1}(\tau)$ the number of boxes in these, and $|\beta|$ the number of all its boxes; $\beta \smallsetminus \Phi'$ deletes the columns of height one at the places of Φ'. With $\tau_e := [-p^e]\tau$,

$$\mathcal{D}(\beta) = c_p \sum_{e \in I_p} \sum_{\tau \in \Phi} \Big[\Big(\frac{\beta_1(\tau)}{p^e} - \beta_1(\tau_e) - \beta_{>1}(\tau_e) \Big)_+ + \Big(\frac{\|\beta\|_{>1}(\tau)}{p^e} - \|\beta\|_{>1}(\tau_e) \Big)_+ - \frac{\beta_{>1}(\tau)}{p^e} \Big] - [p = d] \, \frac{1}{2} \sum_{\tau \in \Phi} \mathrm{rc}(\tau),$$

with (a notation of this chapter) $\mathrm{rc}(\tau) := \min(\beta_1(\tau), \beta_1(\tau_0) + \beta_{>1}(\tau_0)) + \beta_{>1}(\tau) + \min(\|\beta\|_{>1}(\tau), \|\beta\|_{>1}(\tau_0))$ (Definition 49.2.3). The diagram of the data (Definition 34.2.1) has

$$\beta(\tau,1) = a \, \mathbf{1}_{\Phi_a}(\tau), \qquad \beta(\tau,k) = \kappa_1(\tau) - \Big\lfloor \frac{k+t+1}{2} \Big\rfloor,$$

$\beta(\tau,h) = \Delta - (t+1)$ if $h > k$ and $(t+1) \mid h-k$, and $\beta(\tau,h) = 0$ otherwise. For $0 \le j < m$ we read it at heights below n_{j+1} and keep the letter β.

Date: November 26, 2026.

Definition 50.1.1. Let p be a prime with $\chi_K(p) \neq 1$, $j \geq 0$, $\Phi' \subseteq \Phi$, and β the diagram of the data read at heights below n_{j+1}. The *stage bound* is

$$\mathcal{D}_j(\Phi') := \mathcal{D}(\beta \smallsetminus \Phi') + \gamma_p\big(|\beta| - |\beta \smallsetminus \Phi'|\big) - f n_{j+1}^3\big(1 + \log_p \max(|\beta|, 1)\big).$$

Problem 50.1.1. Let $0 \leq j < m$. Read at heights below n_{j+1}, the diagram of the data has $\beta_1(\tau) = a\,\mathbf{1}_{\Phi_a}(\tau)$, $\beta_{>1}(\tau) \leq \kappa(\tau) + x^{60}$ and $k\kappa(\tau) \leq \|\beta\|_{>1}(\tau) \leq k\kappa(\tau) + x^{60}$ for every $\tau \in \Phi$.

50.2. A model on $(\mathbb{Z}/40)^\times$

For $\tau \in \Phi_a$ and $e \in I_p$, the first positive part in $\mathcal{D}(\beta)$ compares a/p^e with $\beta_1(\tau_e) + \beta_{>1}(\tau_e)$; so does $s_{\mathrm{fin},p}(a, \tau)$, with $\kappa(\tau_e)$ in place of the columns. We follow the comparison on a model.

Problem 50.2.1. By Problem 49.1.1, $c_p \sum_{e \in I_p} p^{-e} = \gamma_p$. Deduce that $\gamma_p = p/(p^2 - 1)$ if $\chi_K(p) = -1$, and $\gamma_p = 1/(2d - 2)$ if $p = d$.

The *model*: $\Phi = (\mathbb{Z}/40)^\times$ with $[\nu]$ the class of ν for $(\nu, 40) = 1$, $q_0 = 8$, $\Phi_a = \{\tau \equiv 1 \bmod 8\}$, $\Phi_b = \{7\}$, $x = 6$, $b = 343$, $a = xb = 2058$, $x_1 = 49$, $k = 2$, $\kappa = b$ on Φ_b and $\kappa = a/x_1 = 42$ elsewhere. The primes 3, 7 are treated as inert: $c_p = 1$, I_p is the set of odd $e \geq 1$, and $\gamma_p := c_p \sum_{e \in I_p} p^{-e} = p/(p^2 - 1)$. The *model diagram* has a columns of height one at each a-place, $\kappa(\tau)$ columns of height k at every τ, and no others; it is read at heights below 3. These numbers are not data ($18480 \nmid 8$); the model keeps only the bookkeeping.

Problem 50.2.2. In the model, -3 has order 2 modulo 8, and at $p = 3$ no pair is a collision. At $p = 7$, $-7 \equiv 33 \pmod{40}$, the powers of 33 are $\{1, 33, 9, 17\} = \Phi_a$, and every (τ, e) with $\tau \in \Phi_a$ and e odd is a collision outside $\varnothing$.

Problem 50.2.3. In the model, $\mathrm{gain}(3)/m = 25718/9$ and $\mathrm{gain}(7)/m = 1022$; moreover $C_7(\varnothing) = 2401/2$ and $C_7(\{1, 9\}) = 0$.

In the next three problems β is any diagram with $\beta_1 = a\,\mathbf{1}_{\Phi_a}$ and, for some real $\varepsilon \geq 0$ (a letter of this chapter only) and every τ, $\beta_{>1}(\tau) \leq \kappa(\tau) + \varepsilon$ and $k\kappa(\tau) \leq \|\beta\|_{>1}(\tau) \leq k\kappa(\tau) + \varepsilon$; $\Phi' \subseteq \Phi$, and β_1, $\beta_{>1}$, $\|\beta\|_{>1}$ in the terms of $\mathcal{D}(\beta \smallsetminus \Phi')$ are those of $\beta \smallsetminus \Phi'$ (only β_1 changes). The model diagram is the case $\varepsilon = 0$ with equalities.

Problem 50.2.4. $(\|\beta\|_{>1}(\tau)/p^e - \|\beta\|_{>1}(\tau_e))_+ \geq k(\kappa(\tau)/p^e - \kappa(\tau_e))_+ - \varepsilon$, with equality and $\varepsilon = 0$ for the model diagram.

Problem 50.2.5. Let $\tau \in \Phi_a \smallsetminus \Phi'$ and $e \in I_p$. If $\tau_e \notin \Phi_a \smallsetminus \Phi'$, the first positive part inside the brackets defining $\mathcal{D}(\beta \smallsetminus \Phi')$ at (τ, e) is at least $(a/p^e - \kappa(\tau_e))_+ - \varepsilon$. If (τ, e) is a collision outside Φ', it is 0, which is at least $(a/p^e - \kappa(\tau_e))_+ - a/p^e$.

Problem 50.2.6. Let $1 \in I_p$, $p < x_1$, and $\kappa \geq a/x_1$ on Φ. For every τ, $\gamma_p a \geq c_p \sum_{e \in I_p} (a/p^e - \kappa(\tau_e))_+ + c_p a/x_1$.

Problem 50.2.7. In the model, let $p \in \{3, 7\}$, β the model diagram and $\Phi' \subseteq \Phi$. Then

$$\mathcal{D}(\beta \smallsetminus \Phi') + \gamma_p a\,\#(\Phi_a \cap \Phi') \;\geq\; \frac{\mathrm{gain}(p)}{m} - C_p(\Phi') + \#(\Phi_a \cap \Phi')\,\frac{a}{x_1} - \gamma_p \sum_{\tau \in \Phi} \kappa(\tau).$$

Problem 50.2.8. In the model, at $p = 3$ and $\Phi' = \varnothing$ both sides of Problem 50.2.7 equal 179473/72. At $p = 7$ the left side is $-6139/48$ for $\Phi' = \varnothing$ (the right side is $-15379/48$); for $\Phi' = \{1, 9\}$ it is 46865/48 and the right side is 46277/48, a slack of 49/4.

50.3. The data

Now let β be the diagram of the data read at heights below n_{j+1}, $0 \le j < m$, and let $p < x_1$ be a prime with $\chi_K(p) \neq 1$. In this section take $\varepsilon = x^{60}$.

Problem 50.3.1. (i) If $p^e \ge x_1$, then $(a/p^e - \kappa(\tau_e))_+ = 0$ and $(\kappa(\tau)/p^e - \kappa(\tau_e))_+ = 0$; and $2c_p\lceil \log_p x_1 \rceil x^{60} \le a/(pm)$. (ii) $\gamma_p \beta_{>1}(\tau) \le a/(pm)$ for every τ. (iii) $n_{j+1}^3(1 + \log_p \max(|\beta|, 1)) \le a/(pm)$.

Problem 50.3.2. Let $p = d$. For every τ, the places τ and $\tau_0 = [-1]\tau$ are neither both in Φ_a nor both in Φ_b, and $\mathrm{rc}(\tau) \le 3a/(dm)$, also for $\beta \smallsetminus \Phi'$ in place of β. Hence the correction $\frac{1}{2}\sum_\tau \mathrm{rc}(\tau)$ is at most $2fa/(dm)$.

Problem 50.3.3. For every $\Phi' \subseteq \Phi$, $\mathcal{D}_j(\Phi') \ge \mathrm{gain}(p)/m - C_p(\Phi') + c_p\,\#(\Phi_a \cap \Phi')\,a/x_1 - 5fa/(pm)$. Deduce part (b) of Theorem 50.4.4.

50.4. One kernel

Fix a twist ϑ and $j \ge 0$. A *datum* of the lift is an element of the finite part of the Schwartz space of $\mathrm{Hom}(X_j, X_{j+1})$, the complex span of the finite Heisenberg translates of the vacuum. For a datum φ, let $\mathcal{J}_\varphi$ denote, in this chapter, the kernel of the definite lift from X_j to X_{j+1} built from ϑ, evaluated at φ (Section 43.4): a linear map from the Weyl vectors of the weight of X_j to those of X_{j+1}. Its diagram is β read at heights below n_{j+1}. Fix a prime p and a ring map $\eta\colon \mathbb{C} \to \mathbb{C}_p$.

Definition 50.4.1. Let $\delta \in \mathcal{O}_K$. A *standard datum of denominator* δ on $\mathrm{Hom}(X_j, X_{j+1})$ is an element of the $\mathcal{O}_\eta$-span of the translates by $\mathrm{Heis}(y)$ of the integral vacuum, over the finite adelic y such that δy is integral at every finite place of E above p.

Definition 50.4.2. A datum φ *multiplies gauges by at most* $c \in \mathbb{R}$ if $\|\mathcal{J}_{(g,g')\varphi}\,\omega\|_{g'} \le \max(c, 0)\,\|\omega\|_g$ for all finite adelic points g of the unitary group of X_j, g' of that of X_{j+1}, and all Weyl vectors ω; here $(g, g')\varphi$ is the translate of φ under the Weil representation.

Definition 50.4.3. The *jet series* of a datum φ at scale $c_0 \in \mathbb{C}$ is the Taylor series at 0 of $z \mapsto \mathrm{th}_\varphi(c_0 z)$, where th_φ is the theta function of φ, an entire function of a family $z = (z_\tau)_{\tau\in\Phi}$ of $n_{j+1} \times n_j$ matrices in the standard bases of X_{j+1} and X_j. The *jet scale* is $c_{\mathrm{jet}} := c_{\mathrm{per}}\sqrt{2\pi/\sqrt{d}}/\Omega_0$ (`Parameters.jetScale`), where c_{per} is the period factor fixed in the proof (`Parameters.periodFactor`) and Ω_0 (a letter of this chapter) is the complex number fixed in the proof (`Parameters.cmPeriod`) such that $\Omega_0\mathcal{O}_K$ is the period lattice of the CM curve of K (`Parameters.latticeModule_cmCurve`). A *jet* of a series F is $Q(\partial)F(0)$ for a polynomial Q.

The kernel of the lift is the theta kernel at scale $\pi_M c_{\mathrm{jet}}$ (`Data.liftKernel`), and $|\eta\pi_M| \le 1$ (`Data.norm_star_piMBar_le_one`) [GL]. Four statements are read from the proof [GL].

(I) Integrality. If $\delta \neq 0$ and φ is standard of denominator δ, then every jet of its jet series at scale $\bar{\delta} dc_{\mathrm{jet}}$, along a polynomial with coefficients in $\mathcal{O}_\eta$, is integral at η.

Problem 50.4.1. Let F be a power series over $\mathbb{C}_p$, $c' \in \mathbb{C}_p$, and Q homogeneous of degree l over $\mathbb{C}_p$. Then $Q(\partial)[F(c'z)](0) = c'^l Q(\partial)F(0)$. Hence, under (I), for $c \in \mathbb{C}$ and homogeneous Q of degree l with coefficients in $\mathcal{O}_\eta$, the jet along Q of the jet series of φ at scale cc_{jet} has absolute value at most $|\eta(c/(\bar{\delta}d))|^l$ after η.

(II) Kernel and jets. Let $c_0 \in \mathbb{C}$ and $\mathfrak{b} \in \mathbb{R}$. If every entry of $\mathrm{schur}_\beta(\partial)F(0)$ has absolute value at most $\mathfrak{b}$ after η, for the jet series F at scale c_0 of every standard datum of denominator δ, then every standard datum of denominator δ multiplies the gauges of the theta kernel at scale c_0 by at most $\mathfrak{b}$. Here $\mathrm{schur}_\beta(z)$ is the matrix, in the bases of standard fillings, of the map of Weyl modules of shape β induced by z; its entries are polynomials with integral coefficients (`schur`; for the change of coefficients `map_schur`).

(III) Schur entries. If no column of β has height strictly between n_j and n_{j+1} (note $n_j < n_{j+1}$), then for every series F over $\mathbb{C}_p$ and every entry of $\mathrm{schur}_\beta(\partial)F(0)$ there is an integral family μ such that the absolute value of the entry is at most $|P_\mu(\partial)F(0)|$, for the product of minors P_μ of the output filling indexing the row of that entry.

Problem 50.4.2. A polynomial over $\mathcal{O}_{\mathbb{C}_p}$ in finitely many variables with a unit coefficient takes a unit value at some point with integral coordinates.

Problem 50.4.3. For every $j \geq 0$, the diagram of the data has no column of height h with $n_j < h < n_{j+1}$.

(IV) Normal form. Let $\chi_K(p) \neq 1$, φ a standard datum of denominator 1 and $c \in \mathbb{C}$ with $|\eta c| \leq 1$. Then the jet series of φ at scale cc_{jet}, read in $\mathbb{C}_p$ through η, has the normal form of Section 17.5 for the exponents I_p°, the partner rule $([-p^e]\cdot)_e$, some ϖ with $\operatorname{val}\varpi = 1/(p-1) - \gamma_p$, and some integral family of coefficients.

Status: (I)–(IV) are read from the proof; (III) uses the standard basis theorem [DEP] and (IV) Lubin–Tate theory [LT]; for the formal group of an elliptic curve see [AEC, Ch. IV, §§1–2].

Problem 50.4.4. Let $\chi_K(p) \neq 1$. For every standard datum of denominator 1, with jet series F at scale $\pi_M c_{\mathrm{jet}}$ read through η, every standard filling and every integral family μ,

$$\operatorname{val}\big(P_\mu(\partial)F(0)\big) \;\geq\; \mathcal{D}(\beta) - f n_{j+1}^3 \big(1 + \log_p \max(|\beta|, 1)\big) = \mathcal{D}_j(\varnothing).$$

Hence every standard datum of denominator 1 multiplies gauges by at most $p^{-\mathcal{D}_j(\varnothing)}$.

This is part (a) of the following theorem; part (b) was proved in Section 50.3, and Problem 50.2.7 is its model.

Theorem 50.4.4. *Let p be a prime and $\eta\colon \mathbb{C} \to \mathbb{C}_p$ a ring map.*

(a) *If $\chi_K(p) \neq 1$, then for every twist ϑ, every $j \geq 0$ and every standard datum φ of denominator 1 on $\mathrm{Hom}(X_j, X_{j+1})$, φ multiplies gauges by at most $p^{-\mathcal{D}_j(\varnothing)}$.*

(b) *If $p < x_1$ and $\chi_K(p) \neq 1$, then for every $0 \leq j < m$ and every $\Phi' \subseteq \Phi$,*

$$\mathcal{D}_j(\Phi') \;\geq\; \frac{\mathrm{gain}(p)}{m} - C_p(\Phi') + c_p \,\#(\Phi_a \cap \Phi')\,\frac{a}{x_1} - \frac{f a (\log b)^2}{mp}.$$

Problem 50.4.4 deduces part (a) from (II)–(IV) and Theorem 17.5.1. Statement (I) and Problem 50.4.1 give the jet integrality behind input (i) of Section 48.3. Part (a) is the single-kernel estimate in input (ii) there, and part (b) is input (iii); Problem 48.3.2 uses them with $\Phi' = \varnothing$.

50.5. The size of a collision sum

How much can collisions cost? Problem 48.4.2 of Chapter 48 uses the crude bound $mC_p(\varnothing) \le j_p := \lceil 2mfa/p \rceil$.

Problem 50.5.1. In a second model let $\Phi = (\mathbb{Z}/4)^\times$, let both places be a-places, $a = 24$, and treat $p = 5$ as inert, so that I_5 is the set of odd $e \ge 1$ and $[-5^e]$ exchanges the two places for every $e \in I_5$. Then $C_5(\varnothing) = 10$; with $f = 2$ and $m = 8$, $mC_5(\varnothing) = 80 \le j_5 = 154$.

What has been established. Theorem 50.4.4. Problem 50.4.4 deduces part (a) from (II)–(IV) and Theorem 17.5.1. Part (b), proved by Problems 50.1.1–50.3.3, bounds the shortfall of the stage bound from $\mathrm{gain}(p)/m$ by $C_p(\Phi') + fa(\log b)^2/(mp) - c_p\,\#(\Phi_a \cap \Phi')\,a/x_1$; each erased long row receives the credit $\gamma_p a$ in the definition of the stage bound. Section 48.3 adds the exponents $\mathcal{D}_j$ along the chain of m lifts, and at an exceptional prime a full mark makes the collision sum outside its induced places zero (Problem 48.4.1).

In the Lean formalization. In the Lean proof [GL] (paths relative to `grh/src/`; the namespace `New.` is omitted from names), Theorem 50.4.4(a) is `Data.mem_raises_neg_divisibilityBound` (`New/UpperBound/Divisibility/ValuationAtNonSplitPrimes.lean`) and (b) is `Data.le_divisibilityBound` (`New/UpperBound/Divisibility/JetExponent.lean`), with $\mathcal{D}_j(\Phi')$ `Data.divisibilityBound`. Standard data, "multiplies gauges by at most" and the jet series are `Parameters.standardData`, `Kernel.raises` (at base points $1, 1$) and `Space.jetSeries`. Statements (I)–(IV) specialize `Parameters.norm_jet_jetSeries_le_one`, `Parameters.omega_mem_raises_of_schurJet_le`, `exists_norm_schurJet_le_norm_jet_minorProd` and `Parameters.exists_hasNormalForm_jetSeries`; in (II) the three translating points of the declaration are taken to be 1.

Hints

§50.1.

50.1.1: Below n_{j+1} the possible heights are 1, k and $k+i(t+1)$ with $1 \le i \le j$; height 1 occurs exactly at the a-places. Use $\kappa_1 = \kappa + \frac{3}{2}\Delta$, $\Delta = 2r^8$, $r \le 3x^5$, $m \le 2\sqrt{x}$.

§50.2.

50.2.1: Two geometric series.

50.2.3: At $p = 3$ only $e \in \{1, 3\}$ contribute, at $p = 7$ only $e = 1$ to $s_{\mathrm{fin},p}$; C_7 is a geometric series.

50.2.4: $(y - z)_+$ is increasing in y and decreasing in z.

50.2.5: In the first case $\beta_1(\tau_e) = 0$ after erasure.

50.2.6: Problem 50.2.1; compare the terms $e = 1$, using $p < x_1$ and $\kappa \ge a/x_1$.

50.2.7: Problems 50.2.4–50.2.6 with $\varepsilon = 0$; the last term of $\mathcal{D}$ is $-\gamma_p \sum_\tau \kappa(\tau)$ by Problem 50.2.1.

§50.3.

50.3.1: (i) $\kappa \geq a/x_1$ and $\kappa \leq b \leq a$. (ii) $\gamma_p \leq 2/p$ and Problem 50.1.1. (iii) $|\beta| \leq fa + f(kb + x^{60})$, $n_{j+1} \leq n_m$, and $a/(pm) \geq (x/m)(b/x_1)$; the scale inequalities of Chapter 33 make x/m and b/x_1 huge.

50.3.3: Use the row comparisons only for $p^e < x_1$; Problem 50.2.6 is already summed over e. Count the low columns, the correction at d and the logarithmic term separately. For the final deduction use $(\log b)^2 \geq 5$.

50.3.2: τ_0 has class $-c$ modulo q_0 if τ has class c. Bound each of the three terms of $\mathrm{rc}(\tau)$ by $a/(dm)$.

§50.4.

50.4.1: Compare monomials; the jet series at scale cc_{jet} is that at scale $\bar{\delta}dc_{\mathrm{jet}}$ with z replaced by $(c/(\bar{\delta}d))z$.

50.4.2: Reduce modulo the maximal ideal; $\bar{\mathbb{F}}_p$ is infinite.

50.4.3: $n_j = k + j(t+1)$.

50.4.4: (IV) and Theorem 17.5.1 for each standard datum; the directions in (III) may depend on the entry, so use the common bound in (II). Extend β by $\beta(\tau, 0) = 0$ when comparing $\mathcal{D}(\beta)$ with the predicted divisibility of Theorem 17.5.1.

§50.5.

50.5.1: Count the collisions for each $e \in I_5$.

References

[AEC] J. H. Silverman, *The Arithmetic of Elliptic Curves*, 2nd ed., Springer, 2009.

[DEP] C. De Concini, D. Eisenbud and C. Procesi, Young diagrams and determinantal varieties, *Invent. Math.* **56** (1980), 129–165.

[GL] L. Sernau, *GRH for Dirichlet L-functions, in Lean 4*, a shorter rewriting of the Lean proof, text by Claude, `https://github.com/lsernau/grh-lean`, commit `72fead1`, readable edition `grh/`.

[LT] J. Lubin and J. Tate, Formal complex multiplication in local fields, *Ann. of Math.* **81** (1965), 380–387.

THE SIZE OF THE COMPOSITE LIFT

Prerequisites. Stirling's formula; exterior powers and the singular value decomposition of a complex matrix [HJ, §2.6]. From Chapter 33: the data (Definition 33.3.1), the weights κ, the prime sums s_{fin}, the sizes s_∞, Ω, h_{main}, s_{main}, rem and U (Section 33.4), and the level primes (Section 33.5). From Chapter 34: the places Φ, Φ_a, the spaces X_j, Y_j, the source forms S, whose values lie in Weyl modules with their Weyl (Gram) norms, the lift weights κ_j, the gap $\Delta = 2r^8$, and the diagram $\beta(\tau, h)$ (Definition 34.2.1). From Chapter 48, Section 48.1: c_p, I_p, $s_{\mathrm{fin},p}$ and gain(p); and weak chain data (Definition 48.3.2), the restricted chain $R_{\vartheta,\Psi}$ (Definition 48.3.3) and the expansion of a chain datum into a weak one (Theorem 48.3.4). From Chapter 43, Section 43.4: translations $\mathfrak{t}$, translated vacua $v_j(\mathfrak{t})$, chain data and the composite lift $B_{\vartheta,\Psi}$ with its restriction to Y_m. From Chapter 50: the jet scale c_{jet} (Definition 50.4.3) and the kernel of one lift (Section 50.4). The Chowla–Selberg formula, Theorem 20.3.1; the Fock norm $\|z^a\|^2 = a!$ of Problem 5.4.4; Chapter 23 for the smallest definite lifts.

Theorem A (Chapter 42) compares the size of the composite lift with its divisibility. Chapter 48 treats the divisibility; this sheet treats the size. How large can $B_{1,\Psi}\varphi$ be on every conjugate, if φ is small? The answer has two halves. At one pair of points the kernel of lift j multiplies conjugate Weyl norms by at most $\exp(x^{50} + \mathrm{rs}_j/2)$, where rs_j sums $s_\infty(l)$ over its rows at all places (Section 51.2): a Gaussian integral, and one factorial $l!$ per row of length l. The finite prime sums cancel exactly against the gains (Problem 51.1.4), and at each long place the level N pays for the excess of $m\, s_\infty(a)$ over $m\, s_{\mathrm{main}}$ up to $32a \log b$ (Problem 51.1.7).

51.1. The exponent

We recall the global prime sums and sizes from Chapter 33 and the local gains from Chapter 48. The places Φ are identified with $(\mathbb{Z}/q_1)^\times$, $[\nu]$ is the place of the residue class of an integer ν if $\gcd(\nu, q_1) = 1$, and the identity place otherwise, and Φ_a is the set of a-places. Recall $s_\infty(j) = \log j! + j \log(M/\Omega)$ with $\Omega = e^{\mathrm{CS}(d)}\, 2\pi/\mathrm{rd}_E$, $c_1 = -1 - \mathrm{CS}(d)$, $s_{\mathrm{main}} = a(\log a - \frac{1}{f}\sum_{\tau\in\Phi} \log \kappa(\tau) + c_1)$, $h_{\mathrm{main}} = mk \sum_{\tau\in\Phi}(s_\infty(\kappa(\tau)) - s_{\mathrm{fin}}(\kappa(\tau), \tau))$ and $\mathrm{rem} = \sum_{\tau\in\Phi_a}(s_{\mathrm{fin}}(a, \tau) - s_{\mathrm{main}})$. Let Π be the set of primes $p < x_1$ with $\chi_K(p) \neq 1$ (Section 48.1), and put, in Part VIII,

$$\Sigma = \sum_{p\in\Pi} \mathrm{gain}(p) \log p.$$

We use the following consequences of Chapter 33 (Definition 33.3.1 and Problems 33.2.3, 33.4.1, 33.4.4 and 33.5.4): $x_1 \le a$; $a/x_1 \le \kappa(\tau) \le b \le a$ for every τ; $20 \log b \le \log(M/\Omega) \le 23 \log b$ (Problem 33.4.3); $s_\infty(j) \ge 0$ for integers $0 \le j \le a$; $\log N \ge L_-(\kappa, m, M, \log b)$, as in Definition 33.3.1; $m(1 + \frac{1}{2}\log a) \le a \log b$; and $\log(M \mathrm{rd}_E/2\pi) \le 23 \log b$.

Date: November 26, 2026.

Problem 51.1.1. For a prime power $\nu = p^e$, $e \geq 1$, one has $\Lambda(\nu)(1 - \chi_K(\nu)) = 2c_p \log p$ if $e \in I_p$, and 0 otherwise.

Problem 51.1.2. For every integer $P_0 \geq \lceil x_1 \rceil$, real $y \leq a$ and $\sigma \in \Phi$, $s_{\mathrm{fin}}(y, \sigma) = \sum_{p<P_0} 2\, s_{\mathrm{fin},p}(y, \sigma) \log p$, the sum over primes; in particular one may sum over $p < x_1$.

Problem 51.1.3. If $\chi_K(p) = 1$ or $p \geq x_1$, then $\mathrm{gain}(p) = 0$. Consequently

$$2\Sigma = m \sum_{\tau \in \Phi_a} s_{\mathrm{fin}}(a, \tau) + mk \sum_{\tau \in \Phi} s_{\mathrm{fin}}(\kappa(\tau), \tau).$$

Problem 51.1.4. $h_{\mathrm{main}} - m\,\mathrm{rem} + 2\Sigma = m\,\#\Phi_a\, s_{\mathrm{main}} + mk \sum_{\tau \in \Phi} s_\infty(\kappa(\tau))$.

Problems 51.1.2 and 51.1.3 recall Problems 48.1.4 and 48.1.3 in the form used here. The prime sums have cancelled.

Problem 51.1.5. For every integer $n \geq 1$, $\log n! \leq n \log n - n + 1 + \frac{1}{2} \log n$.

Problem 51.1.6. $\log(M/\Omega) = 1 + c_1 + \log(M \mathrm{rd}_E / 2\pi)$, and

$$s_\infty(a) - s_{\mathrm{main}} \leq a\Big(\frac{1}{f} \sum_{\tau \in \Phi} \log \kappa(\tau) + \log \frac{M \mathrm{rd}_E}{2\pi}\Big) + 1 + \tfrac{1}{2} \log a.$$

Problem 51.1.7. $m(s_\infty(a) - s_{\mathrm{main}}) - a \log N \leq 32\, a \log b$.

Put $C_{\mathrm{ch}} = m\big(\#\Phi_a\, s_\infty(a) + k \sum_{\tau \in \Phi} s_\infty(\kappa(\tau))\big)$.

Problem 51.1.8. $C_{\mathrm{ch}} - \#\Phi_a\, a \log N \leq h_{\mathrm{main}} - m\,\mathrm{rem} + 2\Sigma + 32\, f a \log b$.

For $n = 6$ the two sides of Problem 51.1.5 compare as follows.

Problem 51.1.9. $\log 6! + 6(1 - \log 6) = 1.8286\ldots \leq 1 + \frac{1}{2} \log 6 = 1.8958\ldots$.

51.2. One kernel in one coordinate

Where does s_∞ come from? In the proof the conjugate of a theta jet of a moved translate of the integral vacuum is written as a Gaussian integral of a conjugated polynomial against the vacuum $e^{-\sum_i |y_i|^2/2}$ and a bounded function [GL]. In this sheet l denotes the length of a row, $L \geq 1$ a growth rate, and v, t_0, u are real numbers.

Problem 51.2.1. For $\rho \geq 0$, $l \in \mathbb{N}$ and $v \in \mathbb{R}$, $\rho^l \leq l!\, \exp(lv + \rho e^{-v})$.

Problem 51.2.2. In the one-coordinate model let $l \geq 0$ be an integer, $t_0 > 0$, $L \geq 1$ and $u \geq 0$. If $z \in \mathbb{C}$ and $|z|^2 \leq t_0(2L + 2)u$, then

$$|z|^l \leq \exp\Big(\tfrac{1}{2}\big(l/L + \log l! + l \log t_0\big) + Lu\Big).$$

For a matrix the same device is applied to each row of a diagram. In one variable the Fock norm $\|z^l\|^2 = l!$ of Problem 5.4.4 shows the same factorial.

Problem 51.2.3. Let $n \geq 1$ and let Z be a complex $n \times n$ matrix and $\rho_0 \geq \rho_1 \geq \cdots \geq \rho_{n-1}$ the eigenvalues of Z^*Z. For $1 \leq h \leq n$ the operator norm of $\wedge^h Z$, for the inner product induced on $\wedge^h \mathbb{C}^n$, satisfies $\|\wedge^h Z\|^2 = \rho_0 \rho_1 \cdots \rho_{h-1}$. For $l \geq 1$, with the inner product on $\mathrm{Sym}^l \mathbb{C}^n \subseteq (\mathbb{C}^n)^{\otimes l}$ induced from the tensor power, $\|\mathrm{Sym}^l Z\|^2 \leq \rho_0^l$.

A column of height h carries $\wedge^h$, a row of length l carries Sym^l; a general diagram mixes both, and the proof uses the following bound. *Schur norm.* For each τ in a finite set let z_τ be a complex $n'_\tau \times n_\tau$ matrix with $n_\tau \le n'_\tau$, let $b_{\tau,h}$ be numbers of columns of height h, with $b_{\tau,h} = 0$ for $n_\tau < h < n'_\tau$, and put $l_{\tau,i} = \sum_{i<h<n'_\tau} b_{\tau,h}$. There are $\rho_{\tau,i} \ge 0$, $0 \le i < n_\tau$, with $\sum_{i<n_\tau} \rho_{\tau,i}$ at most the sum of the squared absolute values of the entries of z_τ for each τ, such that the Schur matrix of (z_τ) multiplies the squared Weyl norm of every vector by at most $\prod_\tau \prod_{i<n_\tau} \rho_{\tau,i}^{l_{\tau,i}}$. *Status*: classical linear algebra (singular values); read from the proof [GL].

Problem 51.2.4. Let $L \ge 1$ and $s' \in \mathbb{R}$. Then $Ls'/(2L+2) - s'/2 = -s'/(2L+2)$, and $\frac{1}{\pi}\int_{\mathbb{C}} e^{-|y|^2/c}\,dA(y) = c$ for $c > 0$. For $L = 2$, $\int_0^\infty 2re^{-r^2/6}\,dr = 6 = 2L+2$.

Problem 51.2.5. Let $l \ge 0$ be an integer, $t_0 > 0$, $L \ge 1$, $\mathrm{gr}(l) = \frac{1}{2}(l/L + \log l! + l\log t_0)$, and $H\colon \mathbb{C} \to \mathbb{C}$ measurable with $|H| \le 1$. Then

$$\Big|\frac{1}{\pi}\int_{\mathbb{C}} (\sqrt{t_0}\,y)^l e^{-|y|^2/2} H(y)\,dA(y)\Big| \le e^{\mathrm{gr}(l)}(2L+2),$$

and the Gaussian $\exp(-\sum_i |y_i|^2/(2L+2))$ in n_{c} complex coordinates has integral $(2L+2)^{n_{\mathrm{c}}}$ for the measure $\pi^{-n_{\mathrm{c}}} dA$.

The lift takes its Taylor series at the scale $\pi_M c_{\mathrm{jet}}$, with c_{jet} the jet scale of Definition 50.4.3. For each σ over K the conjugation law below gives a comparison scale t_σ with $|t_\sigma|^2 = 1/\Omega$, and $|\sigma(\pi_M)|^2 = M$; so the growth parameter is $t_0 = |\sigma(\pi_M)t_\sigma|^2 = M/\Omega$, and $2\,\mathrm{gr}(l) = l/L + s_\infty(l)$. Every automorphism of $\mathbb{C}$ gives the same absolute values as one over K [GL]. With $L = a+1$, $l/L \le 2$ for $l \le 2a$. The computation of $|t_\sigma|^2$ uses the area of the conjugate lattice, the Chowla–Selberg unit and the normalization of the vacuum [GL]; the next two inputs enter it.

Conjugates of translated theta functions. Let $d \equiv 7 \pmod 8$ be the prime of the data. A *normalized CM lattice* is a lattice $\Lambda \subset \mathbb{C}$ stable under $\mathcal{O}_K$, with a point $t' \in \mathbb{C}$ of exact order two modulo Λ such that $(1 \pm \sqrt{-d})t'/2 \notin \Lambda$, scaled so that $\wp''_\Lambda(t') = 2$, with a chosen a_1 such that $a_1^2 = 12\wp_\Lambda(t')$; for a lattice D write $T_v^D f(z) = \exp(-\pi(z\bar v + |v|^2/2)/\operatorname{area}(D))f(z+v)$, and let θ be the normalized theta section of Λ of [GL] (the twisted translate by t' of the lattice sigma function, divided by its value at 0). Suppose $\Lambda = \omega_0\mathcal{O}_K$, and let σ be an automorphism of $\mathbb{C}$ over K. There are $\omega' \in \mathbb{C}^\times$, a nonzero ideal $\mathfrak{a}$ of $\mathcal{O}_K$ and a finite adele $\mathfrak{b}$ of K such that the lattice Λ' of the conjugate curve is $\omega'\mathfrak{a}^2/\mathrm{Nm}\,\mathfrak{a}$, has area $|\omega'|^2\sqrt{d}/2$ and contains $n_0\omega'$ for some integer $n_0 \ge 1$; and, with θ' defined in the same way from the conjugate marked lattice, for every $y \in K$ and every $y' \in K$ close enough to $\mathfrak{b}y$ in the finite adeles, applying σ coefficientwise to the Taylor series at 0 of $T^{\Lambda}_{y\omega_0}\theta$ gives the Taylor series at 0 of $T^{\Lambda'}_{y'\omega'}\theta'$. *Status*: this theta formulation is read from the proof [GL]; for the classical main theorem of complex multiplication see [Sh, Thm. 5.4].

The Chowla–Selberg unit. For every normalized CM lattice for K, in any ideal class, there is $u_{\mathrm{CS}} \in \mathbb{C}$ with $|\eta(u_{\mathrm{CS}})|_p = 1$ for every prime p and every ring map $\eta\colon \mathbb{C} \to \mathbb{C}_p$, such that for every automorphism σ of $\mathbb{C}$ over K the area of the lattice of the conjugate curve times $|\sigma(u_{\mathrm{CS}})|^2$ is $\pi e^{\mathrm{CS}(d)}\,2\pi/\sqrt{d}$. *Status*: Theorem 20.3.1 is the classical Chowla–Selberg product over ideal classes [CS]; the statement above is read from the proof [GL].

Let β be the diagram of Definition 34.2.1. Put $a_\tau = a$ if $\tau \in \Phi_a$ and $a_\tau = 0$ otherwise.

Definition 51.2.6. Fix $j < m$. For $\tau \in \Phi$ and $0 \le i < n_j$ let

$$\mathrm{row}_\tau(i) = \sum_{i<h<n_{j+1}} \beta(\tau, h),$$

the length of row i, counted from 0, of the diagram at τ formed by the columns of height less than n_{j+1}. We call these the *row lengths of lift j*, drop j from the notation, and put $\mathrm{rs}_j = \sum_{\tau\in\Phi} \sum_{0\le i<n_j} s_\infty(\mathrm{row}_\tau(i))$.

Write $G_f(V)$ for the group of finite adelic points of the unitary group of a space V. For $j < m$, a translation $\mathfrak{t}$, $g \in G_f(X_j)$ and $g' \in G_f(X_{j+1})$, consider the kernel of lift j of Section 50.4, at the trivial twist and at the datum $v_j(\mathfrak{t})$ moved by (g, g'): a linear map from the Weyl vectors of the weight of X_j to those of X_{j+1}, in which the values of forms lie. The proof establishes [GL]: *on every conjugate this kernel multiplies Weyl norms by at most* $\exp(x^{50} + \mathrm{rs}_j/2)$; that is, for every value ξ and every $\sigma \in \mathrm{Aut}(\mathbb{C})$, the Weyl norm of σ applied to the image of ξ is at most $\exp(x^{50} + \mathrm{rs}_j/2)$ times the Weyl norm of $\sigma\xi$. Here $L = a + 1$, $t_0 = M/\Omega$ and there are $n_{\mathrm{c}} = f n_j n_{j+1}$ coordinates; besides $\mathrm{rs}_j/2$ the exponent contains the logarithm of the vacuum bound, $n_{\mathrm{c}} \log(2a + 4)$ and $\sum_{\tau,i} \mathrm{row}_\tau(i)/(2L)$, and their sum is at most x^{50}.

51.3. The chain

The kernel bounds multiply along each tuple of classes, so their exponents involve $\sum_{j<m} \mathrm{rs}_j$. We bound this sum, count the classes, and restrict to Y_m.

Problem 51.3.1. For integers $l, l_0, l_1 \ge 0$ with $l \le l_0 + l_1$, $s_\infty(l) \le s_\infty(l_0) + l_1\big(\log(l_0 + l_1 + 1) + \log(M/\Omega)\big)$.

Problem 51.3.2. Let $j < m$, $\tau \in \Phi$ and $0 \le i < n_j$. Then $\mathrm{row}_\tau(0) \le a_\tau + b + r^{16}$ (the first-row slack in the proof is $b + a/x_1 + r^{16}$), $\mathrm{row}_\tau(i) \le \kappa(\tau) + r^{16}$ for $0 < i < k$, and $\mathrm{row}_\tau(i) \le r^{16}$ for $i \ge k$. Each row length is at most $2a$.

Problem 51.3.3. $\sum_{j<m} \mathrm{rs}_j \le C_{\mathrm{ch}} + U/2$.

Class count. Let E be a CM field with a chosen CM type and f infinite places, N' a positive integer in the different of E, and r' a nonnegative integer. The standard definite hermitian space of rank r' has at most $(1 + 2c_{\mathrm{sb}}^3)^{4fr'^2}$ classes $\Gamma\backslash G_f/K^\circ$, with Γ the rational points and K° the stabilizer of the standard lattice, where $c_{\mathrm{sb}} = 6N'(fr')^2$; the proof uses short bases in the standard space and applies the bound with $N' = q_1 d$; for sharper transference bounds see [Ba]. For the data, at a level containing the principal congruence subgroup of $\pi_M \pi_N$, in rank at most n_m, there are at most $e^{x^{30}}$ classes. *Status*: read from the proof [GL].

Branching norm. The restriction from X_m to Y_m of Section 43.4 applies an integral branching matrix; its squared operator norm for the Weyl norms is at most $e^{x^{70}}$. *Status*: read from the proof [GL].

For a form F on X_j or on Y_m and a ring homomorphism $\sigma\colon \mathbb{C} \to \mathbb{C}$, $|\sigma F(g)|^2$ denotes the Weyl squared norm of the conjugate value.

Problem 51.3.4. For a form F on X_m, a ring homomorphism $\sigma\colon \mathbb{C} \to \mathbb{C}$ and $h \in G_f(Y_m)$, the restriction of F to Y_m satisfies

$$|\sigma(\mathrm{res}\, F)(h)|^2 \le \exp\Big(x^{70} - \log N \sum_{\tau\in\Phi} (a_\tau - m r^8)\Big)\, |\sigma F(\mathrm{diag}(h, 1))|^2,$$

and $\sum_{\tau\in\Phi}(a_\tau - mr^8) = \#\Phi_a\, a - fmr^8$. Formally, for one place with $a_\tau - mr^8 = 1$ and $\pi_N = 1 + 2\sqrt{-1}$ (so $N = 5$, which is not the level of any data), the scalar contributes $|1/\bar{\pi}_N|^2 = 1/5$ to the squared norm.

Problem 51.3.5. $x^{70} + fmr^8 \log N + 2(mx^{30} + x^{60} + mx^{50}) + 32fa \log b \le U/2$.

Let Ψ be a chain datum for the trivial twist. By Theorem 48.3.4, choose a weak chain datum Ψ' with $B_{1,\Psi} = R_{1,\Psi'}$ on S; then $\sum_{\mathfrak{t}} |\sigma(\Psi'(\mathfrak{t}))| \le e^{x^{60}}$ for every $\sigma \in \mathrm{Aut}(\mathbb{C})$. Fix $\varphi \in S$ and $y \in G_f(Y_m)$. Write $C_{\mathfrak{t}}\varphi$ for the chain of the m lifts of φ with the data $v_j(\mathfrak{t})$. Before restriction the value at $\mathrm{diag}(y, 1)$ is $\sum_{\mathfrak{t}} \Psi'(\mathfrak{t})(C_{\mathfrak{t}}\varphi)(\mathrm{diag}(y, 1))$, and the proof expands it as a sum over the $\mathfrak{t}$ in the support of Ψ' and over the tuples of classes at the levels of $X_0, \dots, X_{m-1}$, of $\Psi'(\mathfrak{t})$ times products of m kernels applied to values of φ. There are at most $e^{mx^{30}}$ tuples of classes. The resulting estimate for the restricted chain, whose exponent is controlled by Problems 51.1.8, 51.3.3, 51.3.4 and 51.3.5, gives the following theorem, which the proof establishes [GL].

Theorem 51.3.6. *Let Ψ be a chain datum for the trivial twist, $\sigma \in \mathrm{Aut}(\mathbb{C})$, $\varphi \in S$ and $c \in \mathbb{R}$. If $|\sigma\varphi(g)|^2 \le e^c$ for every $g \in G_f(X_0)$, then for every $y \in G_f(Y_m)$*

$$|\sigma(B_{1,\Psi}\varphi)(y)|^2 \le \exp\bigl(c + h_{\mathrm{main}} - m\,\mathrm{rem} + 2\Sigma + U\bigr).$$

The theorem is a statement at the trivial twist only. The problems give the arithmetic estimates in its exponent; taken as given are the kernel bound with the Schur norm, the conjugation of translated theta functions and the Chowla–Selberg unit behind it, the class count, the branching norm, and the expansion of a chain datum. In the exponent Σ has the coefficient 2; Chapter 42 sets the divisibility of Chapter 48 against it in Theorem 42.3.2.

In the Lean formalization. In the Lean proof [GL] (prefix `New.` omitted), Theorem 51.3.6 is `Data.weylNormSq_compositeLift_le`, deduced through `Data.IsChainDatum.exists_isWeakChainDatum_compositeLift_eq` from the bound `Data.weylNormSq_restrictedChain_le` for the restricted chain, whose proof expands the chain by `Data.chainCombination_eq_sum`. The conjugate jet is written as an integral in `Parameters.map_jet_eq_integral` (after `Parameters.jet_jetSeries_mul`) and bounded in `Parameters.norm_jet_translate_le`, with the Taylor scale $\pi_M c_{\mathrm{jet}}$ of `Data.liftKernel`, the comparison scale from `Parameters.exists_isJetConjugation`, whose squared modulus $1/\Omega$ is computed in `Parameters.norm_gal_periodFactor_div_mul_areaScale_sq` inside `Parameters.exists_isJetConjugate_translates`, the reduction to automorphisms over K in `Parameters.exists_algEquiv_norm_eq`, $|\sigma(\pi_M)|^2 = M$ from `Data.norm_map_star_piMBar_sq`, and the growth from `sqrt_prod_pow_le_exp`; the first-row slack is in `Data.diagramWeight_le_rowMainLength_add_rowSlack`; the restriction estimate is `Data.weylNormSq_restrictToY_le`; the kernel bound of Section 51.2 is `Data.sqrt_weylNormSq_jetMap_le`, with rs_j the definition `Data.rowSizeSum`. The results taken as inputs on this sheet are `CMLattice.complex_multiplication_theta`, `CMLattice.chowla_selberg`, `weylNormSq_schur_le`, `Space.card_stdClasses_le`, applied with $N' = q_1 d$ in `Data.card_stdClasses_le_exp_mul_log`, with `Data.card_stdClasses_le_exp`, and `exists_branching_matrix` with `Data.isBranchingMap_branching`.

Hints

§51.1.

51.1.2: Problem 51.1.1; the terms with $p^e \ge x_1$ vanish because $\kappa \ge a/x_1$.
51.1.3: Consider I_p in the split case and the positive part in the large-prime case. Which two choices of y give the sums in gain(p)?
51.1.4: Problem 51.1.3.
51.1.5: Show that $\log n! - (n+\frac{1}{2})\log n + n$ decreases in n; the series of $\frac{1}{2}\log\frac{1+t}{1-t}$ helps.
51.1.6: Problem 51.1.5 with $n = a$.
51.1.7: Compare Problem 51.1.6 with the lower bound for $\log N$. Which terms of size $ma(\frac{1}{f}\sum \log\kappa + \log\frac{M\mathrm{rd}_E}{2\pi})$ cancel?
51.1.8: Problems 51.1.4 and 51.1.7, and $\#\Phi_a \le f$.

§51.2.

51.2.1: One term of the exponential series.
51.2.2: Apply Problem 51.2.1 to $\rho = |z|^2$ with v independent of z; which v makes $(2L+2)t_0 e^{-v} \le 2L$?
51.2.3: Singular value decomposition $Z = PDQ^*$; $\wedge^h$ and Sym^l of a unitary matrix are unitary.
51.2.4: Polar coordinates.
51.2.5: Problem 51.2.2 with $u = |y|^2/(2L+2)$, then Problem 51.2.4.

§51.3.

51.3.1: Compare $l!$ with $(l_0+l_1)!$; what is the sign of $\log(M/\Omega)$?
51.3.2: Definition 34.2.1: which heights below n_{j+1} carry columns, and how many? Use $\kappa_1(\tau) = \kappa(\tau) + \frac{3}{2}\Delta$, $\kappa(\tau) \le b$ and the sizes of m, r, x, b in Definition 33.3.1.
51.3.3: Problem 51.3.1 with $l_0 = a_\tau$ in row 0, $l_0 = \kappa(\tau)$ for $0 < i < k$ and $l_0 = 0$ otherwise; how much can one extra box cost (Problem 33.4.3)? Note $k - 1 \le k$. Then $s_\infty(0) = 0$, $s_\infty(\kappa) \ge 0$, and $m \le 2\sqrt{x}$, $a = xb$.
51.3.4: The scalar of the restriction; $|\psi(\bar{\pi}_N)|^2 = N$ for every embedding $\psi\colon E \to \mathbb{C}$, since $\pi_N\bar{\pi}_N = N$ and every complex embedding of E respects complex conjugation. An integral matrix commutes with σ.
51.3.5: Problem 33.5.4 for $\log N$; compare each term with $fa\log^3 b$, using $b \ge x_1^{10^6}$.

References

[Ba] W. Banaszczyk, *New bounds in some transference theorems in the geometry of numbers*, Math. Ann. **296** (1993), 625–635.
[CS] A. Selberg and S. Chowla, *On Epstein's zeta-function*, J. Reine Angew. Math. **227** (1967), 86–110.
[GL] L. Sernau, *GRH for Dirichlet L-functions, in Lean 4*, a shorter rewriting of the Lean proof, text by Claude, `https://github.com/lsernau/grh-lean`, commit `72fead1`, readable edition `grh/`.
[HJ] R. A. Horn and C. R. Johnson, *Matrix Analysis*, 2nd ed., Cambridge University Press, 2013.
[Sh] G. Shimura, *Introduction to the Arithmetic Theory of Automorphic Functions*, Princeton University Press, 1971.

THE LEVEL PRIME AND THE RAMIFIED FORMS

Prerequisites. Chapter 33: the scales and ranks (Definition 33.3.1) and $m \log b \le \log N \le 30 m \log b$ (Problem 33.5.4). Chapter 34: the CM type Φ, the source forms S, their level, the operators T_w, the ramified forms S_{ram} and $D_X = \dim_{\mathbb{C}} S$ (Section 34.5), and the diagram (Definition 34.2.1). Chapter 48, Section 48.3: the gauge $\|\omega\|_g$ of a Weyl vector, "valuation at least", $\mathcal{O}_\eta$ and S_η, and Problem 48.3.1. Chapter 43: translations $\mathfrak{t} \in \mathcal{T}$, the translated vacua $v_j(\mathfrak{t})$ and the definite lifts (Definition 43.4.2); the pair gluing Gl_i, the glued tensor $\mathrm{gl}(\mathfrak{t})$, the restriction res to Y_m and the composite lift $B_{\vartheta,\Psi}$ (Definition 43.4.3); chain data (Definition 43.4.4). Chapter 50, Section 50.4: standard data of denominator δ (Definition 50.4.1), "multiplies gauges by at most" (Definition 50.4.2), the jet scale c_{jet}, statements (I), (II) and Problem 50.4.1. The colength of Chapter 5 (before Theorem 5.4.1), with the same definition over $\mathcal{O}_\eta$. Standard fillings and the Weyl modules of GL_k [Fu, §8].

At the level prime the gain is 0, but the glued pairs of the composite lift carry poles at N: their data translate the vacuum by $-y/N$. How much N-adic valuation does the composite lift lose there, and on how large a module of forms? This is the case $p = N$ of Theorem 48.7.1; Section 48.6 uses it in the form of Theorem 52.4.1 below. On ramified forms every glued pair becomes two direct lifts after an operator Up, and $\mathrm{Up}^{m/2}$ is integral, after a change of base point, on a submodule of small colength.

52.1. Ramified forms

Recall from Section 34.5 that for each prime $w \mid \pi_N$ of E right translation by the idele z_w is an operator T_w on S with $T_w^{N-1} = 1$, and $S_{\mathrm{ram}} = \bigcap_{w|\pi_N} \ker \sum_{i=0}^{N-2} T_w^i$.

Problem 52.1.1. Let $F_1, \dots, F_l$ be commuting operators on a finite-dimensional complex space with $F_i^n = 1$. Then $\bigcap_i \ker \sum_{s<n} F_i^s = \operatorname{im} \prod_i (1 - F_i)$. Hence $S_{\mathrm{ram}} = \operatorname{im} \prod_{w|\pi_N} (1 - T_w)$. For the cyclic shift F of $\mathbb{C}^4$, $Fe_s = e_{s+1}$, the vector $(1-F)e_0 = (1, -1, 0, 0)$ is killed by $\sum_{s<4} F^s$.

Problem 52.1.2. Let $N = 3$ and let F act on $\mathbb{C}$ through the sign character of $\mathbb{F}_3^\times$ at its generator. Then $1 + F = 0$, $1 - F = 2$, so the line is ramified and $|1 - F|^2 = 4$.

52.2. The places above N and the direct lifts

Fix a ring map $\eta\colon \mathbb{C} \to \mathbb{C}_N$. For $\tau \in \Phi$ let w_τ be the place of E above N at which $\eta \circ \Phi_\tau$ is continuous (the prime v_τ of Section 48.4, for $p = N$; we write w for places above N, as in Section 34.5). Let Σ_N (a notation of this chapter) be the set of the conjugates $\bar{w}_\tau$. As $N \equiv 1 \pmod{q_2^2}$, N splits completely in E; so $\tau \mapsto \bar{w}_\tau$ is a bijection from Φ onto Σ_N, which holds exactly one place of each conjugate pair above N; each residue field is $\mathbb{F}_N$. A *residue vector* on X_j is a family $y = (y_w)_{w \in \Sigma_N}$ of vectors $y_w \in \mathbb{F}_N^{n_j}$ in the basis of X_j; it is *primitive* if every $y_w \neq 0$; e_{last} is the last basis vector at every place.

Date: November 26, 2026.

Definition 52.2.1. Let diag_N be the matrix $\mathrm{diag}(1,\dots,1,N)$ at every place of Σ_N. The *base point* δ_j is the finite adelic point of the unitary group of X_j, supported above N, whose component at $w \in \Sigma_N$ is $\mathrm{diag}(1,\dots,1,N)$ if $w \mid \pi_N$ and 1 otherwise. Put $\delta_j^\vee := \delta_j\,\delta_{j,\Sigma}^{-1}$, where $\delta_{j,\Sigma}$ is the point with component diag_N at Σ_N.

For a matrix g_1 over $\prod_{w\in\Sigma_N} E_w$ let $\mathrm{Rt}_j(g_1)$ be right translation of forms on X_j by $\delta_j g_1\,\delta_j^{-1}$: matrices at Σ_N are read through δ_j. For a function f of $n_{j+1}\times n_j$ matrices at Σ_N and a finite datum v of $\mathrm{Hom}(X_j,X_{j+1})$, let $\mathrm{Sch}(f)v$ put f on v at Σ_N in the Schrödinger model, and let $\Theta_j^X[f,v]$ (in this chapter) be the definite lift $X_j \to X_{j+1}$ for the twist ϑ (lift $j{+}1$ of Definition 43.4.2; here, as in Definition 48.3.3, a lift carries the index of its source space) whose datum is $\mathrm{Sch}(f)v$ translated by (δ_j,δ_{j+1}) under the Weil representation. A function of residue matrices is read on the integral matrices through reduction modulo N and extended by 0.

Definition 52.2.2. The *direct datum* dir is the function $\mathrm{col}_{e_{\mathrm{last}}}$, where $\mathrm{col}_y(T)=1$ if T is integral and its last column reduces to y, and $\mathrm{col}_y(T)=0$ otherwise. The *direct lift* j with datum v is $\Theta_j^X[\mathrm{dir},v]$.

Definition 52.2.3. Let $\psi_N(c) := \psi_0(-c/N)$ on $\prod_{w\in\Sigma_N}\mathbb{F}_N$, with ψ_0 the standard character of the finite adeles. For a residue vector y on X_0 whose last entry is a unit at every place, let $\mathfrak{g}_y$ be an integral invertible matrix whose last column and last row reduce to y. On forms on X_0,

$$\mathrm{Up} := \mathrm{Rt}_0(\mathrm{diag}_N^{-1})\sum_y \psi_N(y_{\mathrm{last}})\,\mathrm{Rt}_0(\mathfrak{g}_y),$$

the sum over these y.

A form φ on X_j is *ramified at* Σ_N (in this chapter) if for each $w\in\Sigma_N$ there are a form ψ and a unit scalar c at Σ_N, integral, with $c\equiv 1 \bmod N$ at the places other than w, such that $\varphi = \psi - \mathrm{Rt}_j(c)\psi$.

Problem 52.2.1. Every $\varphi \in S_{\mathrm{ram}}$ is ramified at Σ_N, with $\psi \in S$.

The proof reads the following *lift law* for $\Theta_j^X[\,\cdot\,,v]$, for every datum v. (i) For integral invertible matrices g_1 of size n_j and g_2 of size n_{j+1} at Σ_N, with reductions $\bar g_1$, $\bar g_2$, and every function f of residue matrices, $\mathrm{Rt}_{j+1}(g_2)\circ\Theta_j^X[T\mapsto f(\bar g_2 T\bar g_1),v]\circ\mathrm{Rt}_j(g_1) = \Theta_j^X[f,v]$. (ii) $\mathrm{Rt}_{j+1}(\mathrm{diag}_N^{-1})\circ\Theta_j^X[\mathrm{row},v] = \varepsilon'_j\,\Theta_j^X[\mathrm{dir},v]\circ \mathrm{Rt}_j(\mathrm{diag}_N^{-1})$, where row is the indicator of the integral matrices whose last row reduces to e_{last}, and ε'_j (in this chapter) is the value at diag_N on X_j of the character $g\mapsto\chi(\det g)|\det g|^{-n_{j+1}/2}$, divided by the value at diag_N on X_{j+1} of $g\mapsto\chi(\det g)|\det g|^{-n_j/2}$, with χ the base change to E of the character of the lift $X_j\to X_{j+1}$. Here and below $|\det g| := \prod_{w\in\Sigma_N}|\det g_w|_w$, with $|N|_w = N^{-1}$, and $\chi(\det g)$ reads $\det g$ as an idele.

Problem 52.2.2. Let $w\in\Sigma_N$ and let f be a function of residue matrices with $f(cT)=f(T)$ for every unit $c\in\prod_{\Sigma_N}\mathbb{F}_N^\times$ equal to 1 off w. Then $\Theta_j^X[f,v]\varphi = 0$ for every φ ramified at Σ_N. In particular $\Theta_j^X[\mathrm{col}_y,v]\varphi=0$ if y vanishes at some place.

Let $\mathrm{ch}_y(T) := \psi_N\big((\text{last row of } T)\cdot y\big)$ on integral matrices, 0 elsewhere.

Problem 52.2.3. $\mathrm{GL}_n(\mathbb{F}_N)$ is transitive on $\mathbb{F}_N^n\smallsetminus 0$, a set of N^n-1 elements; so there are $\#\mathrm{Prim}_n = (N^n-1)^f$ primitive residue vectors in rank n, a number prime

to N. For φ ramified at Σ_N and data v, v',

$$\sum_y \Theta^X_{j+1}[\mathrm{ch}_y, v']\,\Theta^X_j[\mathrm{col}_y, v]\,\varphi = \#\mathrm{Prim}_{n_{j+1}} \cdot \Theta^X_{j+1}[\mathrm{ch}_{e_{\mathrm{last}}}, v']\,\Theta^X_j[\mathrm{dir}, v]\,\varphi,$$

the sum over all residue vectors on X_{j+1}. For $N = 3$, $n = 2$, $f = 1$: eight vectors, one orbit.

All lifts become direct. The proof reads two further statements. First, on data fixed by the projection on the vacuum above N, the double lift $X_{2i} \to X_{2i+2}$ with the glued datum $\mathrm{Gl}_i(v \otimes v')$ is $\varepsilon_i\,\mathrm{Rt}_{2i+2}(\mathrm{diag}_N^{-1}) \sum_y \Theta^X_{2i+1}[\mathrm{ch}_y, v']\,\Theta^X_{2i}[\mathrm{col}_y, v]$, where ε_i (in this chapter) is the value of the character of the lift $X_{2i+1} \to X_{2i+2}$, formed with $|\det|^{-n_{2i+1}/2}$, at $\mathrm{diag}(1, \dots, 1, N)$ on X_{2i+2} at the places of Σ_N prime to π_N, times the value of the character of $X_{2i} \to X_{2i+1}$, also formed with $|\det|^{-n_{2i+1}/2}$, at the same matrix on X_{2i} at the places dividing π_N. Second, the following, whose proof sorts the terms of $\Theta^X_{2i+1}[\mathrm{ch}_{e_{\mathrm{last}}}, v']$ by the last row and uses the lift law: *there is $c_{\mathrm{dir}} \in \mathbb{C}$ (in this chapter) such that for all data v_j and all $\varphi \in S_{\mathrm{ram}}$, the chain of the $m/2$ double lifts with the glued data of the projections of the v_j on the vacuum above N sends φ to c_{dir} times the chain of the m direct lifts with data v_j applied to* $\mathrm{Up}^{m/2}\varphi$. *Here*

$$c_{\mathrm{dir}} = \prod_{i<m/2} \Big(\varepsilon_i\, \#\mathrm{Prim}_{n_{2i+1}} \prod_{l<2i+2} \varepsilon'_l \Big).$$

Status: read from the proof. Problems 52.2.2 and 52.2.3 are its first steps. We also read: for g equal to $\mathrm{diag}(1, \dots, 1, N)$ at a set $\Sigma' \subseteq \Sigma_N$ and 1 at the other places of Σ_N, the value at g of the character of any of the lifts, formed with $|\det|^{-r/2}$ for any $r \geq 0$, has N-adic absolute value at most $N^{2b\,\#\Sigma'}$ after η.

Problem 52.2.4. $|\eta(\varepsilon_i)| \leq N^{2fb}$, $|\eta(\varepsilon'_l)| \leq 1$ and $|\eta(\#\mathrm{Prim}_n)| \leq 1$; hence $|\eta(c_{\mathrm{dir}})| \leq N^{mfb}$.

52.3. The colength of the forms integral after $\mathrm{Up}^{m/2}$

A form φ is *integral at* a point h if $\|\varphi(g)\|_{gh} \leq 1$ for every g; so S_η is the module of source forms integral at 1. Write $S_\eta(h)$ (in this chapter) for the $\mathcal{O}_\eta$-module of source forms integral at h; so $S_\eta = S_\eta(1)$. By Section 34.5 the values of source forms lie in $\bigotimes_{\tau \in \Phi_a} \mathrm{Sym}^a \mathbb{C}^k$, whose basis is the families $I = (z^{\alpha_\tau})_{\tau \in \Phi_a}$ of monomials of degree a in k variables; let $e_I := \sum_\tau \alpha_{\tau,k}$ be the degree of I in the last variable.

Problem 52.3.1. Let $k = a = 2$, one place, $N = 3$. The monomials $z_1^2, z_1 z_2, z_2^2$ have degrees $0, 1, 2$ in z_2; the change of lattice multiplies them by $\mathrm{diag}(1, 3, 9)$, of determinant 3^3, and the colength of the span of $3^{\alpha_2} z^\alpha$ in the span of the z^α over $\mathbb{Z}_3$ divides 3^3. The mean degree in z_2 is $1 = a/k$.

A source form is determined by its values at representatives of the double cosets of its level, and these values are arbitrary: the proof reads that the stabilizers of the double cosets are trivial. So the pairs (c, I) of a double coset and a basis vector are D_X in number. Let $D_{\mathrm{last}} := \sum_{(c,I)} e_I$.

Problem 52.3.2. The degree in the u-th variable, summed over the monomials of degree a in k variables, does not depend on u, and k times it is a times the number of these monomials.

Problem 52.3.3. $k\,D_{\mathrm{last}} = \#\Phi_a\, a\, D_X \leq f a\, D_X$.

Definition 52.3.1. S_N is the $\mathcal{O}_\eta$-module of the forms φ on X_0 such that $\mathrm{Up}^{m/2}\varphi$ is a source form integral at δ_0.

The proof reads that every double coset has a representative r_c such that $r_c\delta_0^\vee$ and $\delta_{0,\Sigma}^{-1} r_c \delta_0$ are integral above N, that is, lie in $\mathrm{GL}_k(\mathcal{O}_{E_w})$ at every place w above N.

Problem 52.3.4. $S_\eta \subseteq S_\eta(\delta_0^\vee)$. The coordinates of $\varphi(r_c)$ are integral for $\varphi \in S_\eta(\delta_0^\vee)$, and a source form whose coordinate (c, I) at r_c is divisible by N^{e_I} for all (c, I) lies in $S_\eta(\delta_0)$. Hence the colength of $S_\eta(\delta_0)$ in $S_\eta(\delta_0^\vee)$ divides $N^{D_{\mathrm{last}}}$.

Problem 52.3.5. $(\mathrm{Up}\varphi)(g) = \sum_y \psi_N(y_{\mathrm{last}})\, \varphi(g\, \delta_0^\vee \mathfrak{g}_y \delta_0^{-1})$; hence Up maps $S_\eta(\delta_0)$ into forms integral at $\delta_0^\vee$. As Up preserves S (read from the proof), the colength in S_η of the forms φ with $\mathrm{Up}^i\varphi \in S_\eta(\delta_0)$ divides $N^{(i+1)D_{\mathrm{last}}}$, for every $i \geq 0$.

Problem 52.3.6. $(m/2+1)\, a \leq mbk$, and so $(m/2+1)D_{\mathrm{last}} \leq mfb\, D_X$.

Problems 52.3.3, 52.3.5 with $i = m/2$, and 52.3.6 prove part (a) of Theorem 52.4.1 below, with $e = (m/2+1)D_{\mathrm{last}}$.

52.4. Direct lifts lose little

The Fourier expansion of the direct datum has poles at N, which an element of K must clear.

Problem 52.4.1. Let $K = \mathbb{Q}(\sqrt{-7})$, $\theta_K = (1+\sqrt{-7})/2$, $N = 11$. Then $z^2 - z + 2$ has the roots $5, 7$ modulo 11; with $c_0 = 7$, $(1-2c_0)^2 \equiv -7$ and $(1-2c_0)\cdot 7 \equiv 8 \pmod{11}$. So $\delta := \theta_K - c_0$ lies in the prime $\mathfrak{p} = (11, \delta)$, and $\bar{\delta}\cdot 7$ is a unit at $\mathfrak{p}$.

Problem 52.4.2. Let $\theta_K = (1+\sqrt{-d})/2$, let $c_0 \in \mathbb{Z}$ represent θ_K modulo the prime $\mathfrak{p}$ of K below w_τ (the same for all τ), and $\delta := \theta_K - c_0$. Then $\delta \in w_\tau$ for every τ, and $|\eta(\bar{\delta}d)| = 1$.

The proof reads: *for $j < m$, every translation $\mathfrak{t}$ and every $\delta \in \mathcal{O}_K$ lying in all the w_τ, the datum $N^{2fn_jn_{j+1}}\,\mathrm{Sch}(\mathrm{dir})v_j(\mathfrak{t})$ is standard of denominator δ*; the translates of the vacuum in the expansion of dir have simple poles at the w_τ. Recall from Section 50.4 that the kernel of the lift $X_j \to X_{j+1}$ is the theta kernel at scale $\pi_M c_{\mathrm{jet}}$ and $|\eta\pi_M| \leq 1$. A datum *multiplies gauges from δ_j to δ_{j+1} by at most c* if the inequality of Definition 50.4.2 holds with $\|\cdot\|_{g'\delta_{j+1}}$ and $\|\cdot\|_{g\delta_j}$ in place of $\|\cdot\|_{g'}$ and $\|\cdot\|_g$.

Problem 52.4.3. Let $0 \neq \delta \in \mathcal{O}_K$ with $|\eta\pi_M| \leq |\eta(\bar{\delta}d)|$. Every standard datum of denominator δ multiplies the gauges of the kernel of the lift $X_j \to X_{j+1}$ by at most 1. Hence, for $j < m$, the datum of the direct lift j with $v_j(\mathfrak{t})$ multiplies gauges from δ_j to δ_{j+1} by at most $N^{2fn_jn_{j+1}} \leq N^{fb}$.

Three more statements are read from the proof. For $\mathfrak{t}$ in the support of a chain datum, $v_j(\mathfrak{t})$ is fixed by the projection on the vacuum above N. The direct datum commutes with the action of the levels of X_j and X_{j+1}; so for a chain datum Ψ for ϑ, if every $\mathrm{Sch}(\mathrm{dir})v_j(\mathfrak{t})$, translated by (δ_j, δ_{j+1}), multiplies gauges from δ_j to δ_{j+1} by at most N^{r_j}, then $\sum_{\mathfrak{t}} \Psi(\mathfrak{t})$ times the chain of the m direct lifts with data $v_j(\mathfrak{t})$ maps source forms integral at δ_0 to forms with $\|\cdot(g)\|_{g\delta_m} \leq N^{r_0+\cdots+r_{m-1}}$ for every g, as in Problem 48.3.1. And if a form on X_m satisfies $\|\varphi(g)\|_{g\delta_m} \leq C$ for every g, then its restriction $\mathrm{res}\,\varphi$ to Y_m has valuation at least $-\log_N C$: the branching map

is integral, and its scalar has the absolute value of the determinant factor of δ_m. The branching rule is classical [GW, Thm. 8.1.1]; the integrality of the branching map and the rest are read from the proof.

Problem 52.4.4. Let Ψ be a chain datum for a twist ϑ and $\varphi \in S_{\mathrm{ram}} \cap S_N$. Then $B_{\vartheta,\Psi}\varphi = c_{\mathrm{dir}}\,\mathrm{res}\big(\sum_{\mathfrak{t}} \Psi(\mathfrak{t})\,(\text{chain of direct lifts with } v_j(\mathfrak{t}))(\mathrm{Up}^{m/2}\varphi)\big)$, and it has valuation at least $-2mfb$. Moreover $2mfb\log N \le 4fa(\log b)^2\log x_1$.

Problems 52.2.4, 52.4.3 and 52.4.4 prove part (b).

Theorem 52.4.1. *Let $\eta\colon \mathbb{C} \to \mathbb{C}_N$ be a ring map.*

(a) *There is an integer $0 \le e \le mfb\,D_X$ such that the colength of S_N in S_η divides N^e.*
(b) *For every twist ϑ, every chain datum Ψ for ϑ and every $\varphi \in S_{\mathrm{ram}} \cap S_N$, the form $B_{\vartheta,\Psi}\varphi$ has valuation at least $-2mfb$.*

What has been established. Theorem 52.4.1, the case $p = N$ of Theorem 48.7.1, with $S' = S_N \cap S_\eta$ (the combinations in (a) of elements of S_η stay in S_η), $l = e$ and $\mathrm{loss}(N) = 2mfb$; Problem 52.4.4 bounds its term in the sum of the errors. Taken as given: the statements read from the proof, listed in the remark, and the branching rule.

In the Lean formalization. In the Lean proof [GL] (namespace `New.` omitted), Theorem 52.4.1(a) is `Data.exists_colengthDvd_upIntegralForms_pow` and (b) is `Data.gaugeLe_compositeLift_at_N`. Definitions 52.2.1, 52.2.2, 52.2.3, 52.3.1 are `Data.diagPointN` (with `Data.dualPointN`), `IsSplitLevel.directDatum`, `IsSplitLevel.upOperator` and `Data.upIntegralForms`; Problem 52.1.1 is `Data.ramifiedSourceForms_eq_range`, Problem 52.3.4 is `Data.colengthDvd_integralFormsAt_diagPointN`, and the statement that all lifts become direct is `Data.doubleLiftChain_gluedDoubleLiftDatum_eq_smul_chain` (one pair: `IsSplitLevel.LiftLaw.glued_eq_direct_direct_upOperator`); the integral branching map is `exists_branching_matrix`. The other statements read in the text are: the lift law, `Data.liftLaw_liftAtN` (ε'_j is `Data.upCommutationFactor`); the gluing at N, `Data.liftInPairs_gluedDoubleLiftDatum` (ε_i is `Data.gluedFactor`); the bound on the character values, `Data.norm_detCharAt_diagN_le`; the trivial stabilizers, `Data.classAut_levelX_zero_eq_bot`; the representatives r_c, `Data.exists_mul_dualPointN_mem_integralAbove`; that Up preserves S, `Data.upOperator_mem_sourceForm`; the Fourier step, a step of the proof of `Data.schrodingerOpAt_directDatum_mem_raises`; the translated vacua at N, `Data.vacuumProjFinPart_translateDatum`; the invariance and the bound along the chain, `Data.omega_schrodingerOpAtN_directDatum` and `Data.IsWeakChainDatum.gaugeLe_chain`; the restriction at δ_m, `Data.GaugeLe.restrictToY_of_diag`.

Hints

§52.1.

52.1.1: As in Problems 43.5.1 and 43.5.2: $1 - F^n = (1-F)\sum_{s<n} F^s$; decompose into joint eigenspaces.

§52.2.

52.2.1: Problem 52.1.1 with one factor. For $w \in \Sigma_N$ let u be the one of $w, \bar{w}$ that divides π_N; z_u is 1 off $u, \bar{u}$, and a scalar commutes with δ_0.

52.2.2: Lift law (i) with g_1 the scalar c and $g_2 = 1$.

52.2.3: Write $y = \bar{g}\, e_{\text{last}}$ with g integral invertible, and apply the lift law (i) to both lifts; Problem 52.2.2 for the other y.

52.2.4: Each τ has $\bar{w}_\tau$ in exactly one of the two sets in ε_i. For ε_l': $\chi(\det \mathrm{diag}_N)$ is the same on both spaces, and $|\eta(\sqrt{N})| = N^{-1/2}$; $n_l \le n_{l+1}$.

§52.3.

52.3.1: Sym^2 of $\mathrm{diag}(1,3)$. Over a valuation ring one condition "this coordinate is divisible by z" costs a colength dividing z: use a member of the family whose coordinate divides the others'.

52.3.2: Exchanging two variables permutes the monomials; sum over u.

52.3.3: Sum Problem 52.3.2 over the places of Φ_a, one at a time.

52.3.4: At τ, $\delta_0^\vee$ acts through $\mathrm{diag}(1,\dots,1,N^{-1})$ or 1, and $\delta_{0,\Sigma}$ through $\mathrm{diag}(1,\dots,1,N)$; the last row of an element of the level is $\equiv (0,\dots,0,1) \bmod \pi_N$, so $\delta_0^{-1} k \delta_0$ is integral above N. Every g is $\gamma r_c k$ with γ rational and k in the level, and $\|\gamma\omega\|_{\gamma h} = \|\omega\|_h$. For the colength, impose the divisibility of the (c, I) coordinates one at a time, as in the hint to Problem 52.3.1.

52.3.5: $\mathfrak{g}_y$ is integral above N, so $\|\omega\|_{h\mathfrak{g}_y} = \|\omega\|_h$; and $|\psi_N| = 1$. Induction on i; colengths multiply along a chain of modules.

52.3.6: $a = xb$, $\sqrt{x} \le m$, $k = r + 1 - m \ge x^5 - 2\sqrt{x}$; Problem 52.3.3.

§52.4.

52.4.1: $\theta_K^2 - \theta_K + 2 = 0$; $\bar{\delta} = 1 - \theta_K - c_0$.

52.4.2: Φ_τ restricts to one embedding of K; $(1 - 2\theta_K)^2 = -d$, and $N \nmid d$.

52.4.3: Statements (I), (II) of Section 50.4 and Problem 50.4.1, with Problem 52.4.2; the entries of $\mathrm{schur}_\beta(z)$ are homogeneous. Then $|\eta(N)| = N^{-1}$, $n_j \le n_m$, and the scale inequalities give $2n_m^2 \le b$.

52.4.4: The chain of double lifts is linear in the glued tensor; Problems 52.2.4 and 52.4.3; the values $\Psi(\mathfrak{t})$ are integral at N. For the last claim use Problem 33.5.4, $m \le 2\sqrt{x}$ and $(\log b)\log x_1 \ge 60$.

References

[Fu] W. Fulton, *Young Tableaux*, London Math. Soc. Student Texts 35, Cambridge University Press, 1997.

[GL] L. Sernau, *GRH for Dirichlet L-functions, in Lean 4*, a shorter rewriting of the Lean proof, text by Claude, `https://github.com/lsernau/grh-lean`, commit `72fead1`, readable edition `grh/`.

[GW] R. Goodman and N. R. Wallach, *Symmetry, Representations, and Invariants*, Graduate Texts in Mathematics 255, Springer, 2009.

EXCEPTIONAL PRIMES: A FULL MARK

Prerequisites. Chapter 33: the data and the scale inequalities (Definition 33.3.1, Problem 33.3.3). Chapter 34: the spaces X_j of rank n_j and the diagram β of the data (Definition 34.2.1). Chapter 48: c_p, I_p, gain(p) (Section 48.1); $C_p(\Phi')$, o_p, r_p, exceptional primes, L_p (Section 48.2); gauges, valuations, S_η, weak chain data, translations $\mathfrak{t}$ with translated vacua $v_j(\mathfrak{t})$, and the restricted chain $R_{\vartheta,\Psi}$ (Section 48.3); the primes v_σ, marks, full marks, $\Phi_{\mathfrak{M}}$, a_v, T_v, $Y_v = p^{a_v}T_v$ and $Y_{\mathfrak{M}}$, the product of the Y_v in a fixed order (Section 48.4). Chapter 49: $\beta_{>1}$ (Definition 49.2.1), charges (Definition 49.3.1) and Theorem 49.3.2. Chapter 50: standard data (Definition 50.4.1), "multiplies gauges by at most" (Definition 50.4.2), the stage bound $\mathcal{D}_j(\Phi')$ (Definition 50.1.1), Theorem 50.4.4, statements (III) and (IV) of Section 50.4, Problems 50.1.1, 50.4.3, 50.4.4 and 50.5.1. Hecke operators at a split place (Chapter 24, Section 24.5). Decomposition groups in abelian extensions [Ne, Ch. I, §9]; elementary divisors over a discrete valuation ring.

At an exceptional prime $p < x_1$ the collision sum can exceed the unit of loss L_p (Problem 48.2.5). Chapter 48 therefore applies the scaled Hecke operator $Y_{\mathfrak{M}}$ of a full mark before the chain, and uses the bound of Theorem 53.4.1 below. How does a Hecke operator at primes above p remove the collisions, and what does it cost?

53.1. The primes above an exceptional prime

Let p be a prime with $\chi_K(p) = -1$ and $\eta\colon \mathbb{C} \to \mathbb{C}_p$ a ring map. Then $p \neq d$, and $p \nmid q_1$ by Problem 48.1.1; so p is unramified in E. For $\sigma \in \Phi$, v_σ is the prime of E induced by $\eta \circ \Phi_\sigma$, and $\bar{v}$ is the complex conjugate of v.

Definition 53.1.1. The *residue degree above* p is $f_p := \mathrm{lcm}(2, o)$, where o is the order of $[-p]$ in $\Phi \cong (\mathbb{Z}/q_1)^\times$.

Problem 53.1.1. For $\sigma, \tau \in \Phi$: $v_\sigma = v_\tau$ if and only if $\sigma = [-p]^i\tau$ with i even, and $v_\sigma = \bar{v}_\tau$ if and only if $\sigma = [-p]^i\tau$ with i odd. The residue field of every $v \mid p$ has p^{f_p} elements.

Problem 53.1.2. Let $q_0 = 18480$, $d = 138599$ and $m = 16384$. The prime 479 is inert in K, with $o_{479} = 15$ and $r_{479} = 2$; it is not exceptional. The prime $55439 \equiv 6287 \pmod m$ is inert, with $o_{55439} = r_{55439} = 1$; it is exceptional.

Problem 53.1.3. If $p \not\equiv \pm 1 \pmod m$, then m divides the order of $[-p]$; so f_p is this order, it is even, and $f_p \geq m$. [Check, with $m = 2^{14}$ and $s = 308$: the order of -55439 modulo q_1 has 2-adic valuation 308.]

Problem 53.1.4. Let p be exceptional. For $\tau \in \Phi_a$, $[-p^{o_p}]\tau \in \Phi_a$ and $v_{[-p^{o_p}]\tau} = \bar{v}_\tau$. No prime $v \mid p$ equals $\bar{v}$.

Problem 53.1.5. If $p < x_1$ is exceptional, a full mark at (p, η) exists.

For a full mark, $C_p(\Phi_{\mathfrak{M}}) = 0$ (Problem 48.4.1). Let $\bar{\mathfrak{M}} := \{\bar{v} : v \in \mathfrak{M}\}$ and $\Phi_{\bar{\mathfrak{M}}} := \{\sigma : v_\sigma \in \bar{\mathfrak{M}}\}$.

Date: November 26, 2026.

Problem 53.1.6. Let $\mathfrak{M}$ be a mark. No $\sigma \in \Phi_{\mathfrak{M}} \cup \Phi_{\bar{\mathfrak{M}}}$ is a b-place, so $\kappa(\sigma) = a/x_1$ there. For $v \in \mathfrak{M}$, $\sigma \mapsto [-p]\sigma$ maps $\{\sigma : v_\sigma = v\}$ bijectively onto $\{\sigma : v_\sigma = \bar{v}\}$ and preserves κ.

The *model* is that of Problem 50.5.1: $\Phi = (\mathbb{Z}/4)^\times = \{1, 3\}$, both places are a-places, $a = 24$, and $p = 5$ is treated as inert, so that $[-5^e]$ exchanges 1 and 3 for every $e \in I_5$, the odd $e \geq 1$. Think of 1 as inducing v and 3 as inducing $\bar{v}$, and put $\Phi_{\mathfrak{M}} := \{1\}$. There are two rows, 0 and 1, and β has 24 columns of height one at each place and no others. The model is bookkeeping, not data.

Problem 53.1.7. In the model, $C_5(\varnothing) = 10$ and $C_5(\{1\}) = 0$; $\mathcal{D}(\beta) = 0$, while $\mathcal{D}(\beta \smallsetminus \{1\}) + \gamma_5 \cdot 24 = 10 = 48\gamma_5$, with $\gamma_5 = 5/24$.

Without the mark the collision takes the whole credit $48\gamma_5$; with it, nothing is lost. The erasure is not free: at a neighbour the charges and the diagonal cost a_v (Section 53.2), and Y_v carries the factor p^{a_v} that pays for them.

53.2. One lift at a neighbour

Let $\mathfrak{M}$ be a mark and $j \geq 0$. For $v \in \mathfrak{M}$ the pair $\{v, \bar{v}\}$ is split (Problem 53.1.4), and the unitary group of X_{j+1} at it is $\mathrm{GL}_{n_{j+1}}(E_v)$: g at v and $(\bar{g}^{\,t})^{-1}$ at $\bar{v}$. As p is unramified, it is a uniformizer of E_v.

Definition 53.2.1. A *neighbour of index at most* r_p at $\mathfrak{M}$ is an element of the finite adelic unitary group of X_{j+1} which is 1 away from $\mathfrak{M} \cup \bar{\mathfrak{M}}$ and whose component g_v at each $v \in \mathfrak{M}$ lies in the $\mathrm{GL}_{n_{j+1}}(\mathcal{O}_v)$-double coset of $\mathrm{diag}(p1_i, 1)$ for some $i \leq r_p$.

Problem 53.2.1. An element of the double coset of $\mathrm{diag}(p1_i, 1)$ in $\mathrm{GL}_n(E_v)$ is $g_1 \,\mathrm{diag}(p1_{\mathcal{I}}, 1)\, g_2$ with $g_1, g_2 \in \mathrm{GL}_n(\mathcal{O}_v)$, for every set $\mathcal{I}$ of i rows, $\mathrm{diag}(p1_{\mathcal{I}}, 1)$ having p at the rows of $\mathcal{I}$ and 1 elsewhere.

Fix sets $\mathcal{I}_v$ of rows, $\#\mathcal{I}_v \leq r_p$, for $v \in \mathfrak{M}$. For τ with $v_\tau \in \mathfrak{M}$ or $\bar{v}_\tau \in \mathfrak{M}$ let $\mathcal{I}(\tau) := \mathcal{I}_v$ for that $v \in \mathfrak{M}$; otherwise $\mathcal{I}(\tau) := \varnothing$. The *neighbour diagonal* $g_{\mathcal{I}}$ is the neighbour (Definition 53.2.1) with component $\mathrm{diag}(p1_{\mathcal{I}_v}, 1)$ at each $v \in \mathfrak{M}$.

Problem 53.2.2. (i) At τ, the extension to finite adeles of $u \mapsto \eta(\Phi_\tau(\bar{u}))$ sends $g_{\mathcal{I}}$ to the diagonal matrix with entries $p^{-\epsilon_\tau(i)}$, where $\epsilon_\tau(i) = 1$ if $v_\tau \in \mathfrak{M}$ and $i \in \mathcal{I}(\tau)$, $\epsilon_\tau(i) = -1$ if $\bar{v}_\tau \in \mathfrak{M}$ and $i \in \mathcal{I}(\tau)$, and $\epsilon_\tau(i) = 0$ otherwise; so a box in row i at τ has its gauge multiplied by $|p^{-\epsilon_\tau(i)}| = p^{\epsilon_\tau(i)}$. (ii) For every integer c, $\sum_{\tau:\,\kappa(\tau)=c} \sum_i \epsilon_\tau(i) = 0$.

The following extends statement (II) of Section 50.4 from 1 to a diagonal; it is read from the proof. *(C)* Let ϕ be a standard datum of denominator δ on $\mathrm{Hom}(X_j, X_{j+1})$, let g_1, g_2 be elements of the finite adelic unitary group of X_{j+1} whose components at the places above p are integral with integral inverses, and let g_0 be an element of the same group sent at each τ, as in Problem 53.2.2, to a diagonal matrix with entries $y_\tau(i)$. For a filling $\mathbf{i}$ put $\mathrm{dw}(\mathbf{i}) := \prod_\tau |\det y_\tau|^{e_\tau} \prod_{\text{boxes}} |y_\tau(\text{row})|$, where e_τ, a function of $\kappa(\tau)$ and j, is the exponent of the determinant in the weight at τ. If $\mathrm{dw}(\mathbf{i}')$ times the absolute value of the entry $(\mathbf{i}', \mathbf{i})$ of the Schur jet matrix of the jet series, at the scale of the kernel, of every standard datum of denominator δ is at most $\mathfrak{b}$, then $\omega(1, g_1 g_0 g_2)\phi$ multiplies gauges by at most $\mathfrak{b}$.

For $\tau \in \Phi$, $h \geq 1$ and rows i let $\mathfrak{c}(\tau, h, i) := 1$ if either $v_\tau \in \mathfrak{M}$, $h = 1$ and $i \notin \mathcal{I}(\tau)$, or $\bar{v}_\tau \in \mathfrak{M}$ and $i \in \mathcal{I}(\tau)$; and $\mathfrak{c}(\tau, h, i) := 0$ otherwise.

Problem 53.2.3. The numbers $\mathfrak{c}$ are charges for $(\beta, \Phi_{\mathfrak{M}})$, with β read at heights below n_{j+1}. [With two rows and $\mathcal{I}_v = \{0\}$: $\mathfrak{c}(\tau, 1, \cdot) = (0, 1)$ if $v_\tau \in \mathfrak{M}$, $\mathfrak{c}(\tau, h, \cdot) = (1, 0)$ for every h if $\bar{v}_\tau \in \mathfrak{M}$, and in each pairing exempt by Definition 49.3.1 the two charges add up to 1 in each row.]

Problem 53.2.4. Let ϕ be a standard datum of denominator 1 on $\mathrm{Hom}(X_j, X_{j+1})$ and g a neighbour of index at most r_p at $\mathfrak{M}$. Then $\omega(1, g)\phi$ multiplies gauges by at most

$$p^{\sum_{v\in\mathfrak{M}} a_v + r_p \sum_{\sigma\in\Phi_{\mathfrak{M}}} \beta_{>1}(\sigma) - \mathcal{D}_j(\Phi_{\mathfrak{M}})},$$

with β read at heights below n_{j+1}.

In the model, with $\mathcal{I} = \{0\}$ and one input coordinate, let $F := \exp\bigl(\sum_{i=0,1}(z_{1i}^5 z_{3i} + z_{3i}^5 z_{1i})/5\bigr)$, which has the normal form with $W = 1$. A filling puts a_i boxes in row i at place 1 and a_i' at place 3 (in this sheet), $a_0 + a_1 = a_0' + a_1' = 24$; its jet is $\partial_{z_{10}}^{a_0}\partial_{z_{11}}^{a_1}\partial_{z_{30}}^{a_0'}\partial_{z_{31}}^{a_1'}F(0)$, its charges total $a_1 + a_0'$, and the diagonal weights it by $5^{a_0 - a_0'}$ in absolute value.

Problem 53.2.5. (m) By machine: of the 625 fillings, 25 have a nonzero jet; every nonzero jet has valuation 0; and $\mathrm{val}(\mathrm{jet}) + a_1 + a_0' \geq 8$, with equality only at $(a_0, a_0') = (20, 4)$.

So p^{24} times the weighted jets of the neighbour have valuation at least 8, against 0 for the plain kernel: the mark recovers 8 of the 10, and the missing 2 is the digit loss in the factorials, which the logarithmic term of Theorem 49.3.2 pays for. The model is a direct computation; the error term of that theorem is about 54 here.

53.3. Moving the Hecke operators into the data

For $v \in \mathfrak{M}$, $q_v := p^{f_p}$, and $0 \leq i \leq n_j$, let $T_{v,i}^{(j)}$ be the Hecke operator at v of the double coset of $\mathrm{diag}(p1_i, 1)$ on forms on X_j, and $\mathbf{T}_j(X) := \sum_{i\leq n_j}(-X)^i q_v^{\binom{i}{2}} T_{v,i}^{(j)}$ for an indeterminate X; so $T_v = T_{v,r_p}^{(0)}$.

(A) The split unramified theta correspondence. Let w be a split place of norm q, let hermitian spaces of ranks n and $n+k'$ carry characters unramified at w, let ϕ_0 be a vacuum at w, and let $\Theta(\phi; \varphi)$ be bilinear in data ϕ and forms φ and equivariant at ϕ_0. For φ spherical at w, $\Theta(\phi_0; \varphi)$ is spherical at w and $\mathbf{T}'(X)\Theta(\phi_0; \varphi) = \prod_{l<k'}(1 - q^l \mathrm{fr}\, X)\,\Theta\bigl(\phi_0; \mathbf{T}(q^{k'}\mathrm{fr}\,\mathrm{fr}'^{-1}X)\varphi\bigr)$, where $\mathbf{T}$, $\mathbf{T}'$ are the Hecke polynomials of the two spaces and fr, fr$'$ the Frobenius values of the two characters at w. *Status*: classical [Ra, Ku]; the proof proves it.

(B) For the chain the proof reads (A) as follows. Let Ψ be a weak chain datum for ϑ, $p \nmid \mathrm{Nm}\, Q_\vartheta$, $v \in \mathfrak{M}$ and $j \geq 0$. Let $\chi_{v,j}$ be the value at a uniformizer of E_v of the base change of the character of the lift $X_j \to X_{j+1}$; then $|\eta\chi_{v,j}| = 1$, and for every $\mathfrak{t}$ in the support of Ψ the lift Θ from X_j to X_{j+1} with datum $v_j(\mathfrak{t})$ maps forms spherical at v to forms spherical at v, and on them

$$\mathbf{T}_{j+1}(X)\,\Theta = \mathcal{Q}_j(X)\,\Theta\,\mathbf{T}_j\bigl(p^{(t+1)f_p/2}X\bigr), \qquad \mathcal{Q}_j(X) := \prod_{l=0}^{t}\bigl(1 - q_v^l\, p^{n_j f_p/2}\chi_{v,j}X\bigr).$$

Problem 53.3.1. Model: $q_v = 25$, $p^{f_p/2} = 5$, $\chi_{v,0} = 1$, ranks 1 and 2 ($t = 0$), and $T_{v,1}^{(0)}$ acting by 2. Then $\mathcal{Q}_0(X)\,(1 - 2\cdot 5X) = (1 - 5X)(1 - 10X) = 1 - 15X + 50X^2$; so $T_{v,1}^{(1)}$ acts by 15 and $T_{v,2}^{(1)}$ by 2 on the image of Θ, and $5\,\Theta T_{v,1}^{(0)} = (T_{v,1}^{(1)} - 5)\Theta$.

Problem 53.3.2. Let $\mathcal{Q} \in \mathcal{O}_\eta[X]$ with $\mathcal{Q}(0) = 1$, and let linear maps Θ, T_i, T'_i $(0 \le i \le n)$ satisfy $\sum_i (-X)^i q_v^{\binom{i}{2}} T'_i \Theta = \mathcal{Q}(X)\,\Theta \sum_i (-p^{(t+1)f_p/2}X)^i q_v^{\binom{i}{2}} T_i$ as polynomials in X. Then for every i there are $c_{ii'} \in \mathcal{O}_\eta$, depending only on $\mathcal{Q}$ and q_v, with $p^{(t+1)if_p/2} q_v^{\binom{i}{2}}\,\Theta T_i = \sum_{i' \le i} c_{ii'} T'_{i'} \Theta$.

Problem 53.3.3. For $i \le r_p$, $p^{(t+1)if_p/2} q_v^{\binom{i}{2}}$ divides p^{fr_pt}; and $(j+1)fr_pt \le r_p f(n_m + r_p)$ for $j < m$.

Iterating Problem 53.3.2 along the first $j+1$ lifts, the proof writes $p^{r_p f(n_m+r_p)}$ times the chain of $j+1$ lifts after $T^{(0)}_{v,r_p}$ as $\sum_{i \le r_p} c_i T^{(j+1)}_{v,i}$ after the chain, with c_i independent of the translation, and $c_i \in \mathcal{O}_\eta$ for $j < m$ (Problem 53.3.3); Theorem 25.3.1 computes such coefficients in a model. A Hecke operator of the group of X_{j+1} acting on the datum passes to the lifted form, and is the sum of the translates $\omega(1,u)$ over the cosets u of its double coset. So the datum of lift j is replaced, for each $v \in \mathfrak{M}$ in turn, by $\sum_i c_i p^{a_v - r_p f(n_m+r_p)}\, T^{(j+1)}_{v,i}$ applied to it; the chain with the new data, applied to φ, is the chain applied to $Y^m_{\mathfrak{M}}\varphi$. For $j < m$, by Problem 53.2.4 and as $|\eta(c_i p^{a_v - r_p f(n_m+r_p)})| \le p^{r_p f(n_m+r_p) - a_v}$, the new datum of lift j multiplies gauges by at most p to the power $\#\mathfrak{M} \cdot r_p f(n_m + r_p) + r_p \sum_{\Phi_{\mathfrak{M}}} \beta_{>1} - \mathcal{D}_j(\Phi_{\mathfrak{M}})$: the a_v cancel. The new data still commute with the levels, the exponents add as in Problem 48.3.1, and restriction to Y_m at $p \ne N$ does not increase gauges. The proof obtains, for a mark $\mathfrak{M}$, a weak chain datum Ψ for ϑ with $p \nmid \operatorname{Nm} Q_\vartheta$, and $\varphi \in S_\eta$:

$(\star)$ $R_{\vartheta,\Psi}(Y^m_{\mathfrak{M}}\varphi)$ has valuation at least

$$-\sum_{j<m}\Big(\#\mathfrak{M} \cdot r_p f(n_m + r_p) + r_p \sum_{\sigma \in \Phi_{\mathfrak{M}}} \beta_{>1}(\sigma) - \mathcal{D}_j(\Phi_{\mathfrak{M}})\Big),$$

β read at heights below n_{j+1} in the jth term.

53.4. Paying for the transfer

Let $\mathfrak{M}$ be a mark and $0 \le j < m$, with β read at heights below n_{j+1}.

Problem 53.4.1. For $\sigma \in \Phi_{\mathfrak{M}}$, $r_p \beta_{>1}(\sigma) \le a/(pm) + \mathbf{1}_{\Phi_a}(\sigma)\, a/x_1$.

Problem 53.4.2. $\#\mathfrak{M} \cdot r_p f(n_m + r_p) + r_p \sum_{\sigma \in \Phi_{\mathfrak{M}}} \beta_{>1}(\sigma) \le L_p/m + \#(\Phi_a \cap \Phi_{\mathfrak{M}})\, a/x_1$.

Problem 53.4.3. If $\mathfrak{M}$ is full, then $\#\mathfrak{M} \cdot r_p f(n_m + r_p) + r_p \sum_{\sigma \in \Phi_{\mathfrak{M}}} \beta_{>1}(\sigma) - \mathcal{D}_j(\Phi_{\mathfrak{M}}) \le (2L_p - \operatorname{gain}(p))/m$.

In the model of Problem 50.2.7 at $p = 7$, the set $\{1, 9\}$ plays the part of $\Phi_{\mathfrak{M}}$: $C_7(\{1,9\}) = 0$, and the left side there is $46865/48$, against $\operatorname{gain}(7)/m = 1022$ (Problems 50.2.8 and 50.2.3). Summing Problem 53.4.3 over $j < m$ in $(\star)$ gives the following theorem, read from the proof.

Theorem 53.4.1. *Let p be a prime, $\eta\colon \mathbb{C} \to \mathbb{C}_p$ a ring map, ϑ a twist, Ψ a weak chain datum for ϑ with $p \nmid \operatorname{Nm} Q_\vartheta$, and $\mathfrak{M}$ a full mark at (p,η) (so $p < x_1$ is exceptional). For every $\varphi \in S_\eta$, $R_{\vartheta,\Psi}(Y^m_{\mathfrak{M}}\varphi)$ has valuation at least* $\operatorname{gain}(p) - 2L_p$.

What has been established. Theorem 53.4.1, from ($\star$) and Problems 53.4.1–53.4.3; ($\star$) rests on Problem 53.2.4 (from Problems 53.2.1–53.2.3, (C), Theorem 49.3.2 and (III), (IV) of Chapter 50), on (A) and (B), and on Problems 53.3.2 and 53.3.3. A full mark exists (Problem 53.1.5). Taken as given: the split unramified theta correspondence (A), classical; its form (B) for the chain and the kernel bound (C), read from the proof; the steps of Section 53.3 that lead from Problems 53.3.2 and 53.3.3 to ($\star$), read from the proof; and, from the earlier chapters, Theorem 49.3.2 and statements (III), (IV) of Chapter 50. Problem 48.4.3 adds $p^{j_p}S_\eta$ to the image; what remains for the exceptional primes is the colength of $Y^m_{\mathfrak{M}}S_\eta + p^{j_p}S_\eta$ in S_η (Section 48.4).

In the Lean formalization. In the Lean proof [GL] (paths relative to `grh/src/`; the namespace `New.` is omitted from names), Theorem 53.4.1 is `Data.IsWeakChainDatum.gaugeLe_restrictedChain_of_isFullMark` (`New/UpperBound/Divisibility/LocalDivisibility.lean`); ($\star$) is `Data.IsWeakChainDatum.gaugeLe_scaledHeckeOperator_pow` and Problem 53.2.4 is `Data.IsMarked.ω_ofSplitPlaces_mem_raises` (`New/UpperBound/Divisibility/ValuationAtNonSplitPrimes.lean`); Problems 53.1.5 and 53.4.2 are `Data.exists_isFullMark` and `Data.IsMarked.card_mul_transferExponent_add_sum_lowColumns_le` (`New/UpperBound/Divisibility/MarkedPrimes.lean`). Statement (A) is `SiegelWeil.hecke_transfer_of_pairing`, (B) is `Data.IsWeakChainDatum.exists_heckePolyOp_lift`, which states the existence of a polynomial with integral coefficients and constant term 1 ($\mathcal{Q}_j$ is the one its proof constructs), and (C) is `Parameters.omega_mem_raises_of_schurJet_le`. In the derivation of ($\star$) in Section 53.3, the transfer through the first $j+1$ lifts is `Data.IsWeakChainDatum.exists_hecke_transfer`; the Hecke operator on the datum is `Data.liftKernel_lift_heckeSplit` and `Data.IsMarked.ω_heckeSplit_mem_raises`; the new data are `Data.IsWeakChainDatum.exists_lift_eq_chain_scaledHeckeOperator`; the addition of the exponents and the restriction to Y_m are `Data.IsWeakChainDatum.gaugeLe_chain` and `Data.GaugeLe.restrictToY` (`New/UpperBound/Divisibility/ChainValuation.lean`). The double coset of Definition 53.2.1 is `basicDoubleCoset`, with `ofSplitPlaces`; f_p occurs in `Parameters.q_eq_pow_lcm_of_inert`.

Hints

§53.1.

53.1.1: $\mathrm{Gal}(E/\mathbb{Q}) \cong \mathrm{Gal}(K/\mathbb{Q}) \times (\mathbb{Z}/q_1)^\times$; the Frobenius at p is (nontrivial, p) and complex conjugation is (nontrivial, -1). Compare v_σ and v_τ through the decomposition group.

53.1.2: Orders modulo 18480; r_p is the least h with $m \le p^h$.

53.1.3: $2^{s+1} \mid q_1$ and $m = 2^e$, $s = 22e$ (Definition 33.3.1). Lift the exponent in $(-p)^o \equiv 1 \pmod{2^{s+1}}$.

53.1.4: Classes modulo q_0; Problems 53.1.1 and 53.1.3.

53.1.5: Choose one prime of each pair $\{v_\tau, \bar{v}_\tau\}$, $\tau \in \Phi_a$, by a total order; Problem 53.1.4 for why both are induced by a-places.

53.1.6: The class of $[-p]^i$ modulo q_0 lies in a group of odd order o_p, which does not contain -1.

53.1.7: Geometric series in $1/25$.

§53.2.

53.2.1: Elementary divisors over $\mathcal{O}_v$, and permutation matrices.

53.2.2: (i) The map is continuous for $\bar{v}_\tau$. (ii) Problem 53.1.6.

53.2.3: For $e \in I_p$, $v_{[-p^e]\tau} = \bar{v}_\tau$ and $\mathcal{I}([-p^e]\tau) = \mathcal{I}(\tau)$. Treat the rows in and out of $\mathcal{I}(\tau)$ separately.

53.2.4: Problem 53.2.1 and (C); then, as in Problem 50.4.4, Theorem 49.3.2 with Problem 53.2.3. Count $\epsilon + \mathfrak{c}$ box by box at $\Phi_{\mathfrak{M}}$ and at $\Phi_{\bar{\mathfrak{M}}}$; a column has distinct rows.

53.2.5: Only the monomials $(z_{1i}^5 z_{3i})^k (z_{3i}^5 z_{1i})^l$ contribute; exact rational arithmetic.

§53.3.

53.3.1: Compare the coefficients of X and X^2.

53.3.2: $\mathcal{Q}$ is a unit in $\mathcal{O}_\eta[[X]]$.

53.3.3: $f_p \le f$ and $r_p \le t$; $mt \le n_m$.

§53.4.

53.4.1: Problems 50.1.1 and 53.1.6; $r_p \le s$. If $p > m$, then $r_p = o_p = 1$.

53.4.2: $\#\mathfrak{M} \le f$; the scale inequalities make $f^2 r_p (n_m + r_p)p + fa/m \le fa(\log b)^2/m$.

53.4.3: Theorem 50.4.4(b) and Problem 53.4.2.

References

[GL] L. Sernau, *GRH for Dirichlet L-functions, in Lean 4*, a shorter rewriting of the Lean proof, text by Claude, `https://github.com/lsernau/grh-lean`, commit `72fead1`, readable edition `grh/`.

[Ku] S. S. Kudla, On the local theta-correspondence, *Invent. Math.* **83** (1986), 229–255.

[Ne] J. Neukirch, *Algebraic Number Theory*, Grundlehren Math. Wiss. 322, Springer, 1999.

[Ra] S. Rallis, Langlands' functoriality and the Weil representation, *Amer. J. Math.* **104** (1982), 469–515.

THEOREM C

Prerequisites. Hadamard's and Fischer's inequalities for positive definite Hermitian matrices [HJ, §7.8]. From Chapter 5 heights, covolume and Problem 5.3.2; from Chapter 6 the theorem on a twist for each prime; from Chapter 33 the data and Problem 33.4.6; from Chapter 34 the objects and the target lattice; and the statements of the auxiliary forms, the factorization of the chain determinant and the bound for small ratios (Chapter 55), of small ratios and the cost of one lift (Chapter 60), and of regular families (Chapter 67). Section 54.1 uses no earlier chapter.

Theorem C gives the lower bound used in Chapter 35, *The main inequality*, for the covolume plus twice the index of a linearly independent family of target forms spanning almost all of the target. For each prime ℓ and each field isomorphism $\iota\colon \mathbb{C} \to \overline{\mathbb{Q}}_\ell$, the proof chooses a twist θ_ι. It compares the chain Gram determinant at the trivial twist with its value at θ_ι, using a height bound for the family of ratios for each single lift. We first compare index and Gram determinant in a lattice, then state and prove Theorem C in the form used in the proof. This chapter heads Part IX; the chapters that follow it develop its inputs.

54.1. The comparison in a lattice

Let $N \geq 1$ be an integer, and give $\mathbb{C}^d$ the Hermitian form $\langle v, w\rangle := N\,\bar{v}^{\mathsf{T}} w$. For $y_1, \dots, y_n \in \mathbb{Q}^d$ write $\mathrm{Gram}(y) := \det(\langle y_i, y_j\rangle)_{i,j\leq n}$, and let $H := \log N$.

Problem 54.1.1. If $y_1, \dots, y_d \in \mathbb{Z}^d$ are linearly independent, then $\mathrm{Gram}(y) \geq N^d$, so $\log \mathrm{Gram}(y) \geq dH$. For $N = 5$, $y_1 = (1, 2)$, $y_2 = (2, -1)$ one has $\mathrm{Gram}(y) = 625$.

Problem 54.1.2. Let $y_1, \dots, y_d \in \mathbb{Q}^d$ be linearly independent, and let $u \in M_d(\mathbb{Z})$ with $\det u \neq 0$ be such that $\sum_k u_{ik} y_k \in \mathbb{Z}^d$ for every i. If $\log \mathrm{Gram}(y) \leq c$ and $\log|\det u| \leq \delta$, then $c + 2\delta \geq dH$. For $N = 5$, $y_1 = (\frac{1}{2}, 1)$, $y_2 = (0, \frac{1}{3})$, $u = \mathrm{diag}(2, 3)$, $c = \log \mathrm{Gram}(y)$ and $\delta = \log 6$ there is equality.

Now let the family be shorter than the dimension. Suppose it is completed to a basis by vectors of bounded length.

Problem 54.1.3. Let $y_1, \dots, y_n$ and $z_1, \dots, z_{n'}$ in $\mathbb{Z}^d$ together form a basis of $\mathbb{Q}^d$, with $\langle z_i, z_i\rangle \leq e^\beta$ for every i. Then $\log \mathrm{Gram}(y) + n'\beta \geq dH$. For $d = 3$, $N = 2$, $y_1 = (1, 1, 0)$, $y_2 = (0, 1, 1)$, $z_1 = (1, 0, 0)$: $\mathrm{Gram}(y) = 12$, $\mathrm{Gram}(y, z) = 8$, and $8 \leq 12 \cdot 2$.

Problem 54.1.4. Every linearly independent family $y_1, \dots, y_n \in \mathbb{Z}^d$ is completed to a basis of $\mathbb{Q}^d$ by $d - n$ of the standard basis vectors. Hence $\log \mathrm{Gram}(y) \geq nH$.

In Section 54.2 the main amount enters through the height of the family $\iota \mapsto Z(1)/Z(\theta_\iota)$, where the twist θ_ι is chosen for each pair (ℓ, ι) (Problem 54.2.4).

Date: November 26, 2026.

54.2. Theorem C

We use the parameters q_0, d and the data of Chapter 33, and the objects and notation of Chapter 34: the target forms T, of dimension d_T; the set Tw of m-fold twists ϑ, with the trivial twist 1 and the norm $\operatorname{Nm} Q_\vartheta$ of the modulus; the lower chain Θ_ϑ; the Gram determinants $Z(\vartheta)$ of the chain and $Z_j(\vartheta)$ of the jth single lift at ϑ^j; and families of twists $\theta = (\theta_\iota)$, one twist for each $\iota \mid \ell$. Among the conditions on the data, the scales $x < x_1 < b$ are integers with

$$(\log b)^{100} \le x, \qquad x^{10^6} \le x_1, \qquad x_1^{10^6} \le b, \qquad (\log x_1)^6 \le \log b, \qquad \log\log b \ge 10^{12},$$

the last inequality following from $10^{12}C \le \log\log b$ and $C \ge 1$, with C as in Chapter 33, Section 33.3. Further $a = xb$, $\sqrt{x} \le m \le 2\sqrt{x}$, $x^5 \le r \le 3x^5$, $k = r + 1 - m$, $t = 5r$ and $f \ge 1$. With $U = fa\log^3 b$ write $F := U \log b$. The main amount is $h_{\mathrm{main}} = mk\, h_{\mathrm{dir}}$, and $h_{\mathrm{main}} \ge 0$ by Problem 33.4.6. Heights of families $\iota \mapsto u_\iota$ are those of Chapter 5, Section 5.3; we write $\mathrm{ht}(u) \le c$.

The target lattice. The target lattice on T, with twists Tw, the lifts Θ_ϑ, injective by Problem 59.4.3, the twists allowed at ℓ, the lattices $\mathfrak{L}_{\vartheta,\iota}$, the squared lengths $\|v\|_\sigma^2$ of the σ-conjugated coordinate vectors of $\Theta_1 v$, and index and covolume of a family in T, is that of Definition 34.11.1; its volume at ϑ is $Z(\vartheta)$.

Theorem 6.2.1, for this lattice, reads as follows. Let $y_1, \dots, y_n, z_1, \dots, z_{n'}$ be a basis of T, where y has covolume at most c and index at most δ; let θ be a family of twists with θ_ι allowed at ℓ, and $\gamma\colon \mathrm{Tw} \to \mathbb{C}^\times$; suppose (i) $\gamma(\vartheta)\Theta_\vartheta z_i \in \mathfrak{L}_{\vartheta,\iota}$ for every i, every $\iota \mid \ell$ and every ϑ allowed at ℓ; (ii) $\|z_i\|_\sigma^2 \le e^{c_{\mathrm{short}}}$ for every i and σ; (iii) $\mathrm{ht}(|\gamma(\theta_\iota)|^{-2}) \le c_{\mathrm{den}}$; (iv) $\mathrm{ht}(Z(1)/Z(\theta_\iota)) \le c_{\mathrm{vol}}$. Then

$$0 \le c + 2\delta + n'(c_{\mathrm{short}} + c_{\mathrm{den}}) + c_{\mathrm{vol}}. \tag{1}$$

Four inputs feed it. (a) *Auxiliary forms* (Theorem 55.5.1). There are an integer e_γ and $\gamma\colon \mathrm{Tw} \to \mathbb{C}^\times$ with $\gamma(1) = 1$ and $|\gamma(\vartheta)| = (\operatorname{Nm} Q_\vartheta)^{e_\gamma/2} \prod_{0 \le i,j < m} \rho'_{ij}(\vartheta)$ such that T is spanned by forms z with $\gamma(\vartheta)\Theta_\vartheta z$ integral at ι whenever $\gcd(\ell, \operatorname{Nm} Q_\vartheta) = 1$ and with $\|z\|_\sigma^2 \le \exp(2x_1^2 b^2)$ for every σ. (b) *Single lifts.* There is a family θ with small ratios (Definition 64.2.2) such that $\mathrm{ht}(Z_j(1)/Z_j(\theta_\iota)) \le d_T(F/m - kh_{\mathrm{dir}})$ for $1 \le j \le m$; this combines the cost of one lift (Chapter 60) with a regular family (Chapter 67). Each θ_ι of such a family is allowed at ℓ. (c) *Factorization* (Theorem 55.4.1). There is an integer e_Z such that for every $\vartheta \in \mathrm{Tw}$

$$\frac{Z(\vartheta)}{Z(1)} = \Big((\operatorname{Nm} Q_\vartheta)^{ez/2} \prod_{1 \le i < j \le m} \rho_{ij}(\vartheta)\Big)^{d_T} \prod_{j=1}^{m} \frac{Z_j(\vartheta)}{Z_j(1)}.$$

(d) *Small ratios* (Theorem 55.5.2). If θ has small ratios, then for every integer e both families $\big((\operatorname{Nm} Q_{\theta_\iota})^{e/2} \prod_{0 \le i,j < m} \rho'_{ij}(\theta_\iota)\big)^{-1}$ and $\big((\operatorname{Nm} Q_{\theta_\iota})^{e/2} \prod_{1 \le i < j \le m} \rho_{ij}(\theta_\iota)\big)^{-1}$ have height at most $m^2 t x_1$.

Problem 54.2.1. The data satisfy $2m^2 t x_1 \le b$, $4(2x_1^2 + b^{-1}) \le b$, $b \le F$ and $4/b^2 \le 1/2$.

Problem 54.2.2. If $n \ge (1 - 4/b^2)d_T$ and $d_T = n + n'$, then $n'(2x_1^2 b^2 + b) \le d_T b$.

So the allowance for one completing auxiliary form is $2x_1^2 b^2 + b$, and the total allowance for the n' completing forms is at most $d_T b$.

Problem 54.2.3. For γ as in (a) and θ as in (b), $\mathrm{ht}(|\gamma(\theta_\iota)|^{-2}) \le b$.

Problem 54.2.4. For θ as in (b), $\mathrm{ht}(Z(1)/Z(\theta_\iota)) \le d_T(b + F - h_{\mathrm{main}})$.

Problem 54.2.5. Let $y_1, \dots, y_n \in T$ be linearly independent, with $n \geq (1 - 4/b^2)d_T$, covolume at most c and index at most δ. Then T has a basis $y_1, \dots, y_n, z_1, \dots, z_{n'}$ with each z_i as in (a), and $c + 2\delta \geq d_T(h_{\text{main}} - 3F)$.

Problems 54.2.1–54.2.5 prove the following.

Theorem 54.2.1 (Theorem C)**.** *Let $y_1, \dots, y_n$ be linearly independent target forms with $(1 - 4/b^2)d_T \leq n$, of index at most δ and covolume at most c. Then*

$$d_T(h_{\text{main}} - 3fa \log^4 b) \leq c + 2\delta.$$

In the Lean formalization. In the Lean proof [GL], Theorem 54.2.1 is `New.Data.integral_forms_long`, in `grh/src/New/Determinant/Twist/LongForms.lean`, and the input (b) is `New.Data.exists_hasSmallRatios_heightLe_liftDeterminant_div` in the same file; (1) is the case of the target lattice of `New.TwistedLattice.covolume_add_index_nonneg`, in `grh/src/New/Reduction/Lattices/TwistedLattice.lean`. In `LongForms.lean` the proof of (b) uses `New.exists_isRegularFamily` and `New.Data.heightLe_liftDeterminant_ratio`, and Problems 54.2.2 and 54.2.4 are `New.Data.mul_completion_cost_le` and `New.Data.heightLe_chainDeterminant_one_div`. The bounds of Problem 54.2.1 are instances of `New.Data.le_of_hasLogBound`. Problems 54.2.3 and 54.2.5 are steps in the proof of `New.Data.integral_forms_long`, the basis of Problem 54.2.5 coming from `New.exists_extend_basis_of_span_eq_top`. Theorem 54.2.1 is applied in the proof of `New.star_inequality`.

Hints

§54.1.

54.1.1: $(\langle y_i, y_j \rangle) = N Y Y^{\mathsf{T}}$ for the matrix Y with rows y_i, and $\det Y$ is a nonzero integer.

54.1.2: Problem 54.1.1 for the rows of uY.

54.1.3: Fischer's inequality for the Gram matrix of (y, z), Hadamard's for $\text{Gram}(z)$, then Problem 54.1.1.

54.1.4: Steinitz exchange and Problem 54.1.3; each standard basis vector has squared length N.

§54.2.

54.2.1: $m^2 \leq 4x$, $t \leq 15x^5$ and $x \geq 2$.

54.2.2: $n' \leq 4d_T/b^2$.

54.2.3: Input (d), Problem 5.3.2 and Problem 54.2.1.

54.2.4: Invert (c); bound the scalar by (d) and the single lifts by (b), and add by Problem 5.3.2.

54.2.5: Apply (1) with $c_{\text{short}} = 2x_1^2 b^2$, $c_{\text{den}} = b$ and $c_{\text{vol}} = d_T(b + F - h_{\text{main}})$.

References

[GL] L. Sernau, *GRH for Dirichlet L-functions, in Lean 4*, a shorter rewriting of the Lean proof, text by Claude, `https://github.com/lsernau/grh-lean`, commit `72fead1`, readable edition `grh/`.

[HJ] R. A. Horn and C. R. Johnson, *Matrix Analysis*, 2nd ed., Cambridge Univ. Press, 2013.

THE DETERMINANT OF A CHAIN

Prerequisites. Linear algebra over $\mathbb{C}$: adjoints and determinants. From Chapter 23: the Gaussian moments c_a of Section 23.2, and Problems 23.2.1, 23.2.3 and 23.3.2. From Chapter 34: the chosen places $\mathcal{M}$, the spaces Y_j, W_j, V_j, the principal and good forms $H(V) \supseteq H_g(V)$, the target forms $T = H_g(Y_0)$ of dimension d_T, tame characters ξ with their sets Q_ξ, twists and m-fold twists ϑ, the characters μ_j^0 of the lifts, the lower chain Θ_ξ, the single lifts $\hat{u}_{\xi,j}$ and $u_{\xi,j}$, the determinants $Z(\vartheta)$, $Z_j(\vartheta)$, and the partial Hecke values $L^S(z,\nu)$ and critical pairs, with their ratios $R_P(\vartheta,\epsilon)$ (Definition 34.10.1). From Chapter 56: the twist factor c_Q (Definition 56.3.1), the Rallis operators $\mathcal{R}_j(\xi;V)$ (Definition 56.3.2) and Theorem 56.4.1. From Chapter 57: the Petersson product and Corollary 57.4.1. From Chapter 59: the ratios $\rho_{ij}(\vartheta)$, the product $\mathcal{R}_\vartheta$ and the relation $\doteq$ (Definitions 59.3.2, 59.4.1, 59.3.1), Theorem 59.4.1 and Problem 59.4.3. From Chapter 5: heights of families (Problem 5.3.2); from Chapter 64: families with small ratios (Definition 64.2.2). Chapter 8 explains why a chain of m maps is used; it is not needed for the problems.

How does the determinant $Z(\vartheta)$ of the chain change with the m-fold twist ϑ? By Theorem 55.4.1, its quotient by $Z(1)$ is the product of the m quotients $Z_j(\vartheta)/Z_j(1)$ for single lifts, times a correction factor: a product of pairwise ratios $\rho_{ij}(\vartheta)$ of Hecke L-values, multiplied by $(\operatorname{Nm} Q_\vartheta)^{ez/2}$ with an integer e_Z independent of ϑ, and raised to the power d_T. The problems derive Theorem 55.4.1 from three statements of the following chapters: the Gram identity of one lift (Theorem 56.4.1), the comparison of the good forms on W_j and on Y_0 (Corollary 57.4.1), and the Gram identity of the chain (Theorem 59.4.1), which rests on the exchange identity (Theorem 58.5.1). The proof also states Theorem 55.4.1. Section 55.1 treats the linear algebra in its simplest setting; Sections 55.2–55.4 assemble the theorem. Section 55.5 gives two further results used in the proof of Theorem C; both are read from the proof (Theorems 55.5.1 and 55.5.2).

55.1. Volumes of maps

For a linear map $u\colon U \to V$ of finite-dimensional complex inner product spaces let

$$Z(u) := \det_U(u^* u),$$

the determinant on the domain U; we call it the *volume* of u. Dimensions are complex dimensions, the determinant on the zero space is 1, and inner products are conjugate-linear in the first argument and linear in the second.

Problem 55.1.1. For every orthonormal basis $e_1, \dots, e_d$ of U, $Z(u) = \det\big(\langle ue_a, ue_b\rangle\big)_{a,b}$. The number $Z(u)$ is real and ≥ 0, and $Z(u) > 0$ if and only if u is injective.

Problem 55.1.2. Let S be an endomorphism of U and $a \in \mathbb{C}$ with $\langle ux, uy\rangle = a\langle x, Sy\rangle$ for all $x, y \in U$. Then $Z(u) = a^{\dim U} \det S$.

Date: November 26, 2026.

Problem 55.1.3. If $\theta_j\colon V_{j-1}\to V_j$, for $1\le j\le m$, are linear maps between spaces of one and the same dimension, then $Z(\theta_m\circ\cdots\circ\theta_1)=\prod_{j=1}^{m}Z(\theta_j)$.

When the dimension grows along the chain, equality can fail.

Problem 55.1.4. Let $\theta_2\colon\mathbb{C}^2\to\mathbb{C}^2$ be $\operatorname{diag}(1,2)$, and let $\theta_1,\theta_1'\colon\mathbb{C}\to\mathbb{C}^2$ be $x\mapsto(x,0)$ and $x\mapsto(0,x)$. Then $Z(\theta_1)=Z(\theta_1')=1$ and $Z(\theta_2)=4$, while $Z(\theta_2\theta_1)=1$ and $Z(\theta_2\theta_1')=4$.

What replaces Problem 55.1.3 is an identity for $\Theta^*\Theta$ on the first space itself (Theorem 59.4.1); Problem 59.1.2 is a model of how such an identity can be propagated along a chain.

For $a\ge 0$ divisible by 4, the two lifts from U(1) of Chapter 23 used here have a one-dimensional source. The lift $\Theta_{(a)}$ from U(1) to U(1) is multiplication by $c_a/4$ (Problem 23.2.3), and by Problem 23.3.2 the lift $\Theta_{(a)}$ from U(1) to U(2) satisfies

$$\|\Theta_{(a)}\varphi\|^2=\lambda_a\|\varphi\|^2,\qquad \lambda_a:=\frac{1}{128}\sum_j\binom{a}{j}c_j^2c_{a-j}^2.$$

This finite calculation illustrates the inner product of a lift with itself; the strict rank inequality of the inner product formula (Theorem 56.2.1) first allows a source of rank 1 when the target has rank 3, the case with which Chapter 56 begins.

Problem 55.1.5. For $4\mid a$, the composite of the lift $\mathrm{U}(1)\to\mathrm{U}(1)$ with the lift $\mathrm{U}(1)\to\mathrm{U}(2)$ of Chapter 23, in degree a, has volume $\lambda_a c_a^2/16$, the product of the two volumes.

55.2. One lift

For $1\le j\le m$ and a tame character ξ, the single lift $\hat u_{\xi,j}$ on $H(W_j)$ and its restriction $u_{\xi,j}$ to $H_g(W_j)$ are those of Section 34.9; $H(V)$ carries the Petersson product (Section 57.3). We recall two statements. By Theorem 56.4.1, for every $1\le j\le m$ there is $a_j\in\mathbb{C}$, $a_j\neq 0$, such that for every tame character ξ,

$$\hat u_{\xi,j}^*\,\hat u_{\xi,j}=a_j\,c_{Q_\xi}\,\mathcal{R}_j(\xi;W_j)$$

on $H(W_j)$, with c_Q the twist factor of Definition 56.3.1 and $\mathcal{R}_j(\xi;V)$ the Rallis operator of Definition 56.3.2; and $\hat u_{\xi,j}$ is injective. By Corollary 57.4.1, for $1\le j\le m$: $\dim H_g(W_j)=d_T$, and for every tame character ξ, $\mathcal{R}_j(\xi;Y_0)$ maps T to itself, $\mathcal{R}_j(\xi;W_j)$ maps $H_g(W_j)$ to itself, and

$$\det\bigl(\mathcal{R}_j(\xi;W_j)\mid H_g(W_j)\bigr)=\det\bigl(\mathcal{R}_j(\xi;Y_0)\mid T\bigr).$$

Problem 55.2.1. For $1\le j\le m$ and every tame character ξ, $Z(u_{\xi,j})=(a_jc_{Q_\xi})^{d_T}\det\bigl(\mathcal{R}_j(\xi;Y_0)\mid T\bigr)$. Moreover $Z(u_{\xi,j})>0$.

55.3. Twists and the ratios

Tame characters ξ, their sets Q_ξ and powers ξ^n, twists and m-fold twists ϑ are as in Chapter 34; the power ξ^n has the same set Q_ξ.

Problem 55.3.1. If ϑ is an m-fold twist and $1\le n\le m$, then ϑ^n is a twist with the same set Q_ϑ, so $c_{Q_{\vartheta^n}}=c_{Q_\vartheta}$.

For $1 \le i < j \le m$ and an m-fold twist ϑ, $\rho_{ij}(\vartheta)$ is the ratio of Definition 59.3.2: with $\nu := \mu_j^0/\mu_i^0$,

$$\rho_{ij}(\vartheta) := \prod_{z=1}^{t} \frac{|L^{\mathcal{M}\cup Q_\vartheta}\big(z, (\nu\vartheta^{j-i})^{-1}\big)|}{|L^{\mathcal{M}}(z,\nu^{-1})|},$$

a nonnegative real number. These ratios enter the Gram identity of the chain through the exchange identity (Theorem 58.5.1), whose scalar has squared modulus a constant times the exchange factor $\mathrm{ex}_h(S,\nu)$ of Definition 58.2.3; Chapter 59 applies it with $h = t$ and $S = \mathcal{M} \cup Q_\vartheta$, once for each pair $i < j$.

Problem 55.3.2. $\rho_{ij}(1) = 1$ for $1 \le i < j \le m$.

55.4. The factorization

For an m-fold twist ϑ, the lower chain Θ_ϑ of Section 34.9, restricted to T, takes values in a space of algebraic level forms on Y_m with the class-sum inner product; it is injective (Problem 59.4.3). In the notation of Section 55.1, $Z(\vartheta) = Z(\Theta_\vartheta|_T)$ and $Z_j(\vartheta) = Z(u_{\vartheta^j,j})$. Let $\mathcal{R}_\vartheta = \mathcal{R}_1(\vartheta;Y_0)\,\mathcal{R}_2(\vartheta^2;Y_0)\cdots\mathcal{R}_m(\vartheta^m;Y_0)$ be the endomorphism of T of Definition 59.4.1. By Theorem 59.4.1 there is a function c from m-fold twists to $\mathbb{C}$ with $c \doteq \prod_{1\le i<j\le m}\rho_{ij}$, that is (Definition 59.3.1), with a real number C' and an integer e' such that $|c(\vartheta)|^2 = C'(\mathrm{Nm}\,Q_\vartheta)^{e'}\big(\prod_{1\le i<j\le m}\rho_{ij}(\vartheta)\big)^2$ for every m-fold twist ϑ, and such that for every m-fold twist ϑ and all $x, y \in T$,

$$\langle \Theta_\vartheta x, \Theta_\vartheta y\rangle = c(\vartheta)\, c_{Q_\vartheta}^m\, \langle x, \mathcal{R}_\vartheta y\rangle.$$

Problem 55.4.1. Let X be a set with a point 1, let $N\colon X \to \mathbb{R}_{>0}$ and $f\colon X \to \mathbb{R}_{\ge 0}$ with $N(1) = f(1) = 1$, and let $c\colon X \to \mathbb{C}$, $C' \in \mathbb{R}$ and $e' \in \mathbb{Z}$ satisfy $|c(x)|^2 = C'N(x)^{e'}f(x)^2$ for all x. If $c(1) \ne 0$, then $C' = |c(1)|^2$ and $|c(x)/c(1)| = N(x)^{e'/2}f(x)$ for all x.

Problem 55.4.2. In Theorem 59.4.1, if $c(1) = 0$ then $T = 0$. For every m-fold twist ϑ,

$$Z(\vartheta) = \Big(c(\vartheta)\Big/\prod_{j=1}^{m} a_j\Big)^{d_T}\prod_{j=1}^{m} Z_j(\vartheta),$$

and $Z(\vartheta) > 0$.

Problem 55.4.3. If $T \ne 0$, then for every m-fold twist ϑ,

$$\frac{Z(\vartheta)}{Z(1)} = \Big((\mathrm{Nm}\,Q_\vartheta)^{e'/2}\prod_{1\le i<j\le m}\rho_{ij}(\vartheta)\Big)^{d_T}\prod_{j=1}^{m}\frac{Z_j(\vartheta)}{Z_j(1)}.$$

If $T = 0$, both sides equal 1 (a real number to the power 0 is 1).

The proof states the normalized determinant identity as follows.

Theorem 55.4.1. *Let P be parameters and D admissible data for P. There is an integer e_Z such that for every m-fold twist ϑ:*

(a) $0 < Z(\vartheta)$;
(b) $0 < Z_j(\vartheta)$ *for every integer j with* $1 \le j \le m$;
(c) *in* $\mathbb{C}$,

$$\frac{Z(\vartheta)}{Z(1)} = \Big((\mathrm{Nm}\,Q_\vartheta)^{e_Z/2}\prod_{i=1}^{m}\prod_{j=i+1}^{m}\rho_{ij}(\vartheta)\Big)^{d_T}\prod_{j=1}^{m}\frac{Z_j(\vartheta)}{Z_j(1)}.$$

Here $Z(\vartheta)$ and $Z_j(\vartheta)$ are complex numbers by definition, and (a), (b) say that they are real and positive; the base of the power d_T in (c) is a real number, with $e_Z/2$ a real exponent, and e_Z does not depend on ϑ. Problems 55.2.1 and 55.4.1–55.4.3, with Theorem 56.4.1, Corollary 57.4.1 and Theorem 59.4.1, prove Theorem 55.4.1; one may take $e_Z = e'$ when $T \neq 0$. Thus the volume of the chain at a twist, relative to the trivial twist, is expressed through m volumes of single lifts, a power of $\operatorname{Nm} Q_\vartheta$, and $m(m-1)/2$ ratios ρ_{ij} of L-values.

55.5. Auxiliary forms

The proof of Theorem C extends a linearly independent family of target forms to a basis. For each m-fold twist ϑ, a common nonzero scalar makes the ϑ-lifts of the added forms integral at every $\iota \mid \ell$ with $\ell \nmid \operatorname{Nm} Q_\vartheta$. Both statements of this section are read from the proof. The *turn ratios* are

$$\rho'_{ij}(\vartheta) := \prod_{z=1}^{t} \frac{|L^{\mathcal{M}\cup Q_\vartheta}\big(z, (\mu^0_{i+1}\mu^0_{j+1}\,\vartheta^{j+1})^{-1}\big)|}{|L^{\mathcal{M}}\big(z, (\mu^0_{i+1}\mu^0_{j+1})^{-1}\big)|}, \qquad 0 \le i, j < m,$$

a factor with zero denominator being 0. For an automorphism σ of $\mathbb{C}$ write $\|y\|^2_\sigma$ for the squared norm of the conjugate of a form y by σ.

Theorem 55.5.1 (auxiliary forms)**.** *There are an integer e_γ and numbers $\gamma(\vartheta) \in \mathbb{C}^\times$, one for each m-fold twist, with $\gamma(1) = 1$ and*

$$|\gamma(\vartheta)| = (\operatorname{Nm} Q_\vartheta)^{e_\gamma/2} \prod_{0\le i,j<m} \rho'_{ij}(\vartheta),$$

such that T is spanned by the forms y with the two properties: $\gamma(\vartheta)\Theta_\vartheta y$ is integral at every $\iota \mid \ell$ with $\ell \nmid \operatorname{Nm} Q_\vartheta$, for every m-fold twist ϑ; and $\|\Theta_1 y\|^2_\sigma \le \exp(2x_1^2 b^2)$ for every automorphism σ of $\mathbb{C}$.

Theorem 55.5.2 (small ratios)**.** *Let θ be a family of m-fold twists with small ratios (Definition 64.2.2). For every integer e, the families*

$$\iota \mapsto \Big((\operatorname{Nm} Q_{\theta_\iota})^{e/2} \prod_{1\le i<j\le m} \rho_{ij}(\theta_\iota)\Big)^{-1} \quad \text{and} \quad \iota \mapsto \Big((\operatorname{Nm} Q_{\theta_\iota})^{e/2} \prod_{0\le i,j<m} \rho'_{ij}(\theta_\iota)\Big)^{-1}$$

have height at most $m^2 t x_1$.

By Problem 59.4.6 each ρ_{ij} is a product of t ratios $R_P(\vartheta^{j-i}, 1)$ with P a ramified critical pair; the proof shows that each ρ'_{ij} is likewise a product of t ratios $R_P(\vartheta^n, 1)$, with $1 \le n \le m$ and P a ramified critical pair.

Problem 55.5.1. Let θ be a family of m-fold twists such that, for every $1 \le n \le m$ and every ramified critical pair P, the ratios $R_P(\theta_\iota^n, 1)$ are nonzero and the family $\iota \mapsto R_P(\theta_\iota^n, 1)^{-1}$ has height at most x_1. Then the families $\iota \mapsto \big(\prod_{1\le i<j\le m} \rho_{ij}(\theta_\iota)\big)^{-1}$ and $\iota \mapsto \big(\prod_{0\le i,j<m} \rho'_{ij}(\theta_\iota)\big)^{-1}$ have height at most $m^2 t x_1$; the first is a product of $m(m-1)/2$ inverse ratios ρ_{ij}^{-1}, the second of m^2.

In the Lean formalization. In the Lean proof [GL], Theorem 55.4.1 is `New.Data.exists_chainDeterminant_pos_and_div_chainDeterminant_one_eq` in `New/Determinant/Chain/NormOfChain.lean` of the readable edition; Theorem 55.5.1 is `exists_span_isAuxiliaryForm_eq_top` in `New/Determinant/Twist/LongForms.lean`, with ρ'_{ij} the `turnRatio` of `New/Determinant/`

`AuxiliaryForms/Turns.lean`; and Theorem 55.5.2 is `HasSmallRatios.heightLe_inv_rpow_mul_prod_quotientRatio` in `NormOfChain.lean` together with `HasSmallRatios.heightLe_inv_rpow_mul_prod_turnRatio` in `LongForms.lean`.

Hints

§55.1.

55.1.1: $\langle ue_a, ue_b\rangle = \langle e_a, u^*u\, e_b\rangle$, and u^*u is positive semidefinite with kernel $\ker u$.

55.1.2: Rewrite the hypothesis as an identity of endomorphisms of U.

55.1.3: In orthonormal bases of spaces of equal dimension, $Z(u) = |\det u|^2$.

55.1.4: Problem 55.1.1 with $U = \mathbb{C}$.

55.1.5: Problem 55.1.1 on a line.

§55.2.

55.2.1: Problem 55.1.2 on $H_g(W_j)$, which $\mathcal{R}_j(\xi; W_j)$ preserves; then the equality of determinants and $\dim H_g(W_j) = d_T$. For positivity, Problem 55.1.1 and the injectivity of $\hat{u}_{\xi,j}$.

§55.3.

55.3.1: The definition of ϑ^n in Section 34.6, and Definition 56.3.1.

55.3.2: At the trivial twist $Q_1 = \varnothing$ and $1^{j-i} = 1$.

§55.4.

55.4.1: Evaluate at 1 first.

55.4.2: For the first statement, Theorem 59.4.1 at $\vartheta = 1$, and injectivity. For the formula, Problems 55.1.2, 55.3.1 and 55.2.1; compare the factors c_Q for ϑ^j and ϑ.

55.4.3: Take absolute values in Problem 55.4.2 and divide by the case $\vartheta = 1$, using Problems 55.4.1 and 55.3.2. For $T = 0$, Corollary 57.4.1.

§55.5.

55.5.1: For a product, add the upper bounds for the heights of its factors (Problem 5.3.2). A height bound may be increased, and $m(m-1)/2 \le m^2$.

References

[GL] L. Sernau, *GRH for Dirichlet L-functions, in Lean 4*, a shorter rewriting of the Lean proof, text by Claude, `https://github.com/lsernau/grh-lean`, commit `72fead1`, readable edition `grh/`.

THE NORM OF ONE LIFT

Prerequisites. Adjoints (inner products are conjugate-linear in the first argument). From Chapter 21: the class sets Cl_n, the groups Γ_L and Problems 21.1.2 and 21.1.4. From Chapter 23: the theta function $\Theta_{L,L'}$, the lift (1) and Problems 23.1.5, 23.5.1 and 23.3.2; the Gaussian constant $\vartheta_0 := \sum_{\alpha\in\mathbb{Z}[\mathrm{i}]} e^{-\pi|\alpha|^2}$ of that chapter. From Chapter 22: Section 22.4. From Chapter 34: $\mathcal{M}$, $\bar{G}$ (Section 34.1), W_j, V_j (Section 34.3), $H(V)$ (Section 34.4), with the Petersson product (Section 57.3), tame characters ξ, Q_ξ, (ψ_w) (Section 34.6), μ_j^0 (Section 34.7) and $\hat{u}_{\xi,j}$ on $H(W_j)$ (Section 34.9).

Theorem 55.4.1 of Chapter 55 expresses the volume of the chain, relative to the trivial twist, through the corresponding ratios for m single lifts on good forms, a power of the norm of the twist and ratios of L-values. For each it needs $\hat{u}^*\hat{u} =$ (scalar) $\cdot$ (Hecke series). How is the norm of a theta lift computed, and where does the twist enter?

56.1. The squared norm of a lift is a theta sum on the doubled space

We use the definite model of Chapter 23 in weight 0, from U(1) to U(3). By Problem 21.1.4 the class sets of I_1 and I_3 have one element each; let 1 be the constant form on Cl_1, so $\|1\|^2 = 1/4$. Write $\Theta_{(0)}\colon \mathcal{A}_{(0)}(1) \to \mathcal{A}_{(0)}(3)$ for the lift (1) in weight 0, and $\Theta'_{(0)}$ for the lift in the other direction. In weight 0 the kernel of (1) at (L, L') is the number $\Theta_{L,L'}(0) = \sum_{u\in \mathrm{Hom}_{\mathcal{O}}(L,L')} e^{-\pi h(u,u)}$.

Problem 56.1.1. $(\Theta_{(0)}1)(I_3) = \vartheta_0^3/4 = 0.4111137902\ldots$, where $\vartheta_0 = 1.1803405990\ldots$ is the square of $\sum_{n\in\mathbb{Z}} e^{-\pi n^2}$.

Problem 56.1.2.

$$\frac{\|\Theta_{(0)}1\|^2}{\|1\|^2} = \frac{\vartheta_0^6}{1536} = \frac{1}{384}\cdot\frac{1}{4}\sum_{(\alpha,\beta)\in\mathcal{O}^3\times\mathcal{O}^3} e^{-\pi(|\alpha|^2+|\beta|^2)} = 0.0017605682\ldots,$$

with $\mathcal{O} = \mathbb{Z}[\mathrm{i}]$ and $|\alpha|^2 = \sum_k |\alpha_k|^2$.

The middle expression is a theta sum over $\mathrm{Hom}_{\mathcal{O}}(I_1 \oplus I_1, I_3) = \mathcal{O}^3 \times \mathcal{O}^3$; in general:

Problem 56.1.3. For unimodular Hermitian lattices L, L',

$$\Theta_{L,L'}(0)\,\overline{\Theta_{L,L'}(0)} = \Theta_{L\oplus L,L'}(0).$$

Hence, for the weight-0 lift $\Theta_{(0)}$ from Cl_n to $\mathrm{Cl}_{n'}$ and its reverse $\Theta'_{(0)}$, the kernel of $\Theta'_{(0)}\Theta_{(0)}$ at (L, L), $L \in \mathrm{Cl}_n$, is the sum of $|\Gamma_{L'}|^{-1}\,\Theta_{L\oplus L,L'}(0)$ over $L' \in \mathrm{Cl}_{n'}$.

The class sum models the adelic doubling integral: for a source $V^\flat$ and a target $V^\sharp$, a theta kernel times the conjugate of another is a theta function on $\mathrm{Hom}(V^\flat \oplus (V^\flat)^-, V^\sharp)$, and the doubled source ($(V^\flat)^-$ has the negated form) is split. Let

Date: November 26, 2026.

V^0 and $V^\sharp$ be framed Hermitian spaces, in the sense of Section 34.3, over a CM field with a chosen CM type and Weil data, V^0 with a complete splitting into p hyperbolic planes (in this sheet p counts planes) and $V^\sharp$ of rank $n^\sharp > 2p$, and let ω be the split Weil action on the test space $\mathcal{S}$ of $\mathrm{Hom}(V^0, V^\sharp)$. For a rational Lagrangian $\mathcal{L}$ of V^0 let $D_{\mathcal{L}}(\phi)$ be the value at 0 of $\phi \in \mathcal{S}$ in the Schrödinger model of a splitting whose isotropic space is $\mathcal{L}$. Then the operator norms of the $D_{\mathcal{L}}$ are summable, $g^\sharp \mapsto \theta(\omega(1, g^\sharp)\phi)$ is integrable for every ϕ, and

$$\int_{[\mathrm{U}(V^\sharp)]} \theta(\omega(1, g^\sharp)\phi)\, dg^\sharp = \mathrm{vol}[\mathrm{U}(V^\sharp)] \sum_{\mathcal{L}} D_{\mathcal{L}}(\phi),$$

where $\mathrm{vol}[\mathrm{U}(V^\sharp)]$ is the total mass of the quotient measure. This is the Siegel–Weil formula in Weil's range [We65, Thm. 5]. *Status*: classical; the proof establishes it in this form. For $V^0 = V^\flat \oplus (V^\flat)^-$ the condition is $2n^\flat < n^\sharp$; for $n^\flat = 1$ it first holds for U(3), not for the U(2) of Problem 23.3.2.

For the summability the proof assigns to each $\mathcal{L}$ a vector $\mathbf{e} \in \mathbb{N}^p$ of dyadic exponents (with $0 \in \mathbb{N}$); with $|\mathbf{e}| := e_1 + \cdots + e_p$ and f the number of infinite places, at most $C\, 2^{2fp|\mathbf{e}|}$ Lagrangians have a given $\mathbf{e}$, and $\|D_{\mathcal{L}}\| \le C' 2^{-fn^\sharp|\mathbf{e}|}$.

Problem 56.1.4. For integers $p, f \ge 1$ and $n^\sharp$, $\sum_{\mathbf{e}\in\mathbb{N}^p} 2^{-f(n^\sharp-2p)|\mathbf{e}|} = \sum_{l\ge 0} \binom{l+p-1}{p-1} 2^{-f(n^\sharp-2p)l}$. It converges if and only if $n^\sharp > 2p$, with sum $(1 - 2^{-f(n^\sharp-2p)})^{-p}$; for $p = f = 1$, $n^\sharp = 3$ the sum is 2, and the terms with $l \le 5$ give 63/32.

56.2. Only graphs survive, and unfolding

Which Lagrangians of the doubled space contribute? Over a finite field, let $\mathbb{F}_9 = \mathbb{F}_3[\mathrm{i}]$, with conjugation $z \mapsto \bar z := z^3$.

Problem 56.2.1. The norm $z \mapsto z\bar z$ from $\mathbb{F}_9$ to $\mathbb{F}_3$ has fibres of sizes $1, 4, 4$ over $0, 1, 2$. The form $z_1\bar z_1 - z_2\bar z_2$ on $\mathbb{F}_9^2$ has 33 isotropic vectors (including 0) and 4 isotropic lines, and these lines are the graphs $\{(\delta z, z) : z \in \mathbb{F}_9\}$ of the 4 elements δ of norm 1.

Problem 56.2.2. Let $V^\flat$ be a nondegenerate Hermitian space of dimension $n^\flat$ over a field with involution, with Gram matrix J, and give $V^\flat \oplus (V^\flat)^-$ the Gram matrix $\mathrm{diag}(J, -J)$. Let $\mathcal{L}$ be a Lagrangian, with frame $\binom{K_1}{K_2}$: a $2n^\flat \times n^\flat$ matrix of rank $n^\flat$ whose columns span $\mathcal{L}$. If K_2 is invertible, then $\delta := -K_1K_2^{-1}$ is an isometry of $V^\flat$ and $\mathcal{L} = \{(\delta z, -z) : z \in V^\flat\}$. If $V^\flat$ has no nonzero isotropic vector, every Lagrangian is of this form.

For the clean data ϕ of Theorem 56.2.1 below, the proof shows that only graphs of rational isometries contribute (by Problem 56.2.2 when $V^\flat$ is definite): for the doubled datum of the translates of ϕ', ϕ by g', g, the term of $\{(\delta^{-1}z, -z)\}$ is $\langle \phi', \omega(g'^{-1}\delta g)\phi\rangle$. Integrating against $y(g)\overline{y'(g')}$ then unfolds, as in this finite model.

Problem 56.2.3. Let Γ be a subgroup of a finite group G, let K be a function on G (in this sheet K is a function; the field $\mathbb{Q}(\sqrt{-d})$ does not occur), and let y, y' be functions on G invariant on the left under Γ, with $\langle y', y\rangle := \sum_{g\in\Gamma\backslash G} \overline{y'(g)}\, y(g)$. Then

$$\sum_{g,g'\in\Gamma\backslash G} \sum_{\delta\in\Gamma} K(g'^{-1}\delta g)\, y(g)\, \overline{y'(g')} = \sum_{g\in G} K(g)\, \langle y', y(\cdot\, g)\rangle.$$

The result is the Rallis inner product formula. Let $V^\flat$, $V^\sharp$ be framed Hermitian spaces over a CM field with a chosen CM type and Weil data, of ranks $n^\flat$, $n^\sharp$ with $2n^\flat < n^\sharp$, and let $G^\flat$ be the adelic unitary group of $V^\flat$. Let χ_1, χ_2 be continuous unitary characters of the norm-one ideles trivial on rational points, and let ϕ, ϕ' lie in the adelic test space of $\mathrm{Hom}(V^\flat, V^\sharp)$. Suppose that ϕ is *clean*: either all signs of $V^\flat$ agree, or $\phi = \phi_1 \otimes \phi_0$ for a Schwartz–Bruhat function ϕ_1 at a set of finite places disjoint from its conjugate such that, at some finite place, every matrix in the support of ϕ_1 has a left inverse. Let y, y' be automorphic functions on $G^\flat$ of rapid decay, let $\Theta[\phi]\, y$ be the theta lift of y to the group of $V^\sharp$ with datum ϕ and characters (χ_1, χ_2), and put $K(g) := \langle \phi', \omega(g)\phi \rangle \, \langle y', y(\cdot\, g) \rangle$, where $\omega(g)$ is the action of $(g, 1)$ with characters $(1, \chi_2)$ and the second factor is the Petersson product.

Theorem 56.2.1 (Rallis inner product formula)**.** *K is integrable on all of $G^\flat$, and $\langle \Theta[\phi']y', \Theta[\phi]y \rangle = \mathrm{vol}[\mathrm{U}(V^\sharp)] \int_{G^\flat} K(g)\, dg$.*

This is the unitary form, used here, of Rallis's inner product formula; for the classical method see [Ra87, §§ 2–3]. *Status*: classical; the proof derives it in this form from the Siegel–Weil formula, as Problems 56.2.2 and 56.2.3 model.

56.3. The sharp datum and the twist factor

For $1 \le j \le m$ the single lift $\hat{u}_{\xi,j}$ goes from W_j, of rank r, to V_j, of rank $r+t > 2r$; $H(W_j)$ is finite-dimensional (Chapter 57, Section 57.3 and Problem 57.3.1), so $\hat{u}_{\xi,j}$ has an adjoint. At the places of $\mathcal{M} \cup Q_\xi$ every residue matrix in the support of its finite datum has a left inverse; this support count and the count of all such matrices (through the target level index) give the finite factor in Theorem 56.4.1.

Problem 56.3.1. Of the 5^3 columns of height 3 over $\mathbb{F}_5$, exactly 124 have a left inverse; of the 5^6 columns of height 6, exactly 15624.

Problem 56.3.2. For integers $r \ge 1$ and $t \ge 0$, the number of $(r+t) \times r$ matrices over $\mathbb{F}_q$ with a left inverse is $q^{r(r+t)} \prod_{v=t+1}^{t+r} (1 - q^{-v})$.

Definition 56.3.1. For a finite set Q of finite places of E, with residue fields k_w of order q_w, the *twist factor* is

$$c_Q := (\mathrm{Nm}\, Q)^{rt} \prod_{w \in Q} \prod_{v=t+1}^{t+r} \left(1 - q_w^{-v}\right), \qquad \mathrm{Nm}\, Q := \prod_{w \in Q} q_w,$$

where r is the source rank and t the target rank minus the source rank; for the single lifts of the data, $t = 5r$ and $Q = Q_\xi$.

Problem 56.3.3. $c_Q = \prod_{w \in Q} (\lambda_w / q_w^{r^2})$, where λ_w (in this sheet) is the number of $(r+t) \times r$ matrices over k_w with a left inverse; in particular $c_\varnothing = 1$. Formally evaluating the expression of Definition 56.3.1 at $Q = \{w\}$, $q_w = 5$, $r = 1$ gives $c_Q = 124/5$ for $t = 2$ and $c_Q = 15624/5$ for $t = 5$.

Give the standard lattice stabilizer in each finite adelic unitary group Haar volume 1. When both lifts use the same sharp datum (below) and the unprimed form has principal level, the finite integration in Theorem 56.2.1 is a sum over cosets of the subgroup integral outside $\mathcal{M} \cup Q_\xi$ and their conjugates, and the integral on each coset supplies the mass of the finite datum as a factor; here is the finite model.

Problem 56.3.4. Let Γ and $\mathcal{J}$ be subgroups of a finite group G, let y, y' be functions on $\Gamma\backslash G$, and let y be invariant on the right under $\mathcal{J}$. With the pairing of Problem 56.2.3, $\sum_{g\in G} \mathbf{1}_{\mathcal{J}}(g)\,\langle y', y(\cdot\, g)\rangle = \#\mathcal{J}\,\langle y', y\rangle$.

The lift $\hat{u}_{\xi,j}$ uses a highest-vector Fock datum ϕ_∞ at the infinite places and a finite Weil vector F_{fin}, obtained from the vacuum by imposing, modulo the product of the places of $\mathcal{M}\cup Q_\xi$, the following residue function F (in this sheet) on families $\mathbf{X} = (X_w)_{w\in\mathcal{M}\cup Q_\xi}$ of $(r+t)\times r$ matrices over the k_w: $F(\mathbf{X}) := \prod_{w\in Q_\xi} \psi_w(\det X'_w)$ if X_w is the standard inclusion $\binom{1}{0}$ at every $w\in\mathcal{M}$, and $F(\mathbf{X}) := 0$ otherwise; here X'_w is the top $r\times r$ block of X_w, and $\psi_w(0) := 0$. Let $J_{\mathcal{M}}$ (in this sheet) be the principal level of $H(W_j)$ and K° the stabilizer of the standard lattice. Let S_0 be the set of places of $\mathcal{M}\cup Q_\xi$ and their conjugates. In the matrix coefficients of this lift take $\chi_2 = b_j := \mu_j^0\xi\,\upsilon^{\lfloor (r+t)/2\rfloor}$ in Theorem 56.2.1, with υ the splitting character on the norm-one ideles. The proof shows that F_{fin} is *sharp* for $J_{\mathcal{M}}$ off S_0: for every Fock vector v, $v\otimes F_{\mathrm{fin}}$ is clean and a vacuum off S_0; $\|F_{\mathrm{fin}}\|^2 = \langle F_{\mathrm{fin}}, F_{\mathrm{fin}}\rangle \neq 0$; and for finite g integral outside S_0, $\langle F_{\mathrm{fin}}, \omega(g)F_{\mathrm{fin}}\rangle = \|F_{\mathrm{fin}}\|^2\,\mathbf{1}_{J_{\mathcal{M}}}(g)$. The *mass* of F_{fin} is $\|F_{\mathrm{fin}}\|^2/[K^\circ : J_{\mathcal{M}}]$, where $\|F_{\mathrm{fin}}\|^2$ is the mean of $|F(\mathbf{X})|^2$ over all families $\mathbf{X}$ and $[K^\circ : J_{\mathcal{M}}] = \#\bar{G}$.

Problem 56.3.5. $\sum_{\mathbf{X}} |F(\mathbf{X})|^2 = \#\mathrm{GL}_r(Q_\xi)\cdot(\mathrm{Nm}\,Q_\xi)^{rt}$, where $\#\mathrm{GL}_r(Q) := \prod_{w\in Q}\#\mathrm{GL}_r(k_w)$.

The class-sum product on the target of $\hat{u}_{\xi,j}$ is the index of the level of V_j times the dimension of the coefficient representation times the Petersson product of the associated adelic forms, and the proof shows that this index times $\#\mathrm{GL}_r(Q_\xi)$ is $\prod_{w\in\mathcal{M}\cup Q_\xi}\lambda_w$, the size of the orbit of the standard inclusion. Put

$$c_{\mathrm{ch}} := \prod_{w\in\mathcal{M}}\left(\frac{1}{\#\mathrm{GL}_r(k_w)}\prod_{v=t+1}^{t+r}\left(1-q_w^{-v}\right)\right),$$

a nonzero number that does not depend on ξ.

Problem 56.3.6. With λ_w as in Problem 56.3.3,

$$\frac{(\mathrm{Nm}\,Q_\xi)^{rt}}{\#\bar{G}}\prod_{w\in\mathcal{M}\cup Q_\xi}\frac{\lambda_w}{q_w^{(r+t)r}} = c_{\mathrm{ch}}\,c_{Q_\xi}.$$

So the index of the level of V_j times the mass of F_{fin} is $c_{\mathrm{ch}}c_{Q_\xi}$, and only the factor c_{Q_ξ} depends on ξ.

At the other places the integral becomes a sum over Hecke cosets. Write A (in this sheet) for the set of finite places outside S_0. For a finite point γ of the unitary group of a framed space V of rank r let $\Delta_f(\gamma)$ be its finite Weil multiplier and (in this sheet)

$$\mathrm{mc}(\gamma) := \left(b_j(\det\gamma)\,\Delta_f(\gamma)^{r+t}\right)^{-1},$$

so $\mathrm{mc}(1) = 1$. For a datum that is a vacuum on A, left multiplication by γ supported on A multiplies its matrix coefficient at g, with g integral on A, by $\mathrm{mc}(\gamma)$.

Definition 56.3.2. Let $j\geq 0$ be an integer, ξ a tame character, and V a framed space of rank r, with any signs, such as W_j or Y_0. The *Rallis operator* $\mathcal{R}_j(\xi;V)$ is the endomorphism of $H(V)$ given by

$$\mathcal{R}_j(\xi;V)\,y := \sum_\gamma \mathrm{mc}(\gamma)\,y(\cdot\,\gamma),$$

where γ runs over representatives, equal to 1 outside A, of the finite points of $\mathrm{U}(V)$ modulo those integral at every place of A.

Through the frames, all framed spaces V of rank r have the same finite adelic unitary group, so one family of representatives γ serves every V; the representatives are 1 at the places of $\mathcal{M}$, and neither they nor the coefficients $\mathrm{mc}(\gamma)$ depend on V.

The proof shows that for $2r < r + t$ the series converges absolutely, lies in $H(V)$, and $\langle y', \mathcal{R}_j(\xi; V)\, y\rangle = \sum_\gamma \mathrm{mc}(\gamma)\langle y', y(\cdot\,\gamma)\rangle$ for $y, y' \in H(V)$; it proves the summability of the coefficients by counting neighbouring lattices. For $1 \le j \le m$, the sharp-data form of Theorem 56.2.1 and Problem 56.3.6 give, for every tame character ξ and all $y, y' \in H(W_j)$,

$$\langle \hat{u}_{\xi,j}\, y', \hat{u}_{\xi,j}\, y\rangle = a_j\, c_{Q_\xi}\, \langle y', \mathcal{R}_j(\xi; W_j)\, y\rangle,$$

where a_j is c_{ch} times the dimension of the coefficient representation times a constant c_∞ (in this sheet) that depends only on the spaces and the real data. As ξ has weight 0, a_j does not depend on ξ. Here $c_\infty = \mathrm{vol}[\mathrm{U}(V_j)]\, z_\infty$, where z_∞ (in this sheet) is the integral over the real source group of $\langle \phi_\infty, \Omega(x,1)\phi_\infty\rangle\, \overline{e(x)}/e(1)$, with e the source type kernel and Ω the real Weil action. The proof shows that $z_\infty \neq 0$ and that the lift with datum $\phi_\infty \otimes F_{\mathrm{fin}}$ takes forms of the source type to forms of the target type; for the correspondence at infinity see [Li90].

56.4. Injectivity and the theorem

Is $\mathcal{R}_j(\xi; V)$ injective? The proof partitions A into finitely many disjoint conjugation-stable sets, on each of which the neighbour weights (the number of steps at w times $q_w^{-(r+t)/2}$) add up to at most $1/3$. By sharpness, $b_j \circ \det$ is trivial on the integral points supported on A. On bounded functions fixed by the integral points supported on these places, the series over a union of parts is the composite of their series; on one part the moduli of the $\mathrm{mc}(\gamma)$ off the trivial coset add up to at most $1/2$, by a walk whose one-step weights total at most $1/3$.

Problem 56.4.1. $\sum_{l \ge 1} 3^{-l} = 1/2$. Let y be a bounded function on a group G, and let $g_i \in G$ and $\zeta_i \in \mathbb{C}$, $i \ge 1$, with $\sum_i |\zeta_i| \le 1/2$. If $y + \sum_i \zeta_i\, y(\cdot\, g_i) = 0$, then $y = 0$.

With Problem 56.4.1 this gives what the proof shows: $\mathcal{R}_j(\xi; V)$ is injective.

Problem 56.4.2. Let $u\colon \mathcal{E} \to \mathcal{E}'$ be a linear map of finite-dimensional complex inner product spaces, $\mathcal{R}$ an injective endomorphism of $\mathcal{E}$, and $\zeta \in \mathbb{C}$, $\zeta \neq 0$. If $\langle uy', uy\rangle = \zeta\langle y', \mathcal{R}y\rangle$ for all $y, y' \in \mathcal{E}$, then u is injective.

Problem 56.4.3. In Problem 56.4.2, the identity $\langle uy', uy\rangle = \zeta\langle y', \mathcal{R}y\rangle$ for all y, y' is equivalent to $u^*u = \zeta\,\mathcal{R}$.

Problems 56.3.4–56.3.6 compute the finite factor $c_{\mathrm{ch}} c_{Q_\xi}$ of the Gram identity of Section 56.3, whose other inputs we took from the proof, and Problem 56.4.3 turns it into the following theorem, which the proof states in this form.

Theorem 56.4.1. *For every $1 \le j \le m$ there is $a_j \in \mathbb{C}$, $a_j \neq 0$, such that for every tame character ξ,*

$$\hat{u}^*_{\xi,j}\, \hat{u}_{\xi,j} = a_j\, c_{Q_\xi}\, \mathcal{R}_j(\xi; W_j)$$

on $H(W_j)$.

By Problem 56.4.2 and the injectivity of $\mathcal{R}_j(\xi; W_j)$, the lift $\hat{u}_{\xi,j}$ is injective.

Taken as given were the Siegel–Weil formula in Weil's range, Theorem 56.2.1 in its sharp form, the summability of the coefficients, the archimedean properties of ϕ_∞, the sharpness of F_{fin}, the class-sum product and the index identity on the target of $\hat{u}_{\xi,j}$, and the change of matrix coefficients under left multiplication, and the bound on the neighbour weights behind the injectivity of $\mathcal{R}_j(\xi; V)$. Chapter 57 compares $\det \mathcal{R}_j(\xi; W_j)$ and $\det \mathcal{R}_j(\xi; Y_0)$ on good forms. The rank hypothesis of Theorem 56.2.1 holds for $Y_0 \to Y_1$ but not for $Y_1 \to Y_2$, as $2(r+t) > r + 2t$; the chain identity uses the exchange identity of Chapter 58 instead.

In the Lean formalization. In the Lean proof [GL], Theorem 56.4.1 is `New.Data.exists_adjoint_singleLift_comp_eq` in `New/Determinant/Norms/AdjointThetaLift.lean`, and the Gram identity of Section 56.3, with $\langle y', \mathcal{R}_j(\xi; W_j)\, y\rangle$ written as its series over γ, is `Data.exists_hasSum_inner_singleLift` there. See also, in that file, `DescentPair.twistFactor`, `Data.rallisOperator`, `DescentPair.isSharp_blockDatum` and `DescentPair.gramFactor_div_card`, and in `Lib/SiegelWeil/` the declarations `New.SiegelWeil.siegel_weil`, `New.SiegelWeil.inner_product_formula` (Theorem 56.2.1), `New.SiegelWeil.rallis_inner_product_cosetTerm` and `New.SiegelWeil.eq_zero_of_rallisSeries_eq_zero`.

Hints

§56.1.

56.1.1: Equation (1) with $|\Gamma_{I_1}| = 4$; $\mathrm{Hom}_{\mathcal{O}}(I_1, I_3) = \mathcal{O}^3$, and the sum over $\mathcal{O} = \mathbb{Z} \oplus \mathbb{Z}\mathrm{i}$ factors.

56.1.2: The squared norm on $\mathcal{A}_{(0)}(3)$ and Problem 21.1.2 for I_3.

56.1.3: $\mathrm{Hom}_{\mathcal{O}}(L \oplus L, L') = \mathrm{Hom}_{\mathcal{O}}(L, L')^2$; Problems 23.5.1 and 23.1.5.

56.1.4: Count the $\mathbf{e} \in \mathbb{N}^p$ with $|\mathbf{e}| = l$, and expand $(1-z)^{-p}$.

§56.2.

56.2.1: $(u_1 + u_2\mathrm{i})\overline{(u_1 + u_2\mathrm{i})} = u_1^2 + u_2^2$.

56.2.2: Isotropy reads $K_1^* J K_1 = K_2^* J K_2$; then look at vectors of $\mathcal{L}$ of the form $(z, 0)$.

56.2.3: Fix representatives of $\Gamma\backslash G$ and the representative g'. As δ and the representative g vary together, which values does $g'^{-1}\delta g$ take?

§56.3.

56.3.2: Left inverse means independent columns; choose them one at a time.

56.3.5: Sum place by place; $|\psi_w(d)| = 1$ for $d \neq 0$.

56.3.6: Problem 56.3.2, and the definition of $\bar{G}$.

§56.4.

56.4.1: Compare $\sup|y|$ with its half.

References

[GL] L. Sernau, *GRH for Dirichlet L-functions, in Lean 4*, a shorter rewriting of the Lean proof, text by Claude, `https://github.com/lsernau/grh-lean`, commit `72fead1`, readable edition `grh/`.

[Li90] J.-S. Li, *Theta lifting for unitary representations with nonzero cohomology*, Duke Math. J. **61** (1990), 913–937.

[Ra87] S. Rallis, *L-functions and the oscillator representation*, Lecture Notes in Math. 1245, Springer, 1987.

[We65] A. Weil, *Sur la formule de Siegel dans la théorie des groupes classiques*, Acta Math. **113** (1965), 1–87.

EQUAL MULTIPLICITIES

Prerequisites. Linear algebra over $\mathbb{C}$: traces, characteristic polynomials and Newton's identities [Mac, Ch. I, §2]. Modular forms of weight two on $\Gamma_0(N)$ and their Hecke operators [DS, Ch. 5]. From Chapter 24, *Hecke operators and theta lifts*: Section 24.4, with Problems 24.4.2 and 24.4.3. From Chapter 34, *Spaces, forms and twists*: the chosen places $\mathcal{M}$, the group $\bar{G}$, good families of labels and the idempotent e_0 (Section 34.1); the gap Δ and the target parameter ς_τ (Section 34.2, Problem 34.2.1); the spaces Y_0, W_j and their signs (Sections 34.3 and 34.4, Problem 34.3.1); principal and good forms $H(V) \supseteq H_g(V)$ and the target $T = H_g(Y_0)$ of dimension d_T; tame characters (Section 34.6). From Chapter 33: $r = 3^{e'}$ is odd, $x^5 \le r$, m is even, and the weights $\kappa(\tau)$ are integers. From Chapter 56: the Rallis operators $\mathcal{R}_j(\xi; V)$ (Definition 56.3.2). Inner products are conjugate-linear in the first variable. Problems marked "by machine" use Sage [Sage].

The single lifts of Chapter 55, *The determinant of a chain*, start from the spaces W_j, which have the rank of Y_0 but other signs at the real places. How can a determinant on $H_g(W_j)$ be compared with one on $T = H_g(Y_0)$, when no map between the two spaces is given? In the proof one Hecke algebra acts on both spaces with equal traces. The equality gives their dimensions and characteristic polynomials and, with the decompositions into joint eigenspaces, the multiplicities of the Hecke eigensystems. This sheet derives the consequences, and states the equality (Theorem 57.3.3) with the comparison of trace formulas behind it.

57.1. Hecke operators of a finite group

Here K is a subgroup (the field $\mathbb{Q}(\sqrt{-d})$ does not occur). Let the symmetric group S_3 act on $\mathbb{C}^3$ by $(\sigma v)_i = v_{\sigma^{-1}(i)}$, let $K = \{1, (12)\}$ and $g = (23)$.

Problem 57.1.1. The double coset KgK has 4 elements. For a K-fixed vector $v = (v_1, v_1, v_3)$, the average of σv over $\sigma \in KgK$ is $\left(\frac{v_1+v_3}{2}, \frac{v_1+v_3}{2}, v_1\right)$; in the coordinates (v_1, v_3) of the K-fixed vectors it is $(v_1, v_3) \mapsto \left(\frac{v_1+v_3}{2}, v_1\right)$.

Problem 57.1.2. Let a group G act on a complex inner product space U by unitary operators, let $K \subseteq G$ be a subgroup and $g \in G$ be such that $K_g := K \cap gKg^{-1}$ has finite index in K. On the K-fixed vectors U^K the operator $\mathrm{av}_K(g) := [K : K_g]^{-1} \sum_{\delta K_g \in K/K_g} \delta g$ does not depend on the representatives, maps U^K to itself, and satisfies $\langle z, gy\rangle = \langle z, \mathrm{av}_K(g) y\rangle$ for all $z, y \in U^K$. If K is finite, $\mathrm{av}_K(g)y$ is the average of σy over $\sigma \in KgK$.

Problem 57.1.3. The operator of Problem 57.1.1 has traces $2, \frac{1}{2}, \frac{5}{4}, \frac{7}{8}$ in its powers $0, 1, 2, 3$, characteristic polynomial $(X-1)(X+\frac{1}{2})$ and determinant $-\frac{1}{2}$.

Problem 57.1.4. Let a monoid act linearly, with its unit acting as the identity and products as composites, on finite-dimensional complex spaces U and U', and suppose $\mathrm{tr}_U h = \mathrm{tr}_{U'} h$ for every element h. Then $\dim U = \dim U'$, and every

Date: November 26, 2026.

element h has the same characteristic polynomial, hence the same determinant, on U and on U'.

Problem 57.1.5. The matrices $\mathrm{diag}(1,2)$ and $\left(\begin{smallmatrix} 0 & -2 \\ 1 & 3 \end{smallmatrix}\right)$ both have traces $3, 5, 9$ in their powers $1, 2, 3$, and $\det(h+1) = 6$ for both.

Problem 57.1.6. In Problem 57.1.4, suppose moreover that the monoid is commutative and acts diagonalizably on U and on U'. Then for every function λ from the monoid to $\mathbb{C}$ the joint eigenspaces $\{y : hy = \lambda(h)y \text{ for all } h\}$ in U and in U' have the same dimension.

57.2. Brandt matrices: a model

Where do two spaces with the same Hecke traces come from? The classical case compares a definite quaternion algebra with GL_2. Let B, $\mathcal{O}_1$, $\mathcal{O}_2$, the Brandt matrices $B(\ell)$ for primes $\ell \neq 11$, and the cusp form f be as in Section 24.4 and Problem 24.4.3; $B(\ell)$ acts on functions y on the two classes by $(B(\ell)y)(i) = \sum_j B_{ij}(\ell)\, y(j)$. The space of cusp forms of weight 2 on $\Gamma_0(11)$ is $\mathbb{C}f$ [DS, §3.9], and $T_\ell f = a_\ell(f) f$.

Problem 57.2.1. (By machine.) For $\ell = 2, 3, 5, 7, 13$: $\mathrm{tr}\, B(\ell) = 1, 3, 7, 6, 18$, and $\mathrm{tr}\, B(\ell) - (\ell+1) = a_\ell(f) = -2, -1, 1, -2, 4$.

Problem 57.2.2. (a) If an idempotent e on a finite-dimensional space U commutes with an operator h, then eU is stable under h and $\mathrm{tr}(h \mid eU) = \mathrm{tr}_U(he)$. (b) For a prime $\ell \neq 11$, the constant function is an eigenvector of $B(\ell)$ with eigenvalue $\ell+1$, and the line $U_0 := \{y : y(1)/|\mathcal{O}_1^\times| + y(2)/|\mathcal{O}_2^\times| = 0\}$ is stable under $B(\ell)$; hence $\mathrm{tr}(B(\ell) \mid U_0) = \mathrm{tr}\, B(\ell) - (\ell+1)$.

For the five primes of Problem 57.2.1, Problems 57.2.1 and 57.2.2 give $\mathrm{tr}(B(\ell) \mid U_0) = a_\ell(f)$: once the constants are removed, the Brandt matrices have the traces of the Hecke operators on cusp forms. The equality for every prime $\ell \neq 11$ is the level-11 case of the correspondence of Eichler and of Jacquet and Langlands [Ei73], [JL, §16]; *Status*: classical. It is a model only: the group of units of B and GL_2 differ at 11 as well as at infinity, whereas the proof compares unitary groups that differ only at the real places.

Problem 57.2.3. (By machine.) The quaternion algebra over $\mathbb{Q}$ ramified at 37 and ∞ has three classes of left ideals of a maximal order; its Brandt matrix $B(2)$ has characteristic polynomial $(X-3)X(X+2)$, and T_2 on the cusp forms of weight 2 on $\Gamma_0(37)$ has characteristic polynomial $X(X+2)$.

At level 37 the factor of the constants is $X-3$, and what remains is the characteristic polynomial of T_2 on cusp forms.

57.3. Equal traces

Let V be a framed space of rank r over E with numbered signs $s = (s(0), \ldots, s(r-1))$ (in this sheet s is a system of signs and, below, a an element of a group algebra; the numbers s and a of the data do not occur), such as Y_0 or W_j (Section 34.4). Through the frames, all such V have the same finite adelic unitary group G_f, that of the identity form; it acts on forms on V by right translation. Give $H(V)$ and its subspaces the *Petersson inner product* $\langle y', y\rangle := \int \overline{y'(g)}\, y(g)\, dg$, the integral over

the quotient of the adelic unitary group of V by its rational points, for the quotient measure fixed in the proof.

Definition 57.3.1. The numbered signs s of V satisfy the *gap hypothesis* if at every infinite place $\tau \in \Phi$ the entries $2\varsigma_\tau(0), \dots, 2\varsigma_\tau(r-1)$ are distinct, are congruent to $r-1$ modulo 2, and satisfy $|2\varsigma_\tau(i) - 2\varsigma_\tau(i')| \geq 2\Delta$ whenever $s(i) \neq s(i')$.

Under the gap hypothesis the proof shows that $H(V)$ is finite-dimensional; traces below are taken under this hypothesis.

Problem 57.3.1. The gap hypothesis holds for Y_0 and for W_j, $1 \leq j \leq m$.

Definition 57.3.2. In this sheet $G_f^{\mathcal{M}}$ is the subgroup of the $g \in G_f$ whose component at every $w \in \mathcal{M}$ is 1; the component at w determines that at $\bar{w}$, so these components are 1 as well. An element a of the group algebra $\mathbb{C}[G_f^{\mathcal{M}}]$ is *spherical* if, in every representation of G_f, it maps the vectors fixed by the principal level to vectors fixed by the principal level. A spherical a acts on $H(V)$ for every framed V of rank r; the *Hecke algebra away from* $\mathcal{M}$, $\mathbb{T}^{\mathcal{M}}$, is the algebra of the families of operators on the spaces $H(V)$, one for each V, given in this way by one spherical element. For a finite place w and $i \in \mathbb{N}$, let $h_{w,i} \in \mathbb{T}^{\mathcal{M}}$ be the Hecke operator (the sum of the translates by representatives of its single cosets) of the $\mathrm{GL}_r(\mathcal{O}_w)$-double coset of $\mathrm{diag}(\varpi_w 1_i, 1_{r-i})$ in $\mathrm{GL}_r(E_w)$, with $\mathcal{O}_w$ the local ring of integers and ϖ_w a uniformizer, if w is split, $w, \bar{w} \notin \mathcal{M}$ and $i \leq r$; in all other cases $h_{w,i} := 0$.

In this sheet an *eigensystem* is a family $\lambda = (\lambda_{w,i})$ of complex numbers indexed by the finite places w and $i \in \mathbb{N}$, and $H(V)_\lambda := \{y \in H(V) : h_{w,i} y = \lambda_{w,i} y \text{ for all } w, i\}$. The proof lets $\bar{G}$ act on $H(V)$ through integral lifts whose components outside $\mathcal{M} \cup \overline{\mathcal{M}}$ are 1.

Problem 57.3.2. An element of $G_f^{\mathcal{M}}$ commutes with every element of G_f whose components outside $\mathcal{M} \cup \overline{\mathcal{M}}$ are 1. Hence every $h \in \mathbb{T}^{\mathcal{M}}$ commutes with the action of $\bar{G}$, and so with e_0, on $H(V)$, and maps $H_g(V)$ to itself.

For V satisfying the gap hypothesis and $h \in \mathbb{T}^{\mathcal{M}}$, write $\mathrm{tr}(h \mid H_g(V))$ for the trace of the restriction of h to $H_g(V)$. The proof establishes the following.

Theorem 57.3.3. *Let V and V' be framed spaces of rank r over E whose numbered signs satisfy the gap hypothesis. Then every $h \in \mathbb{T}^{\mathcal{M}}$ has* $\mathrm{tr}(h \mid H_g(V)) = \mathrm{tr}(h \mid H_g(V'))$.

Theorem 57.3.3 is not proved here. The proof deduces it from a comparison of simple trace formulas. Let E be a CM field with a fixed CM type, containing the 5040th roots of unity and having an even number of infinite places. Let V, V' be framed spaces of rank $n \geq 2$ over E with numbered signs s, s', and G_f their common finite adelic group. For each infinite place τ let $l_\tau \in \mathbb{Z}^n$ have distinct entries congruent to $n-1$ modulo 2, with $|l_\tau(i) - l_\tau(i')| \geq 2(500n^3 + 10n^5)$ whenever $s(i) \neq s(i')$ or $s'(i) \neq s'(i')$. Let K_f be a subgroup of the group of integral elements of G_f that contains a neighbourhood of the identity, and let $a \in \mathbb{C}[G_f]$ map K_f-fixed vectors to K_f-fixed vectors in every representation of G_f. Suppose that the test function $a \star 1_{K_f}$ is *cuspidal* at a split place w, with residue field k_w: for every nonempty proper set I of coordinates, with pr_I the diagonal projection onto it, every $\bar{g} \in \mathrm{GL}_n(k_w)$, every family $(u_A)_{A \in M_n(k_w)}$ in $\mathrm{GL}_n(\mathcal{O}_w)$ with u_A reducing to $(1 + \mathrm{pr}_I A(1 - \mathrm{pr}_I))\bar{g}$, and every $g \in G_f$, the sum of $(a \star 1_{K_f})(g\, u_A)$ over $A \in$

$M_n(k_w)$ is zero, u_A being placed in G_f at w. Then operators acting as a on the K_f-fixed forms of parameter l on V and on V' (defined like the principal forms, with l_τ for $2\varsigma_\tau$ and K_f for the principal level) have the same trace. For the classical arguments, see [Lab, Thms. 5.4–5.5], [AC, Ch. 1, Lemmas 2.4–2.6] and, for a cuspidal component, [HL, Prop. 1.10.5]; *Status*: the method is classical; the proof establishes the comparison in this form, with integrable idempotent kernels of discrete series in place of pseudo-coefficients.

The data meet these conditions: the proof shows that E contains the 5040th roots of unity and has an even number of infinite places, and $\Delta = 2r^8 \geq 500r^3 + 10r^5$ and $r \geq 2$ because $r \geq x^5 \geq 9$, x being large. The idempotent e_0 is the sum of the orthogonal idempotents $e_c := \bigotimes_w e_{c_w}$ over the good families c, so by Problem 57.2.2(a) the trace of $h \in \mathbb{T}^{\mathcal{M}}$ on $H_g(V)$ is $\sum_c \mathrm{tr}_{H(V)}(he_c)$. The proof shows that he_c acts on $H(V)$ for every V through one element of $\mathbb{C}[G_f]$ that keeps the principal-level vectors, and that its test function is cuspidal at a chosen place w where c_w is primitive (irreducible with a root of order $(\#k_w)^r - 1$); every good family has such a place (Section 34.1), and chosen places are split. The comparison applies to each term, with K_f the principal level and $l_\tau = 2\varsigma_\tau$.

57.4. Dimensions, eigenspaces and determinants

Problem 57.4.1. $\dim H_g(W_j) = d_T$ for $1 \leq j \leq m$.

When $H(V)$ is finite-dimensional, the proof shows that it is the direct sum of the spaces $H(V)_\lambda$ (the operators $h_{w,i}$ are normal and commute).

Problem 57.4.2. Let λ be an eigensystem and fix finitely many eigensystems $\lambda' \neq \lambda$. A polynomial in finitely many of the $h_{w,i}$, an element of $\mathbb{T}^{\mathcal{M}}$, acts on $H(V)$, for every framed V of rank r, as the identity on $H(V)_\lambda$ and as zero on each of these $H(V)_{\lambda'}$.

Problem 57.4.3. For every eigensystem λ and $1 \leq j \leq m$, the spaces $T \cap H(Y_0)_\lambda$ and $H_g(W_j) \cap H(W_j)_\lambda$ have the same dimension.

Let ξ be a tame character and $j \in \mathbb{N}$. By Definition 56.3.2 and the formula for its matrix coefficients proved with it, for every framed V of rank r and all $z, y \in H(V)$,

$$\langle z, \mathcal{R}_j(\xi; V)\, y\rangle = \sum_\gamma \mathrm{mc}(\gamma)\, \langle z, \gamma y\rangle,$$

a sum, convergent in any order, over the countable family of representatives $\gamma \in G_f$ of that definition, the same family for every V, whose components at the places of $\mathcal{M}$ are 1, with the coefficients $\mathrm{mc}(\gamma)$ of Chapter 56, which depend on ξ, j and γ but not on V; here $\gamma y := y(\cdot\,\gamma)$. For each $\gamma \in G_f^{\mathcal{M}}$ the proof supplies an element $\mathrm{av}(\gamma) \in \mathbb{T}^{\mathcal{M}}$, an average of translates as in Problem 57.1.2, such that $\langle z, \mathrm{av}(\gamma) y\rangle = \langle z, \gamma y\rangle$ for every framed V of rank r and all $z, y \in H(V)$.

Problem 57.4.4. Let U and U' be finite-dimensional complex inner product spaces, and let pairs $(h_i, h_i') \in \mathrm{End}\, U \times \mathrm{End}\, U'$, for i in a countable set, lie in one complex linear subspace. Let $h_\infty \in \mathrm{End}\, U$ and $h_\infty' \in \mathrm{End}\, U'$ be such that $\sum_i \langle z, h_i y\rangle = \langle z, h_\infty y\rangle$ for all $z, y \in U$ and $\sum_i \langle z', h_i' y'\rangle = \langle z', h_\infty' y'\rangle$ for all $z', y' \in U'$, the sums converging in any order. Then (h_∞, h_∞') lies in that subspace. In particular, let a complex algebra act on U and on U' through complex-linear algebra homomorphisms to $\mathrm{End}\, U$ and $\mathrm{End}\, U'$; if each (h_i, h_i') is the action of one element, then one element acts as h_∞ on U and as h_∞' on U'.

Problem 57.4.5. Let V and V' be framed spaces of rank r satisfying the gap hypothesis, ξ a tame character and $j \in \mathbb{N}$. One element of $\mathbb{T}^{\mathcal{M}}$ acts as $\mathcal{R}_j(\xi; V)$ on $H(V)$ and as $\mathcal{R}_j(\xi; V')$ on $H(V')$. In particular $\mathcal{R}_j(\xi; V)$ maps $H_g(V)$ to itself.

Problem 57.4.6. For $1 \le j \le m$ and every tame character ξ, $\det\big(\mathcal{R}_j(\xi; W_j) \mid H_g(W_j)\big) = \det\big(\mathcal{R}_j(\xi; Y_0) \mid T\big)$.

Problems 57.4.1, 57.4.3, 57.4.5 and 57.4.6 prove the following.

Corollary 57.4.1. *Let $1 \le j \le m$. Then $\dim H_g(W_j) = d_T$; for every eigensystem λ the λ-eigenspaces of the $h_{w,i}$ in T and in $H_g(W_j)$ have the same dimension; and for every tame character ξ, $\mathcal{R}_j(\xi; Y_0)$ maps T to itself, $\mathcal{R}_j(\xi; W_j)$ maps $H_g(W_j)$ to itself, and $\det\big(\mathcal{R}_j(\xi; W_j) \mid H_g(W_j)\big) = \det\big(\mathcal{R}_j(\xi; Y_0) \mid T\big)$.*

The problems deduce Corollary 57.4.1 from Theorem 57.3.3, which rests on the comparison of trace formulas taken as given, and from facts read from the proof: finite-dimensionality under the gap hypothesis, the decomposition into joint eigenspaces, the series for the matrix coefficients of $\mathcal{R}_j(\xi; V)$, and the operators $\mathrm{av}(\gamma)$. Chapter 55 combines the corollary with Theorem 56.4.1, which writes $\hat{u}^*_{\xi,j}\hat{u}_{\xi,j}$ as a multiple of $\mathcal{R}_j(\xi; W_j)$, to express the volume of a single lift by a determinant on T (Problem 55.2.1).

In the Lean formalization. In the Lean proof [GL] (`grh/src/`, namespace `New.Data` unless written in full; EM and HE are the files `EqualMultiplicities.lean` and `HeckeEigensystems.lean` in `New/Spanning/Multiplicities/`), Theorem 57.3.3 is `trace_heckeOnGood_eq` (EM). Characteristic polynomials: `charpoly_heckeOnGood_eq`. The dimension assertion of Corollary 57.4.1 is `targetDim_eq_finrank_goodForms_spaceW`, for Y_0, W_j with $1 \le j \le m$; the multiplicity assertion specializes `finrank_goodForms_inf_eigenPart_eq`, stated for two spaces with the gap hypothesis; `rallisOnGood` restricts the Rallis operator to good forms on one, for any tame character and $j \in \mathbb{N}$, and `det_rallisOnGood_eq` equates the determinants on two, for the same character and j. All of these are in EM. Definition 57.3.1 is `New.HCParam.HasGap` for `paramW` and `gap`; the gap for Y_0, W_j is `hasGap_signsY_paramW`, `hasGap_paramW`, and finite-dimensionality the instance after `isCuspKernel_typeKernel_paramW`, in `New/UpperBound/Objects/Rows.lean`. Definition 57.3.2 uses `offLevelGroup`, `sphericalAlgebra`, `heckeAlgebra` and `heckeOperator` (HE). In HE the restriction to good forms is `heckeOnGood`, the eigenspaces are `eigenPart`, and their direct sum is given by `iSup_eigenPart_eq_top` (spanning) and `iSupIndep_eigenPart` (directness). The action of $\bar{G}$ is given by `coe_principalRep_apply` (HE) with `New.liftResidue_mem_supportedOn`, and commutation with it follows from `commute_heckeAlgebra_principalRep` (HE). The proof of `exists_hecke_proj_eigenPart` (HE) constructs the polynomial of Problem 57.4.2. At split places away from the level, `New.heckeSplit_adjoint` identifies the adjoint on principal forms with the operator at the conjugate place; these operators commute by `New.heckeSplit_comm`, which gives normality as well. The comparison of trace formulas is `New.trace_eq_of_isCuspidalAt` (`Lib/Adelic/TraceFormula/CuspidalComparison.lean`), with `New.IsLevel` and `New.IsCuspidalAt`; the reduction to it is `trace_heckeOnGood_eq_sum`, `exists_isPrimitivePolynomial` and `trace_mul_tupleIdem_eq` (EM), and the field conditions on the data follow from the instance of `New.HasPrimitiveRoot5040` for E in `New/Derivatives/Field/PrimeDecomposition.lean` and from

`f_even`. The series for $\mathcal{R}_j(\xi; V)$ is `hasSum_inner_rallisOperator` (`New/Determinant/Norms/AdjointThetaLift.lean`), its representatives and their countability `New.SiegelWeil.cosetRep` and `New.SiegelWeil.countable_quotient_localLevel`; the operators $\mathrm{av}(\gamma)$ and the common operator of Problem 57.4.5 are `exists_heckeAlgebra_inner_eq_inner_translate` and `exists_hecke_eq_rallisOperator` (EM).

Hints

§57.1.

57.1.1: $KgK = Kg \cup Kg(12)$; list the four permutations.

57.1.2: For $h \in K_g$, $g^{-1}hg \in K$ fixes y. Move δ to the other side of the inner product.

57.1.3: Write the operator as a 2×2 matrix; the traces of powers are sums of powers of its eigenvalues.

57.1.4: Take $h = 1$, then the traces of the powers of h, and Newton's identities.

57.1.6: Only finitely many λ occur on $U \oplus U'$.

§57.2.

57.2.1: Sage: the functions `BrandtModule` (with its Hecke matrices) and `EllipticCurve` (for the curve $X_0(11)$, whose traces of Frobenius are the $a_\ell(f)$). For $\ell = 2, 3$, Problems 24.4.2 and 24.4.3.

57.2.2: (b) The row sums of $B(\ell)$ and the relation between $B_{ij}(\ell)$ and $B_{ji}(\ell)$ quoted in Section 24.4; the constants are not in U_0.

57.2.3: Sage: the functions `BrandtModule` and `CuspForms`.

§57.3.

57.3.1: Problem 34.2.1 and its hint. For Y_0 the signs alternate along the entries after the semicolon. For W_j they change from $+1$ to -1 at index $k + j - 1$ if $j < m$, and all are $+1$ if $j = m$.

57.3.2: Compare components place by place; $e_0 \in \mathbb{C}[\bar{G}]$.

§57.4.

57.4.2: For each λ' choose (w, i) with $\lambda_{w,i} \neq \lambda'_{w,i}$; no commutation is needed.

57.4.3: Only finitely many eigensystems occur in $H(Y_0)$ or $H(W_j)$. Compare with Problem 57.1.6.

57.4.4: Finite-dimensional subspaces are closed.

57.4.5: Take K to be the group of integral elements of $G_f^{\mathcal{M}}$. It fixes the principal forms, and $K_\gamma := K \cap \gamma K \gamma^{-1}$ has finite index in K. For a choice of representatives of K/K_γ, the proof shows that the normalized sum of the $\delta\gamma$ in $\mathbb{C}[G_f^{\mathcal{M}}]$ is spherical; it induces the family $\mathrm{av}(\gamma)$, whose action on principal forms is the average of Problem 57.1.2. For the series, Problem 57.4.4 with the elements $\mathrm{mc}(\gamma)\,\mathrm{av}(\gamma)$.

References

[AC] J. Arthur and L. Clozel, *Simple Algebras, Base Change, and the Advanced Theory of the Trace Formula*, Ann. of Math. Stud. 120, Princeton Univ. Press, 1989.

[DS] F. Diamond and J. Shurman, *A First Course in Modular Forms*, Grad. Texts in Math. 228, Springer, 2005.

[Ei73] M. Eichler, *The basis problem for modular forms and the traces of the Hecke operators*, in *Modular Functions of One Variable I*, Lecture Notes in Math. 320, Springer, 1973, 75–151.

[GL] L. Sernau, *GRH for Dirichlet L-functions, in Lean 4*, a shorter rewriting of the Lean proof, text by Claude, `https://github.com/lsernau/grh-lean`, commit `72fead1`, readable edition `grh/`.

[HL] M. Harris and J.-P. Labesse, *Conditional base change for unitary groups*, Asian J. Math. **8** (2004), 653–683.

[JL] H. Jacquet and R. P. Langlands, *Automorphic Forms on* GL(2), Lecture Notes in Math. 114, Springer, 1970.

[Lab] J.-P. Labesse, *Changement de base CM et séries discrètes*, in *On the Stabilization of the Trace Formula*, Stab. Trace Formula Shimura Var. Arith. Appl. 1, Int. Press, 2011, 429–470.

[Mac] I. G. Macdonald, *Symmetric Functions and Hall Polynomials*, 2nd ed., Oxford University Press, 1995.

[Sage] The Sage Developers, *SageMath, the Sage Mathematics Software System*, `https://www.sagemath.org`.

THE EXCHANGE IDENTITY

Prerequisites. Tate's unfolding of the global zeta integral and its Euler product [CF, Ch. XV, §§4.4–4.5]; Poisson summation on $\mathbb{Z}^2$; for Hecke L-series see also [Neu, Ch. VII, §8]. From Chapter 34: tame characters, their weight and tame part (Section 34.6), and the partial Hecke values $L^S(z,\nu)$ (Definition 34.10.1). From Chapter 56: Problem 56.2.1; its theta integrals, and Chapter 12 (Fock models), are background only.

In the determinant of a chain (Chapter 55) each pair of lifts contributes ratios of Hecke L-values. They come from an identity $I^\sharp = c\, I^\flat$ between a theta integral over a large unitary group and one over a small group, whose scalar has $|c|^2 = C\,\mathrm{ex}_h(S,\nu)$, with $\mathrm{ex}_h(S,\nu) = (\mathrm{Nm}\, S)^{h^2} \prod_{z=1}^{h} |L^S(z,\nu)|^2$ and $C > 0$ independent of the character. Why this factor? Removing a hyperbolic plane lowers the index of the exchange factor by one, at the cost of one completed L-value, and a separate equal-rank calculation supplies the equal-rank part of the normalization. The instances are of matching, of ex_h over $\mathbb{Q}(\mathrm{i})$ and of one step; there is none of the identity itself.

58.1. Matched functions

Problem 58.1.1. Over $\mathbb{F}_3$ let χ be the quadratic character, $\Psi(a,c) := \chi$ of the first nonzero entry of (a,c), $\Psi(0,0) := 0$, and $\Phi(x,y) := \Psi(y,-x)$. Then

$$\Phi(\text{last row of } k^{-1}) = \chi(\det k)\, \Psi(\text{first column of } k)$$

for all 48 matrices $k \in \mathrm{GL}_2(\mathbb{F}_3)$, and the common value is $+1$ for 24 of them.

Problem 58.1.2. Let A be a commutative ring, $n = n^\flat + n^\sharp$, and $k \in \mathrm{GL}_n(A)$. For a set I of $n^\flat$ rows, the minor of the first $n^\flat$ columns of k on the rows I is $\pm \det k$ times the minor of the last $n^\sharp$ rows of k^{-1} on the columns not in I. The last $n^\sharp$ rows of k^{-1} times the first $n^\flat$ columns of k is 0; over a field the row span of the former and the column span of the latter are each other's annihilators.

Definition 58.1.3. Let A be a finite commutative ring, χ a character of $A^\times$, and $\sigma\colon \mathcal{B} \sqcup \mathcal{A} \to \mathcal{N}$ a bijection of finite sets (in this sheet $\mathcal{N}$, $\mathcal{A}$, $\mathcal{B}$ are coordinate sets), $\#\mathcal{B} = n^\flat$, $\#\mathcal{A} = n^\sharp$; for $k \in \mathrm{GL}_{\mathcal{N}}(A)$ write $k_{\mathcal{B}}$ for its columns indexed by $\sigma(\mathcal{B})$ and $(k^{-1})_{\mathcal{A}}$ for the rows of k^{-1} indexed by $\sigma(\mathcal{A})$. Functions Φ on $\mathcal{A} \times \mathcal{N}$ matrices and Ψ on $\mathcal{N} \times \mathcal{B}$ matrices over A are *matched* for (σ,χ) if Φ vanishes off the matrices $(k^{-1})_{\mathcal{A}}$, Ψ vanishes off the matrices $k_{\mathcal{B}}$, and $\Phi((k^{-1})_{\mathcal{A}}) = \chi(\det k)\, \Psi(k_{\mathcal{B}})$ for every $k \in \mathrm{GL}_{\mathcal{N}}(A)$.

Problem 58.1.1 gives a matched pair with $n^\flat = n^\sharp = 1$.

Date: November 26, 2026.

58.2. The two theta integrals

Let E be a CM field with a CM type and Weil data as in the proof (the field E of the data is one), υ_E (in this sheet) the splitting character of the Weil data on the ideles of E, and υ its restriction to the norm-one ideles, as in Section 34.7. For a character ν of the norm-one idele classes put $\tilde{\nu}(x) := \nu(x/\bar{x})$. As in Section 34.6, with μ in place of 0, ν has *weight* $\mu\colon \{\text{infinite places}\} \to \mathbb{Z}$ and *tame part* (ψ_w), characters of $k_w^\times$ almost all trivial, if $\nu(u) = \prod_\tau u_\tau^{\mu(\tau)} \prod_w \psi_w(u_w \bmod w)$ for every norm-one idele u with integral finite part.

Definition 58.2.1. A *modulus* is a nonzero ideal $\mathfrak{m} \subseteq \mathcal{O}_E$ such that no prime w divides $\mathfrak{m}$ together with its conjugate $\bar{w}$; $S_\mathfrak{m}$ is the set of primes dividing $\mathfrak{m}$. A character ν is *tame for* $(\mathfrak{m}, \mu, \chi)$, where χ is a character of $(\mathcal{O}_E/\mathfrak{m})^\times$, if $S_\mathfrak{m} \neq \varnothing$ and ν has weight μ and a tame part (ψ_w) with $\psi_w \neq 1$ exactly for $w \in S_\mathfrak{m}$ and $\chi(y) = \prod_{w \in S_\mathfrak{m}} \psi_w(y \bmod w)$.

Let V^0, $V^\sharp$, $V^\flat$ be framed Hermitian spaces over E (Section 34.3) on coordinate sets $\mathcal{N}$, $\mathcal{A}$, $\mathcal{B}$, of ranks n_0, $n^\sharp$, $n^\flat$, with a bijection $\sigma\colon \mathcal{B} \sqcup \mathcal{A} \to \mathcal{N}$ (so $n_0 = n^\sharp + n^\flat$). Assume: the number q_- of negative signs of V^0 is the sum of those of $V^\sharp$ and $V^\flat$; $n^\sharp = n^\flat + 2h$ with $h \in \mathbb{N}$; $2q_- + 2 \leq n_0$; and $n_0 \leq 2\mu(\tau) + 2q_-$ for every infinite place τ, for an integer-valued μ. For a Schwartz vector x of the archimedean Fock model of $(V^0, V^\sharp)$ and a function Φ on $\mathcal{A} \times \mathcal{N}$ matrices over $\mathcal{O}_E/\mathfrak{m}$, $[\Phi, x]$ is the adelic datum equal to x at the infinite places, to Φ read modulo $\mathfrak{m}$ on the matrices integral at $S_\mathfrak{m}$ (and 0 on the others) at the places of $S_\mathfrak{m}$, and to the vacuum elsewhere; likewise $[\Psi, v]$ for $(V^\flat, V^0)$. Put $\nu^0 := \nu^{-1}\upsilon^{n_0/2}$, a character for V^0; characters $\nu^\sharp$ for $V^\sharp$ and $\nu^\flat$ for $V^\flat$ are *compatible with* ν if $\tilde{\nu}^\sharp \upsilon_E^{-n^\sharp} \cdot \tilde{\nu}^\flat \upsilon_E^{-n^\flat} = \tilde{\nu}^{-1}$, equivalently $\nu^\sharp \nu^\flat = \nu^0$. The two functions of $g \in \mathrm{U}(V^0)(\mathbb{A})$ to be compared are

$$I^\sharp(g) := \int_{[\mathrm{U}(V^\sharp)]} \theta^{V^0, V^\sharp}_{\nu^0, \nu^\sharp}[\Phi, x](g, h_1)\, dh_1, \quad I^\flat(g) := \int_{[\mathrm{U}(V^\flat)]} \theta^{V^\flat, V^0}_{\nu^\flat, \nu^0}[\Psi, v](h_2, g)\, dh_2,$$

integrals of theta kernels over the quotients with their quotient measures. Theorem 58.5.1 gives, for each υ, an x making the two integrals proportional on matched data for every compatible pair of characters.

Problem 58.2.2. The last two hypotheses say $\mu(\tau) \geq n_0/2 - q_- \geq 1$ for all τ. The ranks $(n_0, n^\sharp, n^\flat; q_-) = (2,1,1;0), (4,3,1;1), (6,5,1;2)$, with all q_- negative signs in $V^\sharp$, satisfy the hypotheses for every $\mu \geq 1$, with $h = 0, 1, 2$, and $n_0/2 - q_- = 1$ each time; these successive signatures can be realized by adjoining a hyperbolic plane to V^0 and to $V^\sharp$. For $n^\flat = 0$ the smallest case with $h \geq 1$ is $(2,2,0;0)$.

For a finite set S of finite places put $\mathrm{Nm}\, S := \prod_{w \in S} q_w$, $q_w = \#k_w$. Recall (Definition 34.10.1) that for $z > 1$, $L^S(z, \nu)$ is the product of $(1 - \tilde{\nu}_w(\varpi_w) q_w^{-z})^{-1}$ over $w \notin S \cup \bar{S}$, at chosen uniformizers ϖ_w, and at $z = 1$ its limit from the right whenever that limit exists and is finite. For finite S and ν with a tame part and a weight that is not identically zero, the values $L^S(z, \nu)$, $z \geq 1$ real, are finite and nonzero: for $z > 1$ the Euler product converges absolutely, and at $z = 1$ this is Hecke's nonvanishing on the line $\mathrm{Re}\, s = 1$ [La, Ch. XV]. *Status*: classical; the proof establishes it in this form.

Definition 58.2.3. For $h \in \mathbb{N}$, and for real $z \geq 1$, whenever the partial values in the formulas exist and are finite, the *exchange factor* and the *completed value* are

$$\mathrm{ex}_h(S,\nu) := (\mathrm{Nm}\, S)^{h^2} \prod_{z'=1}^{h} |L^S(z',\nu)|^2, \qquad \hat{L}_S(z,\nu) := (\mathrm{Nm}\, S)^{z-1/2} |L^S(z,\nu)|,$$

and $\mathrm{ex}_{-h}(S,\nu) := \mathrm{ex}_h(S,\nu)^{-1}$ when this is defined.

Problem 58.2.4. $\mathrm{ex}_0(S,\nu) = 1$. For $h \in \mathbb{N}$, if the values $L^S(j,\nu)$ are finite for the integers $1 \leq j \leq h+1$ and nonzero for $1 \leq j \leq h$, then $\mathrm{ex}_{h+1}(S,\nu)/\mathrm{ex}_h(S,\nu) = \hat{L}_S(h+1,\nu)^2$.

Problem 58.2.5. Assume $L^S(j,\nu)$ is finite and nonzero for every integer $j \geq 1$. For $d \in \mathbb{Z}$ let $z_d := d+1$ if $d \geq 0$ and $z_d := -d$ if $d \leq -1$. Then $z_d \geq 1$ and $\mathrm{ex}_{d+1}/\mathrm{ex}_d = \hat{L}_S(z_d,\nu)^2$ for every $d \in \mathbb{Z}$.

58.3. The factor over $\mathbb{Q}(\mathrm{i})$

In this section only, the field is $\mathbb{Q}(\mathrm{i})$ and α runs over $\mathbb{Z}[\mathrm{i}] \smallsetminus 0$. The Hecke character with $\tilde{\nu}((\alpha)) := (\alpha/\bar{\alpha})^4$ is unramified at all finite places and trivial on the ideles of $\mathbb{Q}$, so it has the form $x \mapsto \nu(x/\bar{x})$ for a character ν of the norm-one ideles, as the notation says; its L-function is $L(z) := \frac{1}{4}\sum_\alpha \alpha^8 |\alpha|^{-2z-8}$ for real $z > 1$.

Problem 58.3.1. For $y > 0$, $F_8(y) := \sum_\alpha \alpha^8 e^{-\pi y|\alpha|^2}$ satisfies $F_8(1/y) = y^9 F_8(y)$, and with $G_s(y_0) := \int_1^\infty e^{-y_0 y} y^s \, dy/y$ for $y_0 > 0$,

$$L(z) = \frac{\pi^{z+4}}{4\,\Gamma(z+4)} \sum_\alpha \alpha^8 \big[G_{z+4}(\pi|\alpha|^2) + G_{5-z}(\pi|\alpha|^2) \big]$$

for $z > 1$; with $1/\Gamma$ read as an entire function, the right side is defined for all real z. By machine, $L(1) \approx 1.5012288658$ and $L(2) \approx 1.2576665537$.

Let $\mathfrak{p} := (3+2\mathrm{i})$, so that $a + b\mathrm{i} \equiv a + 5b \pmod{\mathfrak{p}}$ and $a - b\mathrm{i} \equiv a - 5b$, and let ψ be the cubic character of $\mathbb{F}_{13}^\times$ with $\psi(2) = e^{2\pi\mathrm{i}/3}$. The twisted character is $\tilde{\nu}'((a+b\mathrm{i})) := \tilde{\nu}((a+b\mathrm{i}))\,\psi\big((a+5b)/(a-5b)\big)$, and 0 if $13 \mid (a+5b)(a-5b)$; take $S = \{\mathfrak{p}\}$, so $\mathrm{Nm}\, S = 13$ and $L^S(z) := L^S(z,\nu') = \frac{1}{4}\sum_\alpha \tilde{\nu}'((\alpha))|\alpha|^{-2z}$ for $z > 1$.

Problem 58.3.2. $\tilde{\nu}'$ is well defined on ideals prime to 13. By machine, $|L^S(1)| \approx 3.3363841832$ and $|L^S(2)| \approx 1.4580689579$; hence $\mathrm{ex}_1 \approx 144.708972$, $\mathrm{ex}_2 \approx 675898.752$, and $\mathrm{ex}_2/\mathrm{ex}_1 = 13^3 |L^S(2)|^2 \approx 4670.745$.

Problem 58.3.3. By machine, $|L^S(z)|/|L(z)| \approx 2.2224354055$ at $z = 1$ and ≈ 1.1593446241 at $z = 2$. The two primes above 5 contribute the factor $|1 - u_5 5^{-z}|^2/|1 - u_5\psi(2)5^{-z}|^2 \approx 2.0102465324$, resp. 1.1487493619, with $u_5 := \tilde{\nu}((2+\mathrm{i}))$.

58.4. Removing a plane

In the comparisons and equal-rank ratios of this section and the next, the indexing character ν (briefly, a *character*) has the fixed weight μ of Section 58.2 and a specified tame part whose nontrivial components form a nonempty finite set S disjoint from $\bar{S}$. Here $\mu \geq 1$ everywhere, and $S = S_{\mathfrak{m}}$ for a triple of Definition 58.2.1. The kernel characters $\nu^\sharp, \nu^\flat$ range over all pairs compatible with ν. The proof has three moves, which we describe in outline; the precise vectors, standard data and normalizations are those of [GL]. Let $\mathbb{H}$ be a hyperbolic plane, $V_+^0 := \mathbb{H} \oplus V^0$, and

$(V^\flat)^-$ the space $V^\flat$ with the opposite form, as in Chapter 56. *First*, at the top the common space is $\mathbb{H}^{n^\flat} \oplus V_+^0$ and the partners are $(V^\flat)^- \oplus V_+^0$ and $(V^\flat)^-$; from prescribed Schwartz vectors the proof builds vectors for the top pairs, and unfolding central Fourier coefficients and a vanishing criterion for singular forms give a fixed real λ and, for each character, $c \in \mathbb{C}$ with $T_{\mathrm{L}} = c\,T_{\mathrm{S}}$ on standard row and column data, where $T_{\mathrm{L}}, T_{\mathrm{S}}$ are intermediate large and small theta integrals (both integrated in the partner variable), and $\lambda|c|^2 = \mathrm{ex}_{n_0/2+1}(S,\nu)\,\mathrm{er}$, er the equal-rank ratio of Section 58.5. This move is not developed here. *Second*, the proof removes $n^\flat + 1$ planes, keeping $(V^\flat)^-$ fixed. At each step it takes both constant terms along an isotropic line of the common space and uses a large partner with the prescribed signs and an adapted splitting. The index decreases by one at each step, from $n_0/2 + 1$ to h (Problems 58.4.1–58.4.4). The proof then passes to matched functions and to the adjoint model, lifts the data modulo $\mathfrak{m}$, and twists both kernels, to obtain $I^\sharp$ and $I^\flat$ for every compatible pair. *Third*, a vector with nonzero constant er is found (Section 58.5). (The letters λ, λ', λ_i, c_{pl}, C_{pl}, c_{sl}, the index d, and the spaces W, V, Y, J of this section and the next are local to this sheet.)

Problem 58.4.1. In $\mathbb{F}_9^2$ with the Hermitian form $N(u) - N(v)$, N the norm to $\mathbb{F}_3$, the average over $c \in \mathbb{F}_3$ of $e^{2\pi i c(N(u)-N(v))/3}$ is 1 at the 33 isotropic vectors of Problem 56.2.1 and 0 elsewhere. Of the 9^4 matrices $w \in M_2(\mathbb{F}_9)$, 81 satisfy $(1,1)w = 0$, and none of these is invertible; $\#\mathrm{GL}_2(\mathbb{F}_9) = 5760$.

Problem 58.4.2. Let $\mathbb{F}$ be a finite field, $\mathbf{e}$ a nontrivial additive character of $\mathbb{F}$, $y \in \mathbb{F}^{n^\flat}$ nonzero, and ℓ a linear form on functions on $M_{n^\flat \times n_0}(\mathbb{F})$ such that $\ell(f) = \ell(f_a)$, $f_a(w) := f(w)\,\mathbf{e}(y^{\mathsf{T}} w a)$, for every f and every $a \in \mathbb{F}^{n_0}$. Then $\ell(f) = 0$ for every f supported on the w with $y^{\mathsf{T}} w \neq 0$, in particular for every f supported on matrices of rank $n^\flat$.

In the proof the small constant term is a sum over rational vectors of $(V^\flat)^-$; the central average (as in Problem 58.4.1) and the vanishing of the zero term on full-rank data (as in Problem 58.4.2) leave only the index zero [GL].

Problem 58.4.3. Let E be any CM field, ν a unitary character of its norm-one idele classes, S a finite set of finite places, $z > 1$ real, and $f = \otimes_w f_w$ Schwartz–Bruhat on $\mathbb{A}_E$; the quotient measure is induced by $d^\times y$ and counting measure. Then

$$\int_{\mathbb{A}_E^\times / E^\times} \sum_{a \in E^\times} f(ay)\,\tilde{\nu}(y)|y|^z\,d^\times y = \int_{\mathbb{A}_E^\times} f(y)\,\tilde{\nu}(y)|y|^z\,d^\times y,$$

and if $\tilde{\nu}$ is unramified and $f_w = 1_{\mathcal{O}_w}$ at every finite $w \notin S \cup \bar{S}$, the finite part of the right side is $L^S(z,\nu)$ times the integrals of $f_w \tilde{\nu}_w |\cdot|^z$ at $w \in S \cup \bar{S}$ (Haar measures with $\mathrm{vol}(\mathcal{O}_w^\times) = 1$). In Problem 58.3.1, $E = \mathbb{Q}(\mathrm{i})$, $S = \varnothing$, $f_\infty(t) = t^8 e^{-\pi|t|^2}$, $f_w = 1_{\mathcal{O}_w}$, and the finite factor is $L(z)$.

On the large side the zero vector is killed by the datum and the surviving line orbit unfolds as in Problem 58.4.3. In outline, the *one-plane formula* reads as follows (the standard row and column data, built from an integral matrix at S and $\tilde{\nu}^{-1}$ of a determinant, the adapted frames and the cone vectors are specified in [GL]). Let the common space be $\mathbb{H} \oplus W$ and the large partner $\mathbb{H} \oplus V$, with adapted splittings, the small partner $(V^\flat)^-$ fixed, $\mathrm{rk}\,W = \mathrm{rk}\,V + n^\flat$ even, and $d := \mathrm{rk}\,V - \mathrm{rk}\,W/2$. There is $C_{\mathrm{pl}} > 0$ independent of the character and, for each character, $c_{\mathrm{pl}} \in \mathbb{C}$

with $|c_{\mathrm{pl}}| = C_{\mathrm{pl}}\hat{L}_S(z_d,\nu)$, z_d as in Problem 58.2.5, such that on the standard row data, for every Schwartz vector x and $g \in \mathrm{U}(W)(\mathbb{A})$, the constant term of the large integral at the Levi point $(1,g)$ is c_{pl} times the downstairs large integral at g of the cone vector of x (the dual cone if $d \le -1$, where Poisson summation precedes evaluation, so that only values of L^S at points ≥ 1 occur). On the standard column data the small constant term at $(1,g)$ is c_{sl} times the downstairs small integral of the zero slice, $c_{\mathrm{sl}} \neq 0$ a fixed vacuum factor. *Status*: for cuspidal input Rallis proves the tower property for the orthogonal–symplectic pair [Ra84, Thm. I.1.1], and Wu gives the unitary tower property [Wu, Prop. 3.1]; the proof computes the contribution of the surviving line orbit for the character and the ramified standard data [GL].

Problem 58.4.4. On the standard data of the one-plane formula, suppose $T_{\mathrm{L}} = c\,T_{\mathrm{S}}$ upstairs with $\lambda|c|^2 = \mathrm{ex}_{d+1}\,\mathrm{er}$. Then downstairs, for the cone vector and the zero slice, $T_{\mathrm{L}} = c'\,T_{\mathrm{S}}$ with $c' = c\,c_{\mathrm{sl}}/c_{\mathrm{pl}}$ and $\lambda'|c'|^2 = \mathrm{ex}_d\,\mathrm{er}$, where $\lambda' = \lambda C_{\mathrm{pl}}^2/|c_{\mathrm{sl}}|^2$ does not depend on the character (note $c_{\mathrm{pl}} \neq 0$).

58.5. The constant of equal rank

After the planes are removed, $\lambda|c|^2 = \mathrm{ex}_h(S,\nu)\,\mathrm{er}$, where the *equal-rank ratio* of a Schwartz vector v_+ for (V_+^0, V_+^0) is $\mathrm{er} = |I_+(v_+)(1)|^2/\mathrm{ex}_{n_0/2+1}$, with $I_+(v_+)$ the large theta integral of (V_+^0, V_+^0), with $\nu^{-1}\upsilon^{n_0/2+1}$ in both slots, for v_+ and the standard function equal to $\tilde{\nu}^{-1}(\det)$ on $\mathrm{GL}_{n_0+2}(\prod_{w\in S}\mathcal{O}_w)$ and 0 elsewhere. This integral is constant in the group variable, so er is a number. More generally, for an even-rank space Y the ratio for (Y,Y) uses the same construction with $\mathrm{rk}\,Y$ in place of n_0+2; for $Y = \mathbb{H}\oplus J$ with $\mathrm{rk}\,J = 2k_0$ its denominator is $\mathrm{ex}_{k_0+1}(S,\nu)$. For the rest of this section fix $k_0 \in \mathbb{N}$ with $k_0 \le \mu(\tau)$ at every infinite place. The next two facts enter the proof that a suitable v_+ has a nonzero constant ratio. *Continuation*: for a character with its set S, the values $L^S(z,\nu)$, $z \ge 1$, extend real-analytically to $(-k_0,\infty)$, nonzero at every integer $j > -k_0$; for integers $-k_0 < j \le 0$ the functional equation in absolute values relates j to $1-j \ge 1$, where the nonvanishing of Section 58.2 applies. For the classical continuation and functional equation see [CF, Ch. XV, §§4.4–4.5]. *Descent of vanishing*: let J be the standard positive definite space of rank $2k_0$; if at one character the equal-rank ratio on $\mathbb{H}\oplus J$ vanishes for every Schwartz vector, then the large integral for $(\mathbb{H}^{2k_0}\oplus\mathbb{H}\oplus J, J^-\oplus\mathbb{H}\oplus J)$ vanishes on every Schwartz vector and standard row datum, and by the continuation this descends through $2k_0+1$ planes to $(J,0)$; this is read from the proof and not developed.

Problem 58.5.1. For the twisted character of Problem 58.3.2 (ramified at $\mathfrak{p}$ and $\bar{\mathfrak{p}}$, so L^S is its full L-function), by machine the continuation has $|L^S(0)| \approx 55.2242116195$ and $|L^S(-1)| \approx 6198.83038564$.

Fix a Schwartz vector for $(\mathbb{H}\oplus J, \mathbb{H}\oplus J)$ and let er be its equal-rank ratio. Exchanging once with an empty small partner, $(V^0, V^\sharp, V^\flat) = (J,J,0)$, and once with an empty large partner, $(J,0,J)$ (a comparison of the proof with index $-k_0$, outside the range $h \ge 0$ of Section 58.2), the proof finds a Schwartz vector y for (J,J) and numbers $\lambda_1,\lambda_2 \in \mathbb{R}$, $\lambda_0 \in \mathbb{C}$ independent of the character, and for each character numbers c_1, c_2 with $\lambda_1|c_1|^2 = \mathrm{ex}_{k_0}\mathrm{er}$, $\lambda_2|c_2|^2 = \mathrm{ex}_{-k_0}\mathrm{er}$, and $c_1c_2 = \lambda_0$.

Problem 58.5.2. Under these relations $\mathrm{er}^2 = \lambda_1\lambda_2|\lambda_0|^2$, independently of the character.

Problem 58.5.3. For the pair $(J,0)$, the vacuum 1 in the one-dimensional Fock space of $\mathrm{Hom}(J,0)$ and the standard datum equal to 1 at the empty matrix, the theta integral over $[\mathrm{U}(0)]$ at $g=1$ is $\mathrm{vol}[\mathrm{U}(0)]\neq 0$. Given one character, some Schwartz vector on $\mathbb{H}\oplus J$ has nonzero equal-rank ratio at it; and some Schwartz vector has equal-rank ratio equal to one positive constant for every character (also when there is no character).

Now take $k_0 = n_0/2 - q_-$, allowed by Problem 58.2.2. Each time a plane is added the proof finds a new Schwartz vector whose ratio is a positive multiple, independent of the character, of the preceding one; after q_- steps and a transfer to the space with the signs of V^0_+ there is v_+ with $\mathrm{er} = C_0$ for every character, $C_0\neq 0$.

Problem 58.5.4. Fix this C_0 and the real coefficient λ of the comparison, both independent of $(\mathfrak{m},\nu,\chi)$, and suppose $\lambda|c|^2 = \mathrm{ex}_h(S,\nu)C_0$ for every character. If a character exists then $c\neq 0$, $\lambda\neq 0$, and $C := C_0/\lambda = |c|^2/\mathrm{ex}_h > 0$ does not depend on $(\mathfrak{m},\nu,\chi)$.

Theorem 58.5.1. *Under the hypotheses of Section 58.2, for every Schwartz vector v of the real Fock model of $(V^\flat,V^0)$ there are a real $C>0$ and a Schwartz vector x of the real Fock model of $(V^0,V^\sharp)$ such that for every modulus $\mathfrak{m}$, every character ν of the norm-one idele classes and every character χ of $(\mathcal{O}_E/\mathfrak{m})^\times$ for which ν is tame for $(\mathfrak{m},\mu,\chi)$, there is $c\in\mathbb{C}$ with*

$$|c|^2 = C\,\mathrm{ex}_h(S_{\mathfrak{m}},\nu)\neq 0$$

and $I^\sharp(g) = c\,I^\flat(g)$ for all characters $\nu^\sharp,\nu^\flat$ compatible with ν, all (Φ,Ψ) matched for (σ,χ) over $\mathcal{O}_E/\mathfrak{m}$, and all $g\in\mathrm{U}(V^0)(\mathbb{A})$.

Here x and C are chosen before $\mathfrak{m},\nu,\chi$; only c depends on them. The theorem is taken from the proof [GL]. Problems 58.2.4, 58.2.5, 58.4.4, 58.5.2, 58.5.3 and 58.5.4 give the scalar calculations, using the comparisons, the continuation, the descent of vanishing and the constructions of equal-rank vectors stated above. The proof adapts a criterion of Freitag for singular forms [Fr]; for singular forms and theta lifts see also [Li97].

Problem 58.5.5. Let S and Q be disjoint finite sets of finite places, $h\in\mathbb{N}$, and ν,ν' characters whose values $L^S(z,\nu)$ and $L^{S\cup Q}(z,\nu')$ are finite, with $L^S(z,\nu)\neq 0$, for each integer $1\le z\le h$. Then

$$\mathrm{ex}_h(S\cup Q,\nu') = \mathrm{ex}_h(S,\nu)\,(\mathrm{Nm}\,Q)^{h^2}\prod_{z=1}^{h}\frac{|L^{S\cup Q}(z,\nu')|^2}{|L^S(z,\nu)|^2}.$$

So $|c|^2 = C\prod_{j=1}^h \hat{L}_S(j,\nu)^2$: the index drops by one with each plane removed, and, when a character exists, the equal-rank value and the comparison coefficient give $C = C_0/\lambda$. Chapter 59 applies Theorem 58.5.1 to the squares of a triangle of lifts, with $S = \mathcal{M}\cup Q_\vartheta$, and uses Problem 58.5.5 to divide by the untwisted value.
In the Lean formalization. In the Lean proof [GL] (readable edition; names relative to `New`): Theorem 58.5.1 is `Exchange.exchange_identity` in `New/Determinant/Exchange/TheoremForPartners.lean`; Definitions 58.2.1 and 58.1.3 are `Modulus`, `Exchange.IsTameFor` and `AreMatched`; ex_h, ex_{-h} and $\hat{L}_S$ are `Exchange.lValueProd`, `Exchange.lValueProdInt` and `Exchange.lSharp`. In `New.Exchange`: the top comparison is `exists_rowColExchangeIdentity_sum`; the large side of the one-plane formula is

`exists_planeConstantTerm_eq_thetaLarge_cone` with its `_dualCone` variant, and plane removal is `exists_rowColExchangeIdentity_removing_plane`; the continuation is `exists_analytic_extension_ne_zero`; the equal-rank constant is `exists_equalRankThetaRatio_eq_const`. The natural-index factor `lValueProd` takes S and ν separately; `lValueProdInt` and `lSharp` take a split tame character with its ramified set.

Hints

§58.1.

58.1.1: The last row of k^{-1} is $(\det k)^{-1}(-c, a)$; χ is quadratic.

58.1.2: For $I = \{1, \dots, n^\flat\}$, replace the first $n^\flat$ rows of k^{-1} by those of the identity and multiply by k.

§58.2.

58.2.2: Use $n_0 = n^\sharp + n^\flat$ and subtract $2q_-$ from the rank bounds.

58.2.5: For $d = -j$, apply Problem 58.2.4 with $h = j - 1$.

§58.3.

58.3.1: Poisson summation ($(a + b\mathrm{i})^8$ is harmonic); split the Mellin integral at $y = 1$. By machine: mpmath's `gammainc`.

58.3.2: $\psi(-1) = 1$. By machine: as in Problem 58.3.1, with the finite Fourier transform of the character modulo 13 on the dual side.

58.3.3: $\tilde{\nu}'((2 \pm \mathrm{i}))$ are $u_5\psi(2)$ and its conjugate.

§58.4.

58.4.1: Orthogonality of the characters of $\mathbb{F}_3$; for the count, $(1, 1)w = 0$ says that the rows of w are opposite.

58.4.2: Use orthogonality in the variable a.

58.4.3: Unfold; the finite integral is a product over places.

58.4.4: Take constant terms of both sides; then Problem 58.2.5.

§58.5.

58.5.1: The split Mellin formula with the finite Fourier transform of the twist, and the entire function $1/\Gamma$.

58.5.2: Compare the factors with indices k_0 and $-k_0$.

58.5.3: $\mathrm{Hom}(J, 0) = 0$. Argue by contradiction with the descent of vanishing; then Problem 58.5.2, $\mathrm{er} \geq 0$.

58.5.4: $\mathrm{ex}_h > 0$.

58.5.5: Split the product over $S \cup Q$.

References

[CF] J. W. S. Cassels and A. Fröhlich (eds.), *Algebraic Number Theory*, Academic Press, 1967; Ch. XV is Tate's thesis (1950).

[Fr] E. Freitag, *Singular Modular Forms and Theta Relations*, Lecture Notes in Math. 1487, Springer, 1991.

[GL] L. Sernau, *GRH for Dirichlet L-functions, in Lean 4*, a shorter rewriting of the Lean proof, text by Claude, `https://github.com/lsernau/grh-lean`, commit `72fead1`, readable edition `grh/`.

[La] S. Lang, *Algebraic Number Theory*, 2nd ed., Springer, 1994.

[Li97] J.-S. Li, Automorphic forms with degenerate Fourier coefficients, *Amer. J. Math.* 119 (1997), 523–578.

[Neu] J. Neukirch, *Algebraic Number Theory*, Springer, 1999.
[Ra84] S. Rallis, On the Howe duality conjecture, *Compositio Math.* 51 (1984), 333–399.
[Wu] C. Wu, Irreducibility of theta lifting for unitary groups, *J. Number Theory* 133 (2013).

SQUARES AND THE TRIANGLE

Prerequisites. Inner products are conjugate-linear in the first argument. From Chapter 56: Theorem 56.4.1, the twist factor c_Q (Definition 56.3.1), the Rallis operators $\mathcal{R}_j(\xi; V)$ (Definition 56.3.2) and Problem 56.3.2. From Chapter 58: moduli $\mathfrak{m}$ and $S_{\mathfrak{m}}$ (Definition 58.2.1), the exchange factor $\mathrm{ex}_h(S, \nu)$ (Definition 58.2.3), Theorem 58.5.1 and Problem 58.5.5. From Chapter 34: $\mathcal{M}$, k_w, q_w, the spaces Y_j (rank $r + jt$), $H(V) \supseteq H_g(V)$, T, m-fold twists ϑ with tame part (ψ_w) and set Q_ϑ, the tame part (ω_w) of χ_M, of order q_2, the characters μ_j^0, the lower chain Θ_ϑ (Section 34.9), and $L^S(z, \nu)$ and critical pairs (Definition 34.10.1). Chapter 33 supplies $t = 5r$ and b, and Section 34.2 defines $\Delta = 2r^8$. Chapter 8 is motivation.

Theorem 55.4.1 factors $Z(\vartheta)/Z(1)$. Its input on the chain is the Gram identity of Theorem 59.4.1 below, proved in this sheet from three statements read from the proof: the realization of a triangle of lifts, the inner product formula on its first edges, and the comparison at the last level. By Theorem 56.4.1 the Gram operator of the single lift on $H(W_j)$ is $a_j c_{Q_\xi} \mathcal{R}_j(\xi; W_j)$. Why is the Gram operator of the chain on T a scalar multiple of the product of the m Rallis operators, and how do ratios of L-values enter that scalar?

59.1. Why a triangle

Problem 59.1.1. With $t = 5r$: $2r < r + t$, but $2(r + (j-1)t) > r + jt$ for every $j \geq 2$. So the condition $2n^\flat < n^\sharp$ of the inner product formula (Theorem 56.2.1) holds for the first lift $Y_0 \to Y_1$ of the chain and for no later lift $Y_{j-1} \to Y_j$.

The following identity would suffice if the Gram operators could be moved through the preceding lifts.

Problem 59.1.2. Let $\theta_j \colon \mathcal{V}_{j-1} \to \mathcal{V}_j$ $(1 \leq j \leq m)$ be linear maps of complex inner product spaces that have adjoints, and $\Theta_j := \theta_j \circ \cdots \circ \theta_1$. Suppose that $\theta_1^* \theta_1 = a_1 \mathcal{E}_1$ and that $\theta_j^* \theta_j \, \Theta_{j-1} = a_j \, \Theta_{j-1} \mathcal{E}_j$ for $2 \leq j \leq m$, with scalars a_j and endomorphisms $\mathcal{E}_j$ of $\mathcal{V}_0$. Then $\Theta_m^* \Theta_m = a_1 \cdots a_m \, \mathcal{E}_1 \mathcal{E}_2 \cdots \mathcal{E}_m$.

For $2 \leq j \leq m$ the ranks of the chain are outside the range of the inner product formula (Problem 59.1.1). The proof applies the formula only on the first edge of each row of a triangle of lifts, and relates the resulting Gram forms by two square laws.

59.2. The triangle and its two square laws

In this sheet a *triangle of size* m consists of inner product spaces $H_{i,n}$ $(i, n \geq 0$, $i + n \leq m)$; a space $H_\circ$ with linear isometric embeddings $H_\circ \to H_{i,0}$, through which we regard $H_\circ$ as a subspace of each $H_{i,0}$; linear maps $\lambda_{i,n} \colon H_{i,n} \to H_{i,n+1}$ (lifts) and $\delta_{i,n} \colon H_{i,n+1} \to H_{i+1,n}$ (descents) for $i + n < m$; and positive integer weights $g_0, g_1, \ldots$. The *weighted rows* are $\lambda_i^{(0)} := 1$ and $\lambda_i^{(n+1)} := g_n \lambda_{i,n} \lambda_i^{(n)} \colon H_{i,0} \to$

Date: November 26, 2026.

$H_{i,n+1}$. The *square* (i,n), for $i+n+2 \le m$, has corners $H_{i,n+1}$, $H_{i,n+2}$, $H_{i+1,n}$, $H_{i+1,n+1}$. We ask:

(F) for $i<m$, $x \in H_\circ$ and $v \in H_{i,1}$: $\langle v, \lambda_{i,0}x\rangle = \langle \delta_{i,0}v, x\rangle$; and $\delta_{i,0}\lambda_{i,0}$ maps $H_\circ \subseteq H_{i,0}$ injectively into $H_\circ \subseteq H_{i+1,0}$;

(D) the *direct law* at each square, with a scalar $c_{i,n}$: $g_n\lambda_{i+1,n}\delta_{i,n} = (g_{n+2}/\bar{c}_{i,n})\,\delta_{i,n+1}\lambda_{i,n+1}$ on $H_{i,n+1}$, where a quotient by 0 means 0;

(A) the *adjoint law* at each square, with a scalar $c^*_{i,n}$: every $v \in H_{i,n+2}$ has an $x \in H_{i,n+1}$ with $\langle \lambda_{i,n+1}y, v\rangle = \langle y, x\rangle$ for all y, and $\langle \delta_{i,n}x, y'\rangle = c^*_{i,n}\langle \delta_{i,n+1}v, \lambda_{i+1,n}y'\rangle$ for all $y' \in H_{i+1,n}$.

Problem 59.2.1. Let $m=2$, every $H_{i,n} = H_\circ = \mathbb{C}$ with the usual inner product and identity embeddings, $(g_0,g_1,g_2)=(2,3,5)$, and let the maps be multiplication by $\lambda_{0,0}=2$, $\lambda_{1,0}=3$, $\lambda_{0,1}=4$, $\delta_{0,0}=2$, $\delta_{1,0}=3$, $\delta_{0,1}=1$. Then (F) holds; the only square is $(0,0)$, its direct law holds exactly with $c_{0,0}=5/3$, and its adjoint law exactly with $c^*_{0,0}=8/3$.

Problem 59.2.2. In Problem 59.2.1, $\lambda_0^{(2)} = g_1\lambda_{0,1}g_0\lambda_{0,0} = 48$, and $48^2 = 2304 = c_{0,0}c^*_{0,0}\,(g_0g_1^2/g_2)\,(g_0\lambda_{0,0}^2)(g_0\lambda_{1,0}^2)$.

In Problems 59.2.3–59.2.6 the triangle is arbitrary and satisfies (F), (D), (A). For $i+n<m$ put $c_i^{[n]} := c_{i,0}c_{i,1}\cdots c_{i,n-1}$ and $c_i^{*[n]} := c^*_{i,0}\cdots c^*_{i,n-1}$ (empty products are 1); Problems 59.2.3, 59.2.5 and 59.2.6 assume $i+n<m$.

Problem 59.2.3. $\lambda_{i+1}^{(n)}\delta_{i,0}\lambda_{i,0} = \dfrac{g_{n+1}}{g_1g_0\,\overline{c_i^{[n]}}}\,\delta_{i,n}\lambda_i^{(n+1)}$ on $H_{i,0}$.

Problem 59.2.4. For $i+n\le m$, $\lambda_i^{(n)}$ is injective on $H_\circ$. If $H_\circ \ne 0$ and $i+n<m$, then $c_i^{[n]} \ne 0$.

Problem 59.2.5. For $x \in H_\circ$ and $v \in H_{i,n+1}$: $\langle v, \lambda_{i,n}\lambda_i^{(n)}x\rangle = c_i^{*[n]}\,\langle \delta_{i,n}v, \lambda_{i+1}^{(n)}x\rangle$.

Problem 59.2.6. For $x,y \in H_\circ$ and $x' := \delta_{i,0}\lambda_{i,0}x \in H_\circ$: $\langle \lambda_i^{(n+1)}x, \lambda_i^{(n+1)}y\rangle = c_i^{[n]}c_i^{*[n]}\,\dfrac{g_0g_1g_n}{g_{n+1}}\,\langle \lambda_{i+1}^{(n)}x', \lambda_{i+1}^{(n)}y\rangle$.

In the chain, $H_{i,n}$ consists of forms on a Hermitian space of rank $r+nt$ whose parameter has n blocks of length t, labelled $i+1,\dots,i+n$. In row 0 these spaces are $Y_0,\dots,Y_m$; the first space of row i is Y_0 with its form multiplied by $(-1)^i$. On labels, the lift $\lambda_{i,n}$ adds block $i+n+1$ and the descent $\delta_{i,n}$ removes block $i+1$. So the square (i,n) removes block $i+1$ and adds block $i+n+2$; we say it carries the pair $(i+1, i+n+2)$.

Problem 59.2.7. As (i,n) runs over the squares of a triangle of size m, the pair $(i+1, i+n+2)$ runs over the pairs $1 \le i' < j' \le m$, each once; there are $m(m-1)/2$ squares. For $m=3$ the squares $(0,0),(0,1),(1,0)$ carry $(1,2),(1,3),(2,3)$.

59.3. The triangle of the chain and its scalars

For an m-fold twist ϑ let $\mathfrak{m} := (\pi_M)\prod_{w\in Q_\vartheta} w$, so $S_\mathfrak{m} = \mathcal{M}\cup Q_\vartheta$, and in this sheet $\mathfrak{R} := \mathcal{O}_E/\mathfrak{m}$, both depending on ϑ; $\mathfrak{R} \cong \prod_{w\in\mathcal{M}\cup Q_\vartheta} k_w$, as p_0, p_1 split completely in E and $\operatorname{Nm} Q_\vartheta$ is prime to M. In the triangle of the chain, $H_\circ = H(Y_0)$, the node $H_{i,n}$ is a space of forms on a space of rank $r+nt$, row 0 runs through $Y_0,\dots,Y_m$, the lift $\lambda_{i,n}$ is a theta lift built from the character $\mu^0_{i+n+1}\vartheta^{i+n+1}$ (times a power of

the splitting character υ, depending on the ranks) with the indicator of $\binom{1}{0}$ modulo $\mathfrak{m}$ as finite datum, and $g_n(\vartheta) := \#\mathrm{GL}_{r+nt}(\mathfrak{R})$. The descents are transposed theta lifts; in each row the proof chooses their polynomials at infinity and the finite datum of $\delta_{i,0}$ so that $\delta_{i,0}$ is adjoint to $\lambda_{i,0}$ on $H_\circ$. For a function p on matrices η of a fixed shape over $\mathfrak{R}$, the *next datum* is the function on the matrices with one more block of rows and of columns, of size t, that equals $p(-\eta)$, divided by the number of possible blocks η', at $\left(\begin{smallmatrix}\eta & \eta'\\ 0 & 1\end{smallmatrix}\right)$, and 0 at all other matrices; the finite datum of $\delta_{i,n+1}$ is the next datum of that of $\delta_{i,n}$.

Realization of the triangle. The proof shows (F), and (D), (A) at each square with functions $c_{i,n}$, $c^*_{i,n}$ of the m-fold twist, as follows. Theorem 58.5.1, on the sum of the two middle Hermitian spaces, gives a finite square law for the two composites around the square on point data; a finite summation turns it into (D) for a datum and its next datum, with $|c_{i,n}(\vartheta)|^2 = C_{i,n}\,\mathrm{ex}_t(\mathcal{M}\cup Q_\vartheta, \nu_{i,n}(\vartheta))$, $C_{i,n}\in\mathbb{R}$ independent of ϑ and $\nu_{i,n}(\vartheta)$ as in Problem 59.3.2. The proof also provides the adjoint vectors in (A), with $c^*_{i,n}\doteq 1$ in the sense of Definition 59.3.1; one of its factors is the scalar of the reversed square, which combines an exchange with partners of equal rank with the inverse of the Fourier constant of Problem 59.3.5. *Status*: read from the proof. For joint harmonics see [Li90, Ho89], for the seesaw principle [Ku84].

Definition 59.3.1. For functions c from m-fold twists to $\mathbb{C}$ and f to $\mathbb{R}$, $c\doteq f$ means: there are $C'\in\mathbb{R}$ (possibly 0) and $e'\in\mathbb{Z}$ with $|c(\vartheta)|^2 = C'(\mathrm{Nm}\,Q_\vartheta)^{e'} f(\vartheta)^2$ for every m-fold twist ϑ.

The relation $c\doteq f$ allows c to vanish identically; if c is nonzero at one twist, its zeros are exactly those of f.

Definition 59.3.2. For $1\le i<j\le m$, $\nu := \mu^0_j/\mu^0_i$ and an m-fold twist ϑ,

$$\rho_{ij}(\vartheta) := \prod_{z=1}^{t} \frac{|L^{\mathcal{M}\cup Q_\vartheta}\big(z,(\nu\vartheta^{j-i})^{-1}\big)|}{|L^{\mathcal{M}}(z,\nu^{-1})|},$$

a quotient by 0 being 0.

The values $L^S(z,\nu)$ in Definition 59.3.2 and in the exchange factors below are finite and nonzero, by the nonvanishing stated in Chapter 58, Section 58.2: the characters have weight $\pm(j-i)\Delta\neq 0$ and a tame part (Problems 59.3.2 and 59.4.6).

Problem 59.3.1. In the square (i,n) the Hermitian spaces underlying the middle corners $H_{i,n+1}$, $H_{i+1,n+1}$ have rank $r+(n+1)t$ each, and those underlying the partners $H_{i,n+2}$, $H_{i+1,n}$ have ranks $r+(n+2)t$ and $r+nt$. So in Theorem 58.5.1, with V^0 the orthogonal sum of the two middle Hermitian spaces, $n_0 = 2(r+(n+1)t)$ and $h=t$. In the reversed square the partners are the spaces underlying $H_{i,n+1}$, $H_{i+1,n+1}$, of equal rank, so $h=0$ and $\mathrm{ex}_0=1$.

For the data, $8m\le 16\sqrt{x} < x^{11}\le T(s)\le q_1 d$ (Definition 33.3.1, Problem 33.3.3) and $q_1 d \mid q_2$ (Chapter 33).

Problem 59.3.2. Let $\nu_{i,n}(\vartheta) := \big((\mu^0_{i+n+2}/\mu^0_{i+1})\vartheta^{n+1}\big)^{-1}$. It has weight $(n+1)\Delta$; moreover $(n+1)\Delta\ge r+(n+1)t$ and $n_0\le 2(n+1)\Delta$. Its tame part is $\omega_w^{-(n+1)}$ at $w\in\mathcal{M}$, $\psi_w^{-(n+1)}$ at $w\in Q_\vartheta$, trivial elsewhere, and nontrivial at every $w\in\mathcal{M}\cup Q_\vartheta$.

Problem 59.3.3. If $c\doteq f$ and $c'\doteq f'$, then $cc'\doteq ff'$. For every square, $c_{i,n}\doteq \rho_{i+1,\,i+n+2}$, with exponent $e'=t^2$, and $c^*_{i,n}\doteq 1$.

The powers of $\#\mathfrak{R}$ in the adjoint law come from finite Fourier transforms $\hat{F}(\mathbf{v}') := \sum_{\mathbf{v}} F(\mathbf{v})\,\mathbf{e}(\mathrm{tr}(\mathbf{v}'\mathbf{v}))$, with $\mathbf{e}$ a primitive additive character of $\mathfrak{R}$. For $\mathfrak{R} = \prod_w k_w$, with primitive characters $\mathbf{e}$ (additive) and χ (multiplicative, 0 on nonunits: every $a \neq 0$ has some $\chi(1+ca) \notin \{0,1\}$) there is $G \in \mathbb{C}$ with $|G|^2 = \#\mathfrak{R}^{t^2}$ such that every function F on $t \times t$ matrices with $F(k\mathbf{v}) = \chi(\det k)F(\mathbf{v})$ for invertible k has $\hat{F}(\mathbf{v}') = G\,\chi^{-1}(\det \mathbf{v}')\,F(1)$, with χ^{-1} also extended by 0. *Status*: for the Gauss sum of a determinant character over a finite field see [Ko63]; for $\mathfrak{R} = \prod_w k_w$ such an F vanishes off the invertible matrices and is a product over w, so the identity follows from the case of fields. At a node of rank $r + nt$ the Fourier identity for the conjugated data has constant $G \cdot \#\mathfrak{R}^{(r+nt)t}$: G from a corner block of size t, and $\#\mathfrak{R}^{(r+nt)t}$ from the sum over a free block of size $(r + nt) \times t$; the reversed square uses its inverse (in the proof of (A)).

Problem 59.3.4. Take the added block of size 1. Over $\mathfrak{R} = \mathbb{F}_3$, with p the indicator of $\{1\}$ on 1×1 matrices, the next datum is $1/3$ at the three matrices $\left(\begin{smallmatrix} -1 & \eta' \\ 0 & 1 \end{smallmatrix}\right)$ ($\eta' \in \mathbb{F}_3$) and 0 elsewhere. With $\mathbf{e}(x) = e^{2\pi i x/3}$, its Fourier transform at $\left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right)$ is $1_{C=0}\,\mathbf{e}(-A + D)$.

Problem 59.3.5. For $\mathbf{e}$ as in Problem 59.3.4 and the nontrivial character χ of $\mathbb{F}_3^\times$, the Gauss sum $\sum_{x \in \mathbb{F}_3^\times} \chi(x)\,\mathbf{e}(x)$ is $i\sqrt{3}$. In general $|G \cdot \#\mathfrak{R}^{(r+nt)t}|^2 = \#\mathfrak{R}^{t(t+2(r+nt))}$; formally, for $\mathfrak{R} = \mathbb{F}_3$ and $r + nt = t = 1$, this is $|3i\sqrt{3}|^2 = 27$.

Problem 59.3.6. Over $\mathbb{F}_q$, the invertible block upper triangular matrices with diagonal blocks of sizes $r, t, \ldots, t$ (j blocks t) form a group of order $\#\mathrm{GL}_r(\mathbb{F}_q)\,\#\mathrm{GL}_t(\mathbb{F}_q)^j\,q^{jrt+t^2 j(j-1)/2}$. For blocks $(1,2)$ over $\mathbb{F}_2$ the order is 24; for $r = 1$, $t = 5$ the exponent is $5, 35, 90$ for $j = 1, 2, 3$.

59.4. The Gram identity of the chain

Definition 59.4.1. For an m-fold twist ϑ, let $\mathcal{R}_\vartheta$ be the endomorphism of T

$$\mathcal{R}_\vartheta := \mathcal{R}_1(\vartheta; Y_0)\,\mathcal{R}_2(\vartheta^2; Y_0) \cdots \mathcal{R}_m(\vartheta^m; Y_0).$$

Each factor preserves T (Corollary 57.4.1). In this sheet $c_{\mathrm{mat}}(\vartheta) := \#\mathfrak{R}^{r(r+t)}$, the number of $(r + t) \times r$ matrices over $\mathfrak{R}$. The inner product formula on the first lift of each row (Problem 59.1.1), with the point datum, gives: for $i < m$ there is $C_i \in \mathbb{C}$, independent of ϑ, with

$$g_0\,\langle \lambda_{i,0}x, \lambda_{i,0}y\rangle = \frac{C_i}{c_{\mathrm{mat}}(\vartheta)}\,\langle x, \mathcal{R}_{i+1}(\vartheta^{i+1}; Y_0)\,y\rangle \qquad (x \in H(Y_0),\ y \in T).$$

Status: read from the proof.

Problem 59.4.1. In a triangle of size m with (F), (D), (A), let $T' \subseteq H_\circ$ be a subspace, $\mathcal{E}_i$ endomorphisms of T' and C_i scalars with $g_0\langle \lambda_{i,0}x, \lambda_{i,0}y\rangle = C_i\langle x, \mathcal{E}_i y\rangle$ for $i < m$, $x \in H_\circ$, $y \in T'$. Then for $i + n = m$, $x \in H_\circ$ and $y \in T'$

$$\langle \lambda_i^{(n)}x, \lambda_i^{(n)}y\rangle = c_{(i)}\,\frac{g_0 g_1^n}{g_n}\,\langle x, \mathcal{E}_i\mathcal{E}_{i+1}\cdots\mathcal{E}_{m-1}\,y\rangle,$$

where $c_{(i)}$ is the product of $C_i, \ldots, C_{m-1}$ and of all $c_{i',n'}c^*_{i',n'}$ with $i' \geq i$.

Problem 59.4.2. For the triangle of the chain there is $c_\triangle \doteq \prod_{1 \leq i < j \leq m} \rho_{ij}$ with

$$\langle \lambda_0^{(m)}x, \lambda_0^{(m)}y\rangle = c_\triangle(\vartheta)\,\frac{g_0 g_1^m}{g_m\,c_{\mathrm{mat}}^m}\,\langle x, \mathcal{R}_\vartheta y\rangle \qquad (x \in H(Y_0),\ y \in T).$$

On $H(Y_0)$ we write Θ_ϑ for the lower chain with values in algebraic forms on Y_m, and on T for its restriction, as in Chapter 34. Its target consists of algebraic forms of the prescribed weight on Y_m that transform under a level, written $K_{\mathrm{last}}(\vartheta)$ in this sheet, by a character determined by ϑ. The group $K_{\mathrm{last}}(\vartheta)$ consists of the elements of the group $K^\circ(Y_m)$ of integral finite adelic unitary matrices of Y_m that reduce to 1 at each $w \in \mathcal{M}$ and to a block upper triangular matrix, with blocks $r, t, \dots, t$, at each $w \in Q_\vartheta$. The proof shows $[K^\circ(Y_m) : K_{\mathrm{last}}(\vartheta)] = \prod_{w\in\mathcal{M}} \#\mathrm{GL}_{r+mt}(k_w) \prod_{w\in Q_\vartheta} [\mathrm{GL}_{r+mt}(k_w) : \mathrm{Par}_w]$, with Par_w the group of Problem 59.3.6 over k_w, and that for $x, y \in H(Y_0)$

$$\langle \Theta_\vartheta x, \Theta_\vartheta y\rangle = c_{\mathrm{wt}}\, [K^\circ(Y_m) : K_{\mathrm{last}}(\vartheta)]\, \langle \lambda_0^{(m)} x, \lambda_0^{(m)} y\rangle,$$

with c_{wt} a positive integer independent of ϑ. *Status*: read from the proof.

Problem 59.4.3. Θ_ϑ is injective on $H(Y_0)$, in particular on T.

Problem 59.4.4. For every m-fold twist ϑ,

$$[K^\circ(Y_m) : K_{\mathrm{last}}(\vartheta)]\, \frac{g_0 g_1^m}{g_m} = \big(c_{\mathrm{mat}}(\vartheta)\, c_{Q_\vartheta}\big)^m\, (\mathrm{Nm}\, Q_\vartheta)^{-mrt - t^2 m(m-1)/2}$$

times a positive number independent of ϑ.

Problem 59.4.5. There is c with $c \doteq \prod_{1\le i<j\le m} \rho_{ij}$ and $\langle \Theta_\vartheta x, \Theta_\vartheta y\rangle = c(\vartheta)\, c_{Q_\vartheta}^m\, \langle x, \mathcal{R}_\vartheta y\rangle$ for all m-fold twists ϑ and $x, y \in T$.

Problems 59.2.3–59.2.7, 59.3.3 and 59.4.1–59.4.5, with the realization of the triangle, the first-edge identity and the description of the last level, prove the following.

Theorem 59.4.1. *There is a function c from m-fold twists to $\mathbb{C}$ with $c \doteq \prod_{1\le i<j\le m} \rho_{ij}$ such that for every m-fold twist ϑ and all $x, y \in T$,*

$$\langle \Theta_\vartheta x, \Theta_\vartheta y\rangle = c(\vartheta)\, c_{Q_\vartheta}^m\, \langle x, \mathcal{R}_\vartheta y\rangle.$$

The data satisfy $t \le \Delta$ and $m\Delta \le 4b$ (as $m\Delta \le 4\sqrt{x}\,(3x^5)^8 < x_1 < b$ by Definition 33.3.1).

Problem 59.4.6. $\rho_{ij}(1) = 1$. The character μ_j^0/μ_i^0 has weight $-(j-i)\Delta$, with $t \le (j-i)\Delta \le 4b$, and tame part (ω_w^{j-i}), nontrivial exactly at the $w \in \mathcal{M}$; so each $P_z := (\mu_j^0/\mu_i^0, z)$, $1 \le z \le t$, is a ramified critical pair (Definition 34.10.1), and $\rho_{ij}(\vartheta) = \prod_{z=1}^t R_{P_z}(\vartheta^{j-i}, 1)$.

Problem 59.4.6 identifies the unprimed ratios of Problem 55.5.1; Theorem 55.5.2, used in Chapter 54, bounds for a family with small ratios the height of the inverses of $(\mathrm{Nm}\, Q_{\theta_\iota})^{e/2} \prod_{i<j} \rho_{ij}(\theta_\iota)$, every $e \in \mathbb{Z}$. We have proved Theorem 59.4.1 from three statements read from the proof; the exchange identity enters through the square laws. Chapter 55 uses it to factor $Z(\vartheta)/Z(1)$.

In the Lean formalization. In the Lean proof [GL] (`grh/src/New/Determinant/Chain/`), Theorem 59.4.1 is `New.Data.exists_inner_chain_eq`; ρ_{ij}, $\mathcal{R}_\vartheta$, $\doteq$ are `quotientRatio`, `rallisProduct`, `HasAbsUpToNormPower` (for the indices used here). The realization is `exists_isTriangle` (flag `false`), using `exists_triangleLift_triangleTransposedLift_comm` for (D) and `exists_triangleTransposedLift_adjoint_comm` for the identity in (A). The first-edge identity is a step in the proof of `exists_inner_weightedChain_eq`. The comparison at the last level is `inner_lowerChainAtLevel`, and the product formula for the index of $K_{\mathrm{last}}(\vartheta)$ is `stdLevelIndex_lastLevel_eq_prod`, both in `ChainNorms.lean`.

Hints

59.2.4: For injectivity, induction on n, passing a kernel vector to row $i+1$ by Problem 59.2.3 and (F). For $c_i^{[n]} \neq 0$, take a nonzero vector of $H_\circ$; a quotient by 0 is 0.

59.2.5: Induction on n; for the step use (A).

59.2.6: Problem 59.2.5 with $v = \lambda_i^{(n+1)} x$, then Problem 59.2.3 for $\lambda_{i+1}^{(n)} x'$.

59.3.2: The weights κ_j of Chapter 34 increase by Δ. For the rank bound use $r \geq 3$, $t = 5r$, $\Delta = 2r^8$; for nontriviality use $0 < n+1 \leq m < q_2$ and the m-fold condition.

59.3.3: Problem 58.5.5 with $S = \mathcal{M}$, $Q = Q_\vartheta$, $h = t$; the untwisted value $\mathrm{ex}_t(\mathcal{M}, \nu_{i,n}(1))$ is a constant. Note $\#\mathfrak{R} = \mathrm{Nm}\, Q_\vartheta \prod_{w \in \mathcal{M}} q_w$.

59.4.1: Induction on n from row $i+1$ to row i, with Problem 59.2.6, and (F) to apply the first-edge relation to x and $\mathcal{E}_{i+1} \cdots \mathcal{E}_{m-1} y$.

59.4.2: Problem 59.4.1 with $\mathcal{E}_i = \mathcal{R}_{i+1}(\vartheta^{i+1}; Y_0)/c_{\mathrm{mat}}$, and Problems 59.2.7 and 59.3.3.

59.4.4: Factor over $w \in \mathcal{M} \cup Q_\vartheta$; at $w \in Q_\vartheta$ use Problem 59.3.6, the stabilizer of an injective $(r+t) \times r$ matrix, and Problem 56.3.2.

59.4.5: Problems 59.4.2 and 59.4.4; for $A \in \mathbb{C}$ and $k \in \mathbb{Z}$, $\vartheta \mapsto A(\mathrm{Nm}\, Q_\vartheta)^k$ satisfies $\doteq 1$.

References

[GL] L. Sernau, *GRH for Dirichlet L-functions, in Lean 4*, a shorter rewriting of the Lean proof, text by Claude, `https://github.com/lsernau/grh-lean`, commit `72fead1`, readable edition `grh/`.

[Ho89] R. Howe, *Transcending classical invariant theory*, J. Amer. Math. Soc. **2** (1989), 535–552.

[Ko63] T. Kondo, *On Gaussian sums attached to the general linear groups over finite fields*, J. Math. Soc. Japan **15** (1963), 244–255.

[Ku84] S. S. Kudla, *Seesaw dual reductive pairs*, in: Automorphic Forms of Several Variables (Katata, 1983), Progr. Math. **46**, Birkhäuser, 1984, 244–268.

[Li90] J.-S. Li, *Theta lifting for unitary representations with nonzero cohomology*, Duke Math. J. **61** (1990), 913–937.

THE COST OF ONE LIFT

Prerequisites. From Chapter 5: heights of families (Section 5.3, Problem 5.3.2). From Chapter 6: sizes read at the trivial twist, valuations at a twist that depends on the prime. The data of Chapter 33 and the objects of Chapter 34. The factorization of Chapter 55. The statements of Chapters 61, 62 and 64 recalled in Section 60.1.

Chapter 55 reduces the Gram determinant of the chain to the determinants $Z_j(\vartheta)$ of single lifts, where for an m-fold twist ϑ the j-th lift is taken at the twist ϑ^j. The proof needs a bound for the height of $Z_j(1)/Z_j(\vartheta)$ when ϑ varies with the prime ℓ and with an isomorphism $\iota \mid \ell$. How does the proof bound the ratio without evaluating either determinant? It multiplies the Gram determinant at a twist by the determinant of the compression of a second operator to the image of the lift, chosen so that the product is a fixed constant times a power of a ratio of Hecke values. The compression determinant is bounded under the automorphisms of $\mathbb{C}$ at the trivial twist only, and at ℓ at the twist (Chapter 61). The ratio of Hecke values is a product of ratios attached to critical pairs (Chapter 62), and for a regular family the inverses of these ratios have bounded height (Chapters 63 and 64). This chapter states the inputs and deduces Theorem 60.2.1 from them. One input, Theorem 60.1.1, is read from the code; the others are proved in the four chapters just named, up to the background each of them lists.

60.1. The inputs

We use the data of Chapter 33: the number f of infinite places, the scales $x < x_1 < b$ and $a = xb$, the number m of lifts, the ranks r and k, the direction amount h_{dir} and the denominator budget $B = U/(mk) = fa\log^3 b/(mk)$ (Definition 33.4.1); and the objects of Chapter 34: twists ϑ and m-fold twists, with modulus Q_ϑ and $\operatorname{Nm} Q_\vartheta$, the target dimension d_T, the single lifts $u_{\vartheta,j}$, and $Z_j(\vartheta) = \det(u^*_{\vartheta^j,j} u_{\vartheta^j,j})$ for an m-fold twist ϑ.

Fix $1 \le j \le m$. The Hecke value product $\mathcal{H}_j(\vartheta)$ of lift j at a twist ϑ is that of Definition 61.3.1. Comparison operators (Υ_ϑ), one operator on the target space of $u_{\vartheta,j}$ for every twist ϑ, are defined in Definition 61.3.3, their compression determinants D_ϑ in (1), and the statement that a real $\mathrm{cl}(\ell)$ clears the projection at (ι, ϑ, j) in Definition 61.3.4. A family $\theta = (\theta_\iota)$ of m-fold twists, one for each prime ℓ and each $\iota \mid \ell$, is regular if it satisfies clauses (i) and (ii) of Definition 64.2.2 and clause (iii) of Definition 64.2.3. Chapter 65 treats the denominators in (iii), and Chapter 67 the existence of regular families.

Theorem 60.1.1. *For every $1 \le j \le m$ the operators $\Upsilon_\vartheta := \mathcal{N} h^2\, g_\vartheta g_\vartheta^*$, one for each twist ϑ, form a comparison operator. Here g_ϑ is a gluing map from tuples of forms on a smaller definite space to the target space of $u_{\vartheta,j}$, h is the hook number of the diagram of the weight of those forms, and $\mathcal{N}$ is the order of Section 34.1, a common multiple of the orders of the stabilizers at the levels used.*

Date: November 26, 2026.

This theorem is read from the code and is not proved in this workbook. For clause (1) of Definition 61.3.3 the proof uses $\mathcal{H}_j(\vartheta)/\mathcal{H}_j(1) = |c_1'|^2/|c_\vartheta'|^2$, with $c_\vartheta' \neq 0$ for every twist. For (2) it also uses $g_\vartheta^* u_{\vartheta,j} = (c_\vartheta')^{-1} u^\circ$, with u° injective and independent of ϑ, as in Problem 61.1.3. For (4) and (5) it writes Υ_ϑ as a sum of operators of rank at most one over a tight frame of tuples.

Three statements are recalled. By Theorem 61.3.1, for every comparison operator every D_ϑ is nonzero,

$$|\iota(D_\vartheta)|_\ell \le e^{d_T r\,\mathrm{cl}(\ell)} \qquad \text{and} \qquad |\sigma(D_1)| \le e^{3d_T f m b \log^2 b},$$

the first for every twist ϑ, every $\iota \mid \ell$ with ℓ prime to $\operatorname{Nm} Q_\vartheta$ and every real $\mathrm{cl}(\ell)$ that clears the projection at (ι, ϑ, j), the second for every $\sigma \in \mathrm{Aut}(\mathbb{C})$; and by Problem 61.3.2, for every m-fold twist ϑ,

$$\frac{Z_j(1)}{Z_j(\vartheta)} = \frac{D_{\vartheta^j}}{D_1}\Big(\frac{\mathcal{H}_j(\vartheta^j)}{\mathcal{H}_j(1)}\Big)^{-d_T}.$$

By Problem 62.5.1, for every twist ϑ the quotient $\mathcal{H}_j(\vartheta)/\mathcal{H}_j(1)$ is a power of $\operatorname{Nm} Q_\vartheta$ times the square of a product of $k/2 + 5m$ ratios $R_P(\vartheta, \epsilon)$ of ramified critical pairs P (Definition 34.10.1), of which $k/2$ are main for j (Definition 62.4.1) and have $\epsilon = 1$. By Theorem 64.4.1, for a regular family θ and a critical pair P main for j, the family $\iota \mapsto R_P(\theta_\iota^j)^{-1}$ has height at most $6B - h_{\mathrm{dir}}$.

60.2. The deduction

Let θ be regular and $1 \le j \le m$, let (Υ_ϑ) be the comparison operator of Theorem 60.1.1, and write $\vartheta_\iota := \theta_\iota^j$.

Problem 60.2.1. The family $\iota \mapsto D_{\vartheta_\iota}/D_1$ has height at most $d_T(3fmb\log^2 b + rB)$.

Problem 60.2.2. The family $\iota \mapsto \big(\mathcal{H}_j(\vartheta_\iota)/\mathcal{H}_j(1)\big)^{-1}$ has height at most $10mx_1 + k(6B - h_{\mathrm{dir}})$.

It remains to compare the constants. The following inequality is derived here from the sizes of the data.

Problem 60.2.3. Let $f \ge 1$, $b > 1$ with $\log b \ge 16$, $x \ge 1$, $\sqrt{x} \le m \le 2\sqrt{x}$, $r \ge 2m$, $k = r + 1 - m$, $1 \le x_1 \le b$, $a = xb$ and $B = fa\log^3 b/(mk)$. Then for every real h_{dir}

$$3fmb\log^2 b + rB + 10mx_1 + k(6B - h_{\mathrm{dir}}) \le k(B\log b - h_{\mathrm{dir}}).$$

The data satisfy these hypotheses.

Problems 60.2.1, 60.2.2, 61.3.2, 64.1.2 and 60.2.3, with Problem 5.3.2, prove the following.

Theorem 60.2.1. *For the data, every regular family θ of m-fold twists, and every $1 \le j \le m$, the family*

$$\iota \longmapsto \frac{Z_j(1)}{Z_j(\theta_\iota)}$$

has height at most $d_T\, k\,(B\log b - h_{\mathrm{dir}})$.

Problem 60.2.4. For the data, $B\log b < h_{\mathrm{dir}}$. So the bound of Theorem 60.2.1 is $-d_T k(h_{\mathrm{dir}} - B\log b)$ with $h_{\mathrm{dir}} - B\log b > 0$.

So the bound of Theorem 60.2.1 is, per unit of d_T, k times the budget $B \log b$ less k times the direction amount. Chapter 54 combines these bounds for $1 \le j \le m$ with the factorization of Chapter 55 and the height bound there for its correction factor. Of the inputs, Theorem 60.1.1 is read from the code; Chapters 61, 62, 63 and 64 prove the others.

In the Lean formalization. In the Lean proof [GL], in the readable edition: Theorem 60.2.1 is `Data.heightLe_liftDeterminant_ratio` and Theorem 60.1.1 is `Data.isComparisonOperator_comparisonOp`, both in `New/OneLift/LiftVolumeHeight.lean`; comparison operators are `Data.IsComparisonOperator`, and the budget B is `Data.denominatorBudget`. The declarations behind the recalled statements are named in Chapters 61, 62 and 64.

Hints

60.2.1: Problem 64.1.1 with $H = D_1$, which is nonzero; the two bounds recalled from Theorem 61.3.1; and the reals $\mathrm{cl}(\ell)$ of clause (iii) of Definition 64.2.3, whose sums are at most B.

60.2.2: Problem 62.5.1 and Theorem 64.4.1 for the $k/2$ main pairs, clause (ii) of Definition 64.2.2 for the $5m$ others, Problems 5.3.2 and 64.1.2; by (i), $\mathrm{Nm}\, Q_{\vartheta_\iota}$ is a unit at ℓ.

60.2.3: The terms in h_{dir} cancel. Compare everything with $kB = fxb \log^3 b/m \ge fmb \log^3 b/4$, and use $r \le 2k$. For the data, use the inequalities between m, r, x, x_1 and b in Chapter 33.

60.2.4: $h_{\mathrm{dir}} \ge b \#\Phi_a$ (Problem 33.4.5), $f = \#\Phi_a\, \varphi(q_0)$ (Problem 33.2.2); compare $\varphi(q_0)\, x \log^4 b$ with mk.

References

[GL] L. Sernau, *GRH for Dirichlet L-functions, in Lean 4*, a shorter rewriting of the Lean proof, text by Claude, `https://github.com/lsernau/grh-lean`, commit `72fead1`, readable edition `grh/`.

COMPRESSIONS AND FALSE LIFTS

Prerequisites. Linear algebra over $\mathbb{C}$: adjoints, orthogonal projections, determinants as products of eigenvalues. The fields $\bar{\mathbb{Q}}_\ell$ and $\mathbb{C}_\ell$, with $|\ell|_\ell = 1/\ell$. Inner products are conjugate-linear in the first variable. From Chapter 29: congruence modules, Problems 29.1.1 and 29.1.2. From Chapter 23: theta lifts between definite spaces and their norms (Theorem 23.3.1). From Chapter 5: isomorphisms $\iota \mid \ell$ and heights of families (Section 5.3); from Chapter 6, Theorem 6.2.1, which needs a height bound for $Z(1)/Z(\theta_\iota)$. For Section 61.3 only: the data (Chapter 33) and the spaces, forms, twists and single lifts of Chapter 34; the gauge and forms integral at a ring map η of Section 48.3; the exchange factors of Chapter 58; Chapters 56 and 57 for two facts recalled there; and Theorem 24.2.1 as a model of a Hecke relation.

This sheet serves Theorem 60.2.1 of Chapter 60, *The cost of one lift*: for a regular family (θ_ι) of m-fold twists (Definition 64.2.3), a bound for the height of $\iota \mapsto Z_j(1)/Z_j(\theta_\iota)$, where $Z_j(\theta_\iota)$ is the Gram determinant of the j-th single lift at the twist θ_ι^j. How can the ratio be bounded without evaluating either determinant? The Gram determinant at a twist, times the determinant of the compression of a second operator to the image of the lift, is a fixed nonzero number times a power of a ratio of Hecke values (Theorem 61.3.1). The compression determinant is bounded under $\mathrm{Aut}(\mathbb{C})$ at the trivial twist, and at ℓ at a twist prime to ℓ at which the projection is cleared. The second bound projects integral forms orthogonal to the *false lifts*: forms that satisfy the equations of a lift and are orthogonal to the lifts (Definition 61.3.2). We model this on lines in $\mathbb{C}^3$, then state the theorem of the proof.

61.1. Compressions

Let A and V be finite-dimensional complex inner product spaces and $u\colon A \to V$ an injective linear map, with image R. Write pr_R for the orthogonal projection of V onto R.

Definition 61.1.1. For $G \in \mathrm{End}\, V$, the *compression* of G to R is $\mathrm{pr}_R\, G|_R \in \mathrm{End}\, R$.

Problem 61.1.1. For every $G \in \mathrm{End}\, V$,

$$\det(u^*u)\, \det(\mathrm{pr}_R\, G|_R) = \det(u^*Gu).$$

Now let ϑ run over a set with an element 1, and suppose given for each ϑ an injective $u_\vartheta\colon A \to V_\vartheta$ with image R_ϑ, an operator $\Upsilon_\vartheta \in \mathrm{End}\, V_\vartheta$, and a complex number $\rho_\vartheta \neq 0$. In this section and the next, $Z(\vartheta) := \det(u_\vartheta^* u_\vartheta)$, $D_\vartheta := \det(\mathrm{pr}_{R_\vartheta}\, \Upsilon_\vartheta|_{R_\vartheta})$ and ρ_ϑ are local notations, models of the objects of Section 61.3.

Problem 61.1.2. Suppose that some $\Upsilon^\circ \in \mathrm{End}\, A$ has $\langle y, \Upsilon^\circ y\rangle > 0$ for every $y \neq 0$ and that $\langle u_\vartheta y', \Upsilon_\vartheta u_\vartheta y\rangle = \rho_\vartheta \langle y', \Upsilon^\circ y\rangle$ for all ϑ and $y', y \in A$. Then $\det \Upsilon^\circ \neq 0$, every D_ϑ is nonzero, and

$$Z(\vartheta)\, D_\vartheta = \det(\Upsilon^\circ)\, \rho_\vartheta^{\dim A} \qquad \text{for every } \vartheta.$$

Date: November 26, 2026.

If moreover $\rho_1 = 1$, then $Z(1)/Z(\vartheta) = (D_\vartheta/D_1)\,\rho_\vartheta^{-\dim A}$.

So $Z(\vartheta)$ is traded for ρ_ϑ and D_ϑ. The simplest operators have rank one.

Problem 61.1.3. Let $A = \mathbb{C}$, $u_\vartheta(1) = v_\vartheta$, and $\Upsilon_\vartheta = g_\vartheta g_\vartheta^*$ with $g_\vartheta\colon \mathbb{C} \to V_\vartheta$, $g_\vartheta(1) = w_\vartheta$. Then $Z(\vartheta) = \|v_\vartheta\|^2$ and $D_\vartheta = |\langle w_\vartheta, v_\vartheta\rangle|^2/\|v_\vartheta\|^2$. If $\langle w_\vartheta, v_\vartheta\rangle = c_\vartheta^{-1}\mathrm{per}$ with numbers $c_\vartheta \neq 0$ and $\mathrm{per} \neq 0$, per independent of ϑ, the hypothesis of Problem 61.1.2 holds with $\rho_\vartheta = |c_1|^2/|c_\vartheta|^2$ and $\Upsilon^\circ = |\mathrm{per}|^2/|c_1|^2$.

The *toy* is the following pair of lines in $\mathbb{C}^3$, with the standard inner product, and the set $\{1, \vartheta\}$:

$$v_1 = (1,-1,0), \quad v_\vartheta = (1,1,-2), \qquad w_1 = (2,0,1), \quad w_\vartheta = (1,1,0),$$

with $u_1(z) = zv_1$, $u_\vartheta(z) = zv_\vartheta$, $\Upsilon_1 = w_1 w_1^*$ and $\Upsilon_\vartheta = w_\vartheta w_\vartheta^*$.

Problem 61.1.4. In the toy $Z(1) = 2$ and $Z(\vartheta) = 6$, $D_1 = 2$ and $D_\vartheta = 2/3$, and $Z(1)D_1 = Z(\vartheta)D_\vartheta = 4$.

Problem 61.1.5. Replace w_ϑ by $3w_\vartheta$. Then $D_\vartheta = 6$, the hypothesis of Problem 61.1.2 holds with $\Upsilon^\circ = 4$, $\rho_1 = 1$ and $\rho_\vartheta = 9$, and $(D_\vartheta/D_1)\,\rho_\vartheta^{-1} = 1/3 = Z(1)/Z(\vartheta)$.

Determinants are bounded through eigenvalues.

Problem 61.1.6. Let Y be a finite-dimensional complex vector space, $G \in \operatorname{End} Y$, $f_0\colon \mathbb{C} \to F_0$ a ring homomorphism into a field with an absolute value, and $c \in \mathbb{R}$. If $|f_0(\alpha)| \le c$ for every eigenvalue α of G, then $|f_0(\det G)| \le c^{\dim Y}$.

61.2. False lifts in $\mathbb{C}^3$

Where do bounds for D_ϑ come from? Let $V = \mathbb{C}^n$ with $\langle y, z\rangle = \sum \bar{y}_i z_i$. An automorphism σ of $\mathbb{C}$ acts on V coordinatewise; put $\langle y, z\rangle_\sigma := \langle \sigma y, \sigma z\rangle$, so that $\langle y, y\rangle_\sigma = \|\sigma y\|^2$. For $\iota \mid \ell$ let $\mathcal{L}_\iota := \{y \in V : |\iota(y_i)|_\ell \le 1 \text{ for all } i\}$, the vectors *integral at* ι.

In this section let $X \subseteq V$ be a subspace, the space cut out by the equations that every lift satisfies, and $R \subseteq X$ a subspace, the *lifts*. Put $F := X \cap R^\perp$, the *false lifts*: they satisfy the equations that define X but are orthogonal to the lifts. Let $\Upsilon \in \operatorname{End} V$ with $\Upsilon(R) \perp F$, and put $D := \det(\mathrm{pr}_R\, \Upsilon|_R)$. In Section 61.3, X is the intersection of the image of an idempotent with the kernel of a Hecke operator.

Problem 61.2.1. If $y \perp F$, then $\mathrm{pr}_R\, y = \mathrm{pr}_X\, y$.

Problem 61.2.2. Let $e, \mathbf{H} \in \operatorname{End} V$ with $e = e^* = e^2$, and $X = \operatorname{im} e \cap \ker \mathbf{H}$. Then $F^\perp = R + \ker e + \operatorname{im} \mathbf{H}^*$. In the toy, with e the identity and $\mathbf{H}$ the matrix with all entries 1, $X = \{y : y_1 + y_2 + y_3 = 0\}$ contains $R_1 = \mathbb{C}v_1$ and $R_\vartheta = \mathbb{C}v_\vartheta$; the false lifts are $F_1 = \mathbb{C}v_\vartheta$ and $F_\vartheta = \mathbb{C}v_1$, and $F_1^\perp = \mathbb{C}v_1 + \mathbb{C}(1,1,1)$.

The projection to R can fail to commute with σ. The next two problems give sufficient conditions for $\|\sigma(\mathrm{pr}_R\, y)\| \le \|\sigma y\|$ when $y \perp F$.

Problem 61.2.3. Let $K_0 \subset \mathbb{C}$ be a subfield, Galois over $\mathbb{Q}$ with abelian Galois group, such as $\mathbb{Q}$ or $\mathbb{Q}(\mathrm{i})$, and suppose that X is spanned by vectors with coordinates in K_0. For $\sigma \in \mathrm{Aut}(\mathbb{C})$ and $y \in V$, $\sigma(\mathrm{pr}_X\, y) = \mathrm{pr}_{\sigma X}(\sigma y)$, where σX is spanned by the images under σ of such spanning vectors. Hence $\|\sigma(\mathrm{pr}_R\, y)\| \le \|\sigma y\|$ whenever $y \perp F$.

The next problem models, without rationality, the adjoint identities stated after Definition 61.3.2.

Problem 61.2.4. Let $e, \mathbf{H}$ and X be as in Problem 61.2.2, and suppose that for every $\sigma \in \mathrm{Aut}(\mathbb{C})$: $\langle ey, z\rangle_\sigma = \langle y, ez\rangle_\sigma$ for all y, z, and $\langle \mathbf{H}y, z\rangle_\sigma = 0$ whenever $\mathbf{H}z = 0$. Then $\operatorname{im}\mathbf{H}^* = \operatorname{im}\mathbf{H}$. For every $y \perp F$ there are $z \in R$ and $x \in V$ such that $y = z + x$ and $\langle x, z'\rangle_\sigma = 0$ for every $z' \in R$ and every $\sigma \in \mathrm{Aut}(\mathbb{C})$. For each such y, $\|\sigma(\mathrm{pr}_R\, y)\| \le \|\sigma y\|$ for every $\sigma \in \mathrm{Aut}(\mathbb{C})$.

Problem 61.2.5. Suppose that $\|\sigma(\mathrm{pr}_R\, y)\| \le \|\sigma y\|$ for every σ and every $y \perp F$, and that $\|\sigma(\Upsilon y)\| \le \exp(c)\,\|\sigma y\|$ for all $y \in V$ and $\sigma \in \mathrm{Aut}(\mathbb{C})$. Then $|\sigma(D)| \le \exp(c \dim R)$ for all σ.

Problem 61.2.6. Suppose that $\Upsilon(\mathcal{L}_\iota) \subseteq \mathcal{L}_\iota$, and that $\Lambda \in \operatorname{End} R$ satisfies $\Lambda(\mathrm{pr}_R\, y) \in \mathcal{L}_\iota$ for every $y \in \mathcal{L}_\iota$ with $y \perp F$. Then $|\iota(\det\Lambda \cdot D)|_\ell \le 1$.

For X spanned by vectors in $\mathbb{Q}^n$, the least positive integer c with $c\,\mathrm{pr}_X(\mathbb{Z}^n) \subseteq \mathbb{Z}^n$ is the exponent of the congruence module of X for $\mathbb{Q}^n = (X \cap \mathbb{Q}^n) \oplus (X^\perp \cap \mathbb{Q}^n)$ (Problem 29.1.2). We return to the toy, with $w_\vartheta = (1, 1, 0)$ and X as in Problem 61.2.2.

Problem 61.2.7. For the decomposition $\mathbb{Q}^3 = (X \cap \mathbb{Q}^3) \oplus \mathbb{Q}(1,1,1)$, the congruence module of X in $\mathbb{Z}^3$ is $\mathbb{Z}/3\mathbb{Z}$, and $3\,\mathrm{pr}_X(\mathbb{Z}^3) \subseteq \mathbb{Z}^3$. Hence, for $R = R_1$ and for $R = R_\vartheta$ and at every ι, $\Lambda = 3$ satisfies the hypothesis on Λ in Problem 61.2.6. For $R = R_1$ already $\Lambda = 1$ does.

Problem 61.2.8. In the toy, $\Upsilon_1(R_1) \perp F_1$ and $\Upsilon_\vartheta(R_\vartheta) \perp F_\vartheta$. The hypotheses of Problem 61.2.5 hold for Υ_1 with $\exp(c) = 5$, so $|\sigma(D_1)| \le 5$ for every $\sigma \in \mathrm{Aut}(\mathbb{C})$; those of Problem 61.2.6 hold for Υ_ϑ at $\iota \mid 3$ with $\Lambda = 3$, so $|D_\vartheta|_3 \le 3$, and equality holds.

So for rational X: if $c\,\mathrm{pr}_X(\mathbb{Z}^n) \subseteq \mathbb{Z}^n$ and Υ preserves $\mathcal{L}_\iota$, then $c^{\dim R} D$ is integral at ι; and under the hypotheses of Problem 61.2.5, $|\sigma(D)| \le \exp(c' \dim R)$, where $\exp(c')$ is the operator bound there. Neither bound uses $\det(u^*u)$.

61.3. The general statement

We use the data of Chapter 33 and the objects of Chapter 34: the chosen places $\mathcal{M}$ and their residue fields k_w, with $q_w := \#k_w$; the group $\bar{G}$ and the idempotent e_0; the good forms $H_g(W_j)$; twists ϑ, with modulus Q_ϑ and $\mathrm{Nm}\,Q_\vartheta$, and m-fold twists; the characters μ_j^0, υ and χ_M; the single lifts $u_{\xi,j}$ and $Z_j(\vartheta)$. Fix $1 \le j \le m$. For a twist ϑ, the single lift $u_{\vartheta,j}$ maps $H_g(W_j)$ to the space of algebraic forms on V_j with the weight, level and level character prescribed by the lift datum. Write $R_{\vartheta,j}$ for its image and $\mathrm{pr}_{\vartheta,j}$ for the orthogonal projection onto that image. We use two facts from Chapters 56 and 57: $u_{\vartheta,j}$ is injective for every tame character ϑ (Problem 56.4.2 with Theorem 56.4.1), and $\dim H_g(W_j) = d_T$ (Corollary 57.4.1).

For $\sigma \in \mathrm{Aut}(\mathbb{C})$ and a form y on V_j, in this sheet $N_\sigma(y)$ is the class sum, weighted by the reciprocal orders of the stabilizers, of the squared Gram norms of the vectors $\sigma(y(g))$; $N_1(y) = \|y\|^2$. For a ring homomorphism $\eta\colon \mathbb{C} \to \mathbb{C}_\ell$, a form is *integral at* η if its value at every finite adelic point has gauge at most 1, the gauge of Section 48.3; integral at $\iota \mid \ell$ means integral at ι followed by $\bar{\mathbb{Q}}_\ell \subset \mathbb{C}_\ell$.

Definition 61.3.1. Put $z_\varnothing := (7m + k)/2$, $z_+ := m$, $z_- := m/2$, integers, as is $(t - 11m - 1)/2$, since $m = 2^e$ and $r = 3^{e'}$ (Definition 33.3.1); $\epsilon_\varnothing = \epsilon_+ = 1$ and

$\epsilon_- = -1$; $\nu_\varnothing := \mu_j^0\, \upsilon^{\,j+(t-11m-1)/2}$ and $\nu_\pm := \upsilon^{-z_\pm} \chi_M^{\pm j}$. The *Hecke value product* of lift j at a twist ϑ is

$$\begin{aligned}\mathcal{H}_j(\vartheta) &:= \prod_{i\in\{\varnothing,+,-\}} \mathrm{ex}_{z_i}\big(\mathcal{M}\cup Q_\vartheta,\, (\nu_i\vartheta^{\epsilon_i})^{-1}\big)\\ &= \prod_i \Big[\Big(\prod_{w\in\mathcal{M}\cup Q_\vartheta} q_w\Big)^{z_i^2} \prod_{n=1}^{z_i} \big|L^{\mathcal{M}\cup Q_\vartheta}\big(n, (\nu_i\vartheta^{\epsilon_i})^{-1}\big)\big|^2\Big],\end{aligned}$$

with the exchange factors of Definition 58.2.3 and the partial Hecke values $L^S(z,\nu)$ of Definition 34.10.1.

Let w be a finite place of E with $\bar w \neq w$ and $w, \bar w \notin \mathcal{M}\cup Q_\vartheta$. Let $\mathbf{H}_w$ be the Hecke polynomial of lift j at w, an operator on the forms on V_j made of the Hecke operators at w, evaluated at its test value at w, a number determined by the datum of the lift. The group $\bar G$ acts on these forms by right translation on the block of rank r of V_j, twisted by the tame part of the character of the lift, and e_0 acts through this action.

Definition 61.3.2. The *false lifts at* w are the forms in $\operatorname{im} e_0 \cap \ker \mathbf{H}_w$ that are orthogonal to $R_{\vartheta,j}$. A form is *orthogonal to the false lifts* if it is orthogonal to the false lifts at every such w.

For every such w, the image $R_{\vartheta,j}$ is contained in $\operatorname{im} e_0 \cap \ker \mathbf{H}_w$: this is the unramified Hecke relation of a theta lift, with the equivariance of the lift under $\bar G$; for its background see [Ra82], and Theorem 24.2.1 is a lattice-theta analogue. *Status*: we take the inclusion from the proof, as well as the estimate below. So $\operatorname{im} e_0 \cap \ker \mathbf{H}_w$ plays the part of X in Section 61.2, at each w. For $\sigma \in \mathrm{Aut}(\mathbb{C})$ let $\mathfrak{b}_\sigma$ be the pairing on forms that is σ^{-1} of the class sum of the Gram pairings of the values after σ, so that $N_\sigma(y)$ is the real part of $\sigma(\mathfrak{b}_\sigma(y,y))$. The *projection estimate* is $N_\sigma(\mathrm{pr}_{\vartheta,j}\, y) \le N_\sigma(y)$ for every σ and every y orthogonal to the false lifts; its proof is that of Problem 61.2.4 at one place w, using that for each σ, e_0 is self-adjoint for $\mathfrak{b}_\sigma$ and $\mathbf{H}_w$ has an adjoint for $\mathfrak{b}_\sigma$ that commutes with $\mathbf{H}_w$.

Definition 61.3.3. A family of operators Υ_ϑ on the target space of $u_{\vartheta,j}$, one for every twist ϑ, is a *comparison operator* if: (1) the ratio $\mathcal{H}_j(\vartheta)/\mathcal{H}_j(1)$ is defined and nonzero for every twist ϑ; (2) some $\Upsilon^\circ \in \operatorname{End} H_g(W_j)$ has $\langle y, \Upsilon^\circ y\rangle > 0$ for $y \neq 0$ and $\langle u_{\vartheta,j} y', \Upsilon_\vartheta u_{\vartheta,j} y\rangle = (\mathcal{H}_j(\vartheta)/\mathcal{H}_j(1))\langle y', \Upsilon^\circ y\rangle$ for every twist ϑ and all $y', y \in H_g(W_j)$; (3) for every twist ϑ and $z \in R_{\vartheta,j}$, $\Upsilon_\vartheta z$ is orthogonal to the false lifts; (4) for every twist ϑ, every prime ℓ prime to $\operatorname{Nm} Q_\vartheta$, and every $\eta\colon \mathbb{C} \to \mathbb{C}_\ell$, Υ_ϑ maps forms integral at η to forms integral at η; (5) $N_\sigma(\Upsilon_1 y) \le \exp(3fmb\log^2 b)^2\, N_\sigma(y)$ for every form y at the trivial twist and every $\sigma \in \mathrm{Aut}(\mathbb{C})$.

For a comparison operator put

$$D_\vartheta := \det\big(\mathrm{pr}_{\vartheta,j}\, \Upsilon_\vartheta|_{R_{\vartheta,j}}\big). \tag{1}$$

Definition 61.3.4. For $\iota \mid \ell$, a twist ϑ and a real number $\mathrm{cl}(\ell)$, say that $\mathrm{cl}(\ell)$ *clears the projection* at (ι,ϑ,j) if some $\Lambda \in \operatorname{End} R_{\vartheta,j}$ has $|\iota(\det\Lambda)|_\ell \ge e^{-(\dim R_{\vartheta,j})\, r\, \mathrm{cl}(\ell)}$ and $\Lambda(\mathrm{pr}_{\vartheta,j}\, y)$ is integral at ι for every y that is integral at ι and orthogonal to the false lifts.

Every class of the finite adelic group modulo the rational points and the level has a representative whose components above ℓ are integral, by weak approximation.

Problem 61.3.1. Let $y \neq 0$ be a form in the target space of $u_{\vartheta,j}$, let $\eta\colon \mathbb{C} \to \mathbb{C}_\ell$, and fix class representatives integral above ℓ. At $g = g_0 s g_1$, with g_0 rational, s a representative and g_1 in the level, the gauge of $y(g)$ is the largest absolute value of a coordinate of $\eta(y(s))$. Hence there is $c \in \mathbb{C}^\times$ such that cy is integral at η and αcy is integral at η only if $|\eta(\alpha)|_\ell \leq 1$.

Problems 61.1.1, 61.1.2, 61.1.6, 61.2.5, 61.2.6 and 61.3.1, carried over to forms with the projection estimate, the facts that $N_\sigma(y) > 0$ for $y \neq 0$ and $N_\sigma(ay) = |\sigma(a)|^2 N_\sigma(y)$, the injectivity of $u_{\vartheta,j}$ and $\dim H_g(W_j) = d_T$ (so that $\dim R_{\vartheta,j} = d_T$), prove the following equivalent form of the three results identified in the Lean remark below.

Theorem 61.3.1. *Let $1 \leq j \leq m$ and let (Υ_ϑ) be a comparison operator.* (a) *The number $\det(u_{\vartheta,j}^* u_{\vartheta,j})\, D_\vartheta\, (\mathcal{H}_j(\vartheta)/\mathcal{H}_j(1))^{-d_T}$ is nonzero and does not depend on the twist ϑ.* (b) *For every twist ϑ, every $\iota \mid \ell$ with ℓ prime to $\operatorname{Nm} Q_\vartheta$, and every real $\operatorname{cl}(\ell)$ that clears the projection at (ι, ϑ, j), $|\iota(D_\vartheta)|_\ell \leq e^{d_T r \operatorname{cl}(\ell)}$.* (c) *$|\sigma(D_1)| \leq e^{3 d_T f m b \log^2 b}$ for every $\sigma \in \operatorname{Aut}(\mathbb{C})$.*

In particular every D_ϑ is nonzero. For an m-fold twist ϑ the power ϑ^j is a twist (Section 34.6), and $1^j = 1$.

Problem 61.3.2. For every comparison operator and every m-fold twist ϑ,

$$\frac{Z_j(1)}{Z_j(\vartheta)} = \frac{D_{\vartheta^j}}{D_1} \Big(\frac{\mathcal{H}_j(\vartheta^j)}{\mathcal{H}_j(1)} \Big)^{-d_T}.$$

Chapter 60 combines Problem 61.3.2 and Theorem 61.3.1(b), (c) with the comparison operator of Theorem 60.1.1 and the height bound of Problem 60.2.2 to prove Theorem 60.2.1. Taken as given here: the injectivity of the single lifts, $\dim H_g(W_j) = d_T$, the inclusion of the lifts in $\operatorname{im} e_0 \cap \ker \mathbf{H}_w$, and the projection estimate.

In the Lean formalization. In the Lean proof [GL], in `grh/src/New/OneLift/LiftVolumeHeight.lean` unless said otherwise: Theorem 61.3.1 is `Data.IsComparisonOperator.exists_normDet_sq_mul_det_eq` (a), `.norm_padic_det_liftCompression_le` (b) and `.norm_map_det_liftCompression_le` (c), stated with $\dim H_g(W_j)$ in place of d_T and with a named constant in (a); comparison operators are `Data.IsComparisonOperator`; $\mathcal{H}_j$ is `Data.heckeValueProd` (`New/OneLift/ComparisonOperator/ThreeExchanges.lean`); orthogonality to the false lifts is `DescentPair.IsOrthogonalToFalseLifts` (`New/OneLift/TestedForms.lean`); clearing is `Data.ClearsProjection` (`New/Determinant/Twist/FitTwists.lean`); the inclusion of the lifts in $\operatorname{im} e_0 \cap \ker \mathbf{H}_w$ is `Data.range_goodLift_le_range_inf_ker`, the projection estimate is `Data.normSqAt_starProjection_range_goodLift_le`, and the scaling conclusion of Problem 61.3.1 is the specialization of `DescentPair.exists_smul_mem_integralForms_maximal` to the datum of lift j, whose proof contains the gauge calculation.

Hints

§61.1.

61.1.1: Since u^* kills $R^\perp$, $u^*Gu = u^* \operatorname{pr}_R Gu$. Write u as an isomorphism $A \to R$ followed by the inclusion.
61.1.2: Problem 61.1.1 with $G = \Upsilon_\vartheta$; the hypothesis says $u_\vartheta^* \Upsilon_\vartheta u_\vartheta = \rho_\vartheta \Upsilon^\circ$.
61.1.3: $g_\vartheta^* v = \langle w_\vartheta, v \rangle$.
61.1.4: Problem 61.1.3.
61.1.6: Factor the characteristic polynomial over $\mathbb{C}$.

§61.2.

61.2.1: $X = R \oplus F$, orthogonally.
61.2.2: Take orthogonal complements in the definition of F.
61.2.3: $\operatorname{pr}_X = \mathsf{B}(\mathsf{B}^*\mathsf{B})^{-1}\mathsf{B}^*$ for a matrix B whose columns form a basis of X and have coordinates in K_0; on K_0, complex conjugation commutes with σ.
61.2.4: At $\sigma = 1$, $\ker \mathbf{H} \subseteq (\operatorname{im} \mathbf{H})^\perp = \ker \mathbf{H}^*$. Decompose y by Problem 61.2.2, and use $R \subseteq \operatorname{im} e \cap \ker \mathbf{H}$.
61.2.5: Take an eigenvector z of $\operatorname{pr}_R \Upsilon|_R$ and apply the hypothesis to Υz; then Problem 61.1.6.
61.2.6: Scale an eigenvector of $\Lambda \operatorname{pr}_R \Upsilon|_R$ to be integral at ι with a coordinate of absolute value 1.
61.2.7: Problem 29.1.1: the index of $(\mathbb{Z}^3 \cap X) \oplus \mathbb{Z}(1,1,1)$ in $\mathbb{Z}^3$; then Problems 61.2.1 and 29.1.2. For R_1, write $\operatorname{pr}_{R_1} y$ for $y \perp v_\vartheta$.
61.2.8: $\|w_1\|^2 = 5$, and w_1 has rational coordinates; for equality, Problem 61.1.4.

§61.3.

61.3.1: Use the transformation law at $g_0 s g_1$, whose level character has finite order, and compare the coordinates at all the representatives.
61.3.2: Theorem 61.3.1(a) at ϑ^j and at 1.

References

[GL] L. Sernau, *GRH for Dirichlet L-functions, in Lean 4*, a shorter rewriting of the Lean proof, text by Claude, `https://github.com/lsernau/grh-lean`, commit `72fead1`, readable edition `grh/`.

[Ra82] S. Rallis, *Langlands' functoriality and the Weil representation*, Amer. J. Math. **104** (1982), 469–515.

HECKE VALUES AS NORMS OF LIFTS

Prerequisites. Euler products of Hecke L-functions [Ne, Ch. VII, §8]. Chapter 23 (Sections 23.2, 23.3; Problems 23.2.3, 23.3.3, 23.3.4); Chapter 5 (heights, Section 5.3; Problems 5.3.1, 5.4.4); the data, B (Definition 33.4.1) and s_∞ of Chapter 33; from Chapter 34 the chosen places $\mathcal{M}$, $\mathcal{N}$, tame characters, υ, χ_M with residue characters ω, the vacuum scale c_{vac} and critical pairs; integrality at $\eta\colon \mathbb{C} \to \mathbb{C}_\ell$ (Section 48.3); c_{jet} (Definition 50.4.3); Theorem 56.2.1; $\mathcal{H}_j$ (Definition 61.3.1). We write $|y|_\iota := |\iota(y)|_\ell$, $|\ell|_\ell = 1/\ell$.

For a regular family θ of m-fold twists and $1 \le j \le m$, Chapter 60 bounds the height of $Z_j(1)/Z_j(\theta_\iota)$, and Problem 61.3.2 expresses this quotient through the compression determinants and the quotient $\mathcal{H}_j(\vartheta)/\mathcal{H}_j(1)$ of products of Hecke values at $\vartheta = \theta_\iota^j$. How can a ratio of L-values be bounded at every $\iota \mid \ell$? For a critical pair with $z \ge 2$, the squared norm of a theta lift of a character from U(1), divided by $(\operatorname{Nm} Q_\xi)^{2z-1}$, is the partial Hecke value times a constant independent of the twist ξ; an integer multiple of it is integral away from $\operatorname{Nm} Q_\xi$; and for a main pair the untwisted squared norm has bounded height. We begin with a lift between two lines over $\mathbb{Z}[\mathrm{i}]$ and with the local factors in rank four over $\mathbb{F}_3$.

62.1. A Hecke value as a squared norm

In this section only, c_a, ϑ_0 and $L(\bar\upsilon_n, s)$ have the meanings of Sections 23.2 and 23.3. By Problem 23.2.3 the lift $\Theta_{(4)}$ between two lines is multiplication by $c_4/4$, and Problem 23.3.4 gives

$$\frac{c_4^2}{16} = 2100\,\vartheta_0^2\,(2\pi)^{-8}\,L(\bar\upsilon_8, 8).$$

Problem 62.1.1. To the precision shown, $c_4 \approx 0.14319133702$, $\vartheta_0 \approx 1.18034059902$, $L(\bar\upsilon_8, 8) \approx 1.06394325884$, and both sides of the display are ≈ 0.00128148493742.

This lift has rank one, which Theorem 62.4.1 excludes (it needs rank $2z \ge 4$); it shows only the shape of part (i), a squared norm equal to a fixed constant times a Hecke value. The size of the L-value itself is controlled by its Euler product, once the coefficients are unitary.

Problem 62.1.2. $L(\bar\upsilon_8, 8) = \sum_{\mathfrak{a}} (\bar\alpha/|\alpha|)^8 \operatorname{Nm}\mathfrak{a}^{-4}$, the sum over the nonzero ideals $\mathfrak{a} = (\alpha)$ of $\mathbb{Z}[\mathrm{i}]$, with coefficients of absolute value 1. Hence $\log L(\bar\upsilon_8, 8) \le \log \zeta_{\mathbb{Q}(\mathrm{i})}(4)$; numerically $0.0620 \le 0.0680$.

In the proof the character is lifted to a definite space of rank n, with a finite datum on columns of length n at finitely many places. At each such place w, with residue field $\mathbb{F}_q$, three factors enter: the mean of the squared absolute value of the datum on $\mathbb{F}_q^n$, the index of the target level in the integral group, and $(1 - q^{-n})^{-1}$, restored from the denominator Euler product in the vacuum sum. At a *chosen* place the datum is the indicator of a fixed basis vector, and the level fixes that

Date: November 26, 2026.

vector. At a place of the modulus Q_ξ it is the residue character of one coordinate, extended by zero, whose squared absolute value is the indicator of the complement of the coordinate hyperplane; the level preserves the hyperplane.

Problem 62.1.3. For $q = 3$, $n = 4$: one fixed vector is a proportion $1/81$ of $\mathbb{F}_3^4$, $\mathrm{GL}_4(\mathbb{F}_3)$ acts transitively on the 80 nonzero vectors, $(1 - 3^{-4})^{-1} = 81/80$, and the product is 1. In general $q^{-n}(q^n - 1)(1 - q^{-n})^{-1} = 1$.

Problem 62.1.4. For $q = 3$, $n = 4$: the vectors with nonzero first coordinate are a proportion $2/3$, $\mathrm{GL}_4(\mathbb{F}_3)$ acts transitively on the 40 hyperplanes, and $\frac{2}{3} \cdot 40 \cdot \frac{81}{80} = 27 = 3^3$. In general $\frac{q-1}{q}(1 + q + \cdots + q^{n-1})(1 - q^{-n})^{-1} = q^{n-1}$.

So the three factors give 1 at a chosen place and q^{n-1} at a place of the modulus: this is the power of $\mathrm{Nm}\, Q_\xi$ in Theorem 62.4.1. (The index of the source level of $\mathrm{U}(1)$ supplies a separate factor $q - 1$ at each chosen place.)

62.2. The lift of a character

Recall from Definition 34.10.1 that a critical pair $P = (\nu, z)$ has a character ν of weight $-\mathrm{wt}_P$, with $z \le \mathrm{wt}_P(\tau) \le 4b$, tame part trivial off $\mathcal{M}$, and $1 \le z \le t$; that $L^S(z, \mu)$ is the Euler product of the unitary Hecke character $y \mapsto \mu(y/\bar{y})$ of E, evaluated at chosen uniformizers, over the places outside $S \cup \bar{S}$, with its value at $z = 1$ given by the limit from the right whenever that limit exists in $\mathbb{C}$ (when $S \cup \bar{S}$ contains the ramified places, this is the partial Hecke L-function); and that for a tame character ξ and $\epsilon = \pm 1$

$$R_P(\xi, \epsilon) = \frac{|L^{\mathcal{M} \cup Q_\xi}(z, (\nu\xi^\epsilon)^{-1})|}{|L^{\mathcal{M}}(z, \nu^{-1})|}, \qquad R_P(\xi) = R_P(\xi, 1).$$

Definition 62.2.1. The *row* of a critical pair $P = (\nu, z)$ is $\lambda_P(\tau) := \mathrm{wt}_P(\tau) - z \ge 0$, for $\tau \in \Phi$. In this chapter $|\lambda_P| := \sum_{\tau \in \Phi} \lambda_P(\tau)$.

Definition 62.2.2. Let $P = (\nu, z)$ be a critical pair with $z \ge 2$ and ξ a tame character. Consider the theta lift of the constant function 1 on $\mathrm{U}(1)$ to the standard definite space of rank $2z$, for the character $\nu\xi$, with the following datum: at infinity the highest vector of the weight with one row of length $\lambda_P(\tau)$ at each τ; at the places of $\mathcal{M}$ the indicator of one fixed basis vector, at the places of Q_ξ the residue characters of ξ at one fixed coordinate, extended by zero (as in Section 62.1); the vacuum elsewhere. The *lift of the constant* $\phi_{P,\xi}$ is this lift times the index of the chosen level of $\mathrm{U}(1)$ and times $c_{\mathrm{vac}}^{2z}(\pi_M c_{\mathrm{jet}})^{|\lambda_P|}$.

The class sum of the theta kernel of this datum over $\mathrm{U}(1)$ at the chosen level equals the theta lift of 1 times the source level index; multiplying this class sum by $c_{\mathrm{vac}}^{2z}(\pi_M c_{\mathrm{jet}})^{|\lambda_P|}$ gives $\phi_{P,\xi}$. Its squared norm is computed by Theorem 56.2.1 for this sharp datum, which the proof checks (*Status*: the Rallis inner product formula [Ra, Li]). At infinity the Fock vector is paired with itself.

Problem 62.2.1. In the Fock space of Section 23.3, with variables $u_{\tau,1}, \ldots, u_{\tau,2z}$ at τ, the vector $\prod_\tau u_{\tau,1}^{\lambda_P(\tau)}$ has squared norm $\prod_\tau \lambda_P(\tau)!$.

Fix a critical pair $P = (\nu, z)$ with $z \ge 2$. The proof combines the formula of Theorem 56.2.1, the vacuum sum (the partial Hecke value divided by the product of $(1 - \varepsilon_w q_w^{-z})^{-1}$ over the finite places outside $\mathcal{M} \cup Q_\xi$ and its conjugates, with opposite signs ε_w at distinct conjugate places and $+1$ at a self-conjugate place), the local

factors of Problems 62.1.3 and 62.1.4 at the places of $\mathcal{M}\cup Q_\xi$, and Problem 62.2.1. It obtains a complex number $C_P\neq 0$, independent of ξ, with

$$\|\phi_{P,\xi}\|^2 = C_P\, L^{\mathcal{M}\cup Q_\xi}\big(z,(\nu\xi)^{-1}\big)\,(\mathrm{Nm}\,Q_\xi)^{2z-1}$$

for every tame character ξ. Here C_P is the squared modulus of the scale times the volumes of the two adelic quotients, divided by the full signed Euler product at z, times $\prod_{w\in\mathcal{M}}(q_w-1)$, the hook number $\prod_\tau \lambda_P(\tau)!$ and the dimension of the weight. The lift is nonzero for every tame ξ.

Problem 62.2.2. Let χ be a unitary Hecke character of E, S a finite set of finite places, and (in this problem) $L^S(s,\chi)$ its L-function without the factors at S. For real $s\geq 2$, $L^S(s,\chi)$ is nonzero and $|\log|L^S(s,\chi)|| \leq [E:\mathbb{Q}]\log\zeta(2) = 2f\log\zeta(2) < 4f$.

The proof uses the bound $4f$.

62.3. Integrality, and the direction of the estimate

Definition 62.3.1. For a critical pair $P=(\nu,z)$ with $z\geq 2$ let $d_P := M^{4fz}(Md)^{|\lambda_P|}$, and for a tame character ξ let the *algebraic part* be

$$\mathrm{alg}_P(\xi) := \mathcal{N}\, d_P^2\, \frac{\|\phi_{P,\xi}\|^2}{(\mathrm{Nm}\,Q_\xi)^{2z-1}}.$$

At primes $\ell\nmid \mathrm{Nm}\,Q_\xi$ the number d_P clears the denominators of the scaled theta kernel: M^{4fz} those of the finite datum, and Md per box of the row those of the derivatives. The proof shows that for every such ℓ and every ring homomorphism $\eta\colon\mathbb{C}\to\mathbb{C}_\ell$ the form $d_P\phi_{P,\xi}$ is integral at η (*Status*: read from the code). The squared norm is a class sum, $\|\phi\|^2 = \sum_c |\Gamma_c|^{-1}\langle\phi(g_c),\phi(g_c)\rangle$, over representatives g_c with finite stabilizers Γ_c.

Problem 62.3.1. Let I and T be finite sets, G an $I\times I$ hermitian matrix with entries in $\mathbb{Z}$, and $\eta\colon\mathbb{C}\to\mathbb{C}_\ell$ a ring homomorphism. For $c\in T$ let $a_c\in\mathbb{C}^I$, and let γ_c be a positive integer dividing a fixed integer $A\geq 1$. If $|\eta(a_{c,i})|\leq 1$ and $|\eta(\bar a_{c,i})|\leq 1$ for all c,i, then $|\eta(A\sum_c \gamma_c^{-1}\, a_c^* G a_c)|\leq 1$.

Problem 62.3.1 models two inputs read from the code. At any finite adelic point, the Gram pairing of two values of gauge at most one, the first at $\eta\circ$ (complex conjugation) and the second at η, is integral at η. On the standard definite space of rank at most $2n_m$, for every level contained in the stabilizer of the standard lattice, every class stabilizer has order dividing $\mathcal{N}$.

Problem 62.3.2. Let $P=(\nu,z)$ be a critical pair with $z\geq 2$ and ξ a tame character. Given the norm formula of Section 62.2, the integrality of $d_P\phi_{P,\xi}$, the Gram-pairing integrality and the divisibility of the stabilizer orders: $|\eta(\mathrm{alg}_P(\xi))|_\ell \leq 1$ for every prime $\ell\nmid\mathrm{Nm}\,Q_\xi$ and every $\eta\colon\mathbb{C}\to\mathbb{C}_\ell$; at $\xi=1$ this holds at every prime; and $R_P(\xi)=\mathrm{alg}_P(\xi)/\mathrm{alg}_P(1) = \big(\|\phi_{P,\xi}\|^2/(\mathrm{Nm}\,Q_\xi)^{2z-1}\big)/\|\phi_{P,1}\|^2$.

Fix a critical pair $P=(\nu,z)$ with $z\geq 2$. For $1\leq j\leq m$ and a regular family θ of m-fold twists (Definition 64.2.3), write $\vartheta_\iota := \theta_\iota^j$. The family to be estimated has terms $R_P(\vartheta_\iota)^{-1} = \mathrm{alg}_P(1)/\mathrm{alg}_P(\vartheta_\iota)$. The denominator is integral at ι, as $\ell\nmid\mathrm{Nm}\,Q_{\vartheta_\iota}$; its inverse need not be small there.

Problem 62.3.3. For $n\geq 1$, the number $y_n := (2+\mathrm{i})^n$ is integral at every ι, and $|\sigma(y_n)| = 5^{n/2}$ for every $\sigma\in\mathrm{Aut}(\mathbb{C})$; yet $|y_n^{-1}|_\iota = 5^n$ for $\iota\mid 5$ with $|2+\mathrm{i}|_\iota = 1/5$.

Thus an integral denominator can have a large inverse at the specified embedding, while Theorem 62.4.1(ii) gives only an upper bound for the absolute value of the denominator.

62.4. The size of the untwisted norm

Definition 62.4.1. A critical pair $P = (\nu, z)$ is *main for* j if $z \geq 10$, $m < z \leq r$, $1 \leq j \leq m$, the tame part of ν is ω^j, and $\kappa_j(\tau) + r - t \leq \mathrm{wt}_P(\tau) \leq \kappa_j(\tau)$ for every τ. It has *empty row* if $z \geq 2$ and $\mathrm{wt}_P(\tau) = z$ for every τ, or equivalently if $z \geq 2$ and $\lambda_P(\tau) = 0$ for every τ.

Problem 62.4.1. $s_\infty(y+1) \geq s_\infty(y)$ for every integer $y \geq 0$.

Problem 62.4.2. If P is main for j, then $\kappa(\tau) \leq \lambda_P(\tau) \leq \kappa(\tau) + x^{42}$ for every $\tau \in \Phi$.

The conjugates of the squared norm are read from the code. For $\sigma \in \mathrm{Aut}(\mathbb{C})$ fixing K and each integer $z \geq 2$ there is $c_{\sigma,z} \in \mathbb{R}$ such that every critical pair $P = (\nu, z)$ satisfies

$$\log\bigl|\sigma\bigl(\|\phi_{P,1}\|^2\bigr)\bigr| = c_{\sigma,z} + r_{\sigma,P} + \sum_{\tau\in\Phi} s_\infty(\lambda_P(\tau))$$

with a real $r_{\sigma,P} \geq -4f$, and $r_{\sigma,P} \leq 4f$ if P has empty row. Here $r_{\sigma,P}$ is the logarithm of the dimension of the transported weight (which is 1 for an empty row) plus $\log|L|$ for the inverse transported character at z away from $\mathcal{M}$, bounded by the $4f$ of Problem 62.2.2. The factors $M^{|\lambda_P|}$, $\Omega^{-|\lambda_P|}$ and $\prod_\tau \lambda_P(\tau)!$ come from $|\pi_M|^2 = M$, from conjugating the scaled jets, and from Problem 62.2.1. (*Status*: read from the code, which uses the conjugation of CM theta series and the Chowla–Selberg formula for the common area of the lattices $\sigma(u)\Lambda^\sigma$, with Λ^σ the conjugate lattice and u a number of absolute value 1 at every finite place; classical background: [Sh, Thm. 5.4], Theorem 20.3.1.) The proof also uses that for $2 \leq z \leq r$, with the same z as P, the pair $P_0 := (\upsilon^{-z}, z)$ is a critical pair with empty row and trivial tame part, and that $\mathcal{N}d_{P_0}^2 \leq e^{x^{33}}$.

Problem 62.4.3. For the data, $x^{33} + 8f \leq B$.

Problem 62.4.4. Let $P = (\nu, z)$ be main for j and $H := \mathrm{alg}_{P_0}(1)/\|\phi_{P,1}\|^2$. Then $\log|\sigma H| \leq B - \sum_\tau s_\infty(\kappa(\tau))$ for every $\sigma \in \mathrm{Aut}(\mathbb{C})$ and $|H\|\phi_{P,1}\|^2|_\iota \leq 1$ for every ι. Hence the constant family $\iota \mapsto \|\phi_{P,1}\|^2$ has height at most $B - \sum_\tau s_\infty(\kappa(\tau))$.

Problem 62.3.2 proves (i) and (ii) of the following theorem, and Problem 62.4.4 proves (iii).

Theorem 62.4.1. *Let $P = (\nu, z)$ be a critical pair with $z \geq 2$.* (i) *For every tame character ξ, $R_P(\xi) = \bigl(\|\phi_{P,\xi}\|^2/(\mathrm{Nm}\, Q_\xi)^{2z-1}\bigr)/\|\phi_{P,1}\|^2$.* (ii) *For every tame character ξ, every prime $\ell \nmid \mathrm{Nm}\, Q_\xi$ and every ring homomorphism $\eta\colon \mathbb{C} \to \mathbb{C}_\ell$, $|\eta(\mathrm{alg}_P(\xi))|_\ell \leq 1$.* (iii) *If P is main for j, the constant family $\iota \mapsto \|\phi_{P,1}\|^2$ has height at most $B - \sum_{\tau\in\Phi} s_\infty(\kappa(\tau))$.*

62.5. The Hecke product as a product of ratios

Recall from Definition 61.3.1 that $\mathcal{H}_j(\vartheta)$ is a product over $i \in \{\varnothing, +, -\}$ of $(\prod_{w\in S} q_w)^{z_i^2} \prod_{v=1}^{z_i} |L^S(v, (\nu_i \vartheta^{\epsilon_i})^{-1})|^2$, with $S = \mathcal{M} \cup Q_\vartheta$, lengths $z_\varnothing = (7m + k)/2$, $z_+ = m$, $z_- = m/2$, signs $\epsilon_\varnothing = \epsilon_+ = 1$, $\epsilon_- = -1$, and characters $\nu_\varnothing =$

$\mu_j^0 v^{j+(t-11m-1)/2}$, $\nu_\pm = v^{-z_\pm}\chi_M^{\pm j}$; each (ν_i, z_i) is a critical pair. At $v = 1$ we use that $L^S(1,\mu) \neq 0$ for an automorphic character μ of U(1) with nonzero weight and a tame part, for every finite set S of finite places of E (*Status*: classical [La, Ch. XV]).

Problem 62.5.1. Let $1 \le j \le m$ and let ϑ be a twist. (a) For $1 \le v \le z_i$, (ν_i, v) is a critical pair, and

$$\frac{\mathcal{H}_j(\vartheta)}{\mathcal{H}_j(1)} = (\mathrm{Nm}\, Q_\vartheta)^{z_\varnothing^2+z_+^2+z_-^2}\Big(\prod_i \prod_{v=1}^{z_i} R_{(\nu_i,v)}(\vartheta, \epsilon_i)\Big)^2.$$

(b) All these pairs are ramified; the $k/2$ pairs $(\nu_\varnothing, v)$ with $7m/2 < v \le z_\varnothing$ are moreover main for j, and the remaining indices number $5m$. (c) Formally for $m = 2$, $k = 4$: $(z_\varnothing, z_+, z_-) = (9, 2, 1)$, the exponent is 86, and the index range $7m/2 < v \le z_\varnothing$ has 2 positions, leaving 10 others.

At $\vartheta_\iota = \theta_\iota^j$ for a regular family, the inverse of $\mathcal{H}_j(\vartheta_\iota)/\mathcal{H}_j(1)$ has the factor $(\mathrm{Nm}\, Q_{\vartheta_\iota})^{-(z_\varnothing^2+z_+^2+z_-^2)}$, a unit at $\iota \mid \ell$. For the $5m$ remaining factors, regularity bounds the height of the inverse ratios by x_1 (Definition 64.2.2). For the $k/2$ main factors see Theorem 64.4.1.

We have proved Theorem 62.4.1 and the factorization of Problem 62.5.1. Taken as given: the norm formula of Section 62.2 (Theorem 56.2.1 for the sharp datum, the vacuum sum, the nonvanishing of the lift); the integrality of $d_P\phi_{P,\xi}$, of Gram pairings, and the divisibility of the stabilizer orders by $\mathcal{N}$; the formula of Section 62.4 for the conjugates of $\|\phi_{P,1}\|^2$, with the pair P_0 and the bound $\mathcal{N} d_{P_0}^2 \le e^{x^{33}}$; and $L^S(1,\mu) \neq 0$. Chapter 64 supplies the lower bound for $|\mathrm{alg}_P(\vartheta_\iota)|_\iota$ that Problem 62.3.3 shows is missing; it needs Theorem 62.4.1, Definitions 62.2.1–62.3.1 and Problems 62.4.2 and 62.5.1.

In the Lean formalization. In the Lean proof [GL] (`grh/src/`, namespace `New.` omitted; files in `New/OneLift/HeckeValues/` unless a path is given; auxiliary steps by name only): Theorem 62.4.1 is `Data.CriticalPair.ratio_eq_algPart_div` (`TwistedRatio.lean`), `Data.CriticalPair.integralAlgebraicPart_mem_integralAway` (`AlgebraicPartIntegrality.lean`) and `Data.heightLe_norm_trivialLift_sq` (`AlgebraicPartSize.lean`). Definitions 62.2.2 and 62.3.1 are `Data.CriticalPair.trivialLift` and `Data.CriticalPair.integralAlgebraicPart` (`CharacterLiftNorm.lean`), and Definition 62.4.1 is `Data.CriticalPair.IsMainPair` (`New/Determinant/Twist/FitTwists.lean`) and `Data.CriticalPair.HasEmptyRow` (`CharacterLiftNorm.lean`). The norm formula is derived from `LValueData.inner_trivialLift_self_eq_L` (`CharacterLiftNorm.lean`), which is stated for the class sum, without the scale $c_{\mathrm{vac}}^{2z}(\pi_M c_{\mathrm{jet}})^{|\lambda_P|}$; the integrality of $d_P\phi_{P,\xi}$ is `Data.CriticalPair.denomBound_smul_trivialLift_mem_integralForms`, and the displayed formula of Section 62.4 is `Data.CriticalPair.exists_log_norm_map_norm_sq_trivialLift_eq_add_sum_jetSize`. Auxiliary steps (a leading dot repeats the preceding namespace): `Data.CriticalPair.lValueData`, `.rowLengthSum`, `DescentPair.residueBlockDatum`, `LValueData.relIndex_descentResidueLevel`, `.stdLevelIndex_chosenLevel`,

`LValueData.trivialLift`, `.trivialLift_eq_smul_thetaLift`, `.isSharp_blockDatum`, `.inner_thetaLift_constForm_self`, `.integral_fockInner_realPairWeil`, `.hookNumber_eq_prod_factorial`, `Data.CriticalPair.exists_ne_zero_algPart_eq_mul_L`, `.L_inv_mul`, `.trivialLift_ne_zero`, `.denomBound`, `.weylGauge_denomBound_smul_pointKernel_le_one`, `LevelPlaces.LevelForm.inner_eq_stdClassSum`, `Data.CriticalPair.ratio_eq_integralAlgebraicPart_div`, `.norm_trivialLift_sq_eq_mul_inner`, `.exists_norm_map_inner_trivialLift_eq_mul`, `LValueData.map_trivialLift`; local factors, `LValueData.blockMeanSquare_mul_relIndex_mul_prod_eq_pow`; vacuum sum, `vacuumSum_eq_L_div_eulerProd`; Euler bound, `eulerProd_ne_zero_and_abs_log_norm_le`, specialized to $4f$ in `Data.exists_log_norm_inner_trivialLift_eq`; pairings and stabilizers, `gramForm_mem_embValRing` and `LevelPlaces.LevelForm.norm_nsmul_inner_le_one` and `Data.card_classAut_dvd_chosenGroupOrder`; CM, `CMLattice.complex_multiplication_theta` and `CMLattice.chowla_selberg`; P_0 and $e^{x^{33}}$, `Data.exists_hasEmptyRow` and `Data.CriticalPair.chosenGroupOrder_mul_denomBound_sq_le`; nonvanishing at 1, `AutChar.HasWeight.L_ne_zero`; the Hecke product, `Data.exchangePair`, `Data.CriticalPair.lowerPoint`, `Data.heckeValueProd_eq_mul_prod_ratio_sq`, `Data.isMainPair_lowerPoint_exchangePair_none`, `Data.isRamified_lowerPoint_exchangePair` and `Data.exists_heckeValueProd_eq_mul_prod_ratio`; the inverse ratios of main pairs, `Data.heightLe_inv_ratio`.

Hints

62.1.2: $\bar\alpha^8|\alpha|^{-16} = (\bar\alpha/|\alpha|)^8|\alpha|^{-8}$; compare with $\zeta_{\mathbb{Q}(\mathrm{i})}(4)$.

62.2.1: Problem 5.4.4; the norm factors over the variables.

62.2.2: Compare with $\zeta_E(s) \le \zeta(s)^{[E:\mathbb{Q}]}$.

62.3.3: Problem 5.3.1.

62.3.2: The Gram-pairing bound at each representative of the class sum, as in Problem 62.3.1; $\operatorname{Nm} Q_\xi$ is a unit at ℓ. For the ratio compare the norm formula at ξ and at 1.

62.4.1: Problem 33.4.3.

62.4.2: $z \le r$; $\kappa_j - \kappa = (j + \frac12)\Delta$ (Section 34.2); Definition 33.3.1.

62.4.3: $B = fxb \log^3 b/(mk)$ with $mk \le 6x^{11/2}$, and $b \ge x^{10^{12}}$.

62.4.4: Subtract the displayed formulas for P_0 and P (same z); then Problems 62.4.1, 62.4.2, 62.4.3, and 62.3.2 at $\xi = 1$. An automorphism not fixing K is complex conjugation composed with one that does.

62.5.1: (a) $\mathcal{M}$ and Q_ϑ are disjoint; divide each factor by its value at $\vartheta = 1$. (b) Problem 34.10.1, also for ω^{-j}. For the weights, μ_j^0 has weight $-\kappa_j$ and υ weight 1; use $r \ge x^5$, $m \le 2\sqrt{x}$ (Definition 33.3.1).

References

[GL] L. Sernau, *GRH for Dirichlet L-functions, in Lean 4*, a shorter rewriting of the Lean proof, text by Claude, `https://github.com/lsernau/grh-lean`, commit `72fead1`, readable edition `grh/`.

[La] S. Lang, *Algebraic Number Theory*, 2nd ed., GTM 110, Springer, 1994.

[Li] J.-S. Li, Non-vanishing theorems for the cohomology of certain arithmetic quotients, *J. reine angew. Math.* **428** (1992), 177–217.

[Ne] J. Neukirch, *Algebraic Number Theory*, Grundlehren 322, Springer, 1999.

[Ra] S. Rallis, *L-functions and the oscillator representation*, LNM 1245, Springer, 1987.

[Sh] G. Shimura, *Introduction to the Arithmetic Theory of Automorphic Functions*, 1971.

THE BOUND IS ATTAINED AT MANY PLACES

Prerequisites. Chapter 19: the least valuation $\mu(n)$ on the lemniscate, Theorems 19.2.1 and 19.3.1 with the series $y(z)$ and the ring $\mathfrak{o}[[y]]$ of Section 19.3, and Problems 19.1.1, 19.3.1, 19.3.2, 19.4.1, 19.4.2 and 19.4.3. The moments $t(a,w)$ of Section 15.1 and Theorem 16.3.1. The data (Definition 33.3.1, the constant v_0 of Section 33.3), the integral vacuum (Section 34.8), the local prime sums $s_{\mathrm{fin},p}$, the numbers c_p and the sets I_p (Section 48.1), and the jet series of a datum with its scale c_{jet} (Definition 50.4.3). Lagrange's four-square theorem; the ultrametric inequality in $\mathbb{C}_p$, whose valuation val has $\mathrm{val}(p)=1$.

Chapter 60 bounds the cost of one lift using the test forms of Chapter 64. At a prime p prime to the norm of the twist, a test form uses a Taylor coefficient on twelve copies of the variables; multiplied by $c_{\mathrm{vac}}^{12}\prod_\tau \lambda(\tau)!$ and divided by one c_{att} independent of p, it must have valuation at most the divisibility $s_{\mathrm{fin},p}^{\mathrm{tot}}$ predicted by the prime sum. How can one normalization serve all primes, when the partners $[-p^e]\tau$ of a place lower the prediction?

63.1. One curve, one partner

Recall $\mu(n)\le\gamma_p n$, $\gamma_p=p/(p^2-1)$, for $p\equiv 3 \pmod 4$ (Theorem 19.2.1).

Problem 63.1.1. For $p=3$: $\mu(3),\mu(9),\mu(11),\mu(81)=1,3,4,30$, each below $3n/8$.

For $p\equiv 3 \pmod 4$, $w\ge 0$ and $G\in\mathbb{Z}_p[\mathrm{i}][[X_1,X_2]]$ with $X_1=\mathrm{sl}\,s$, $X_2=\mathrm{sl}\,t$, the valuation of $\partial_s^{pw}\partial_t^{w}G(0,0)$ is at least $\mu(pw)+\mu(w)$ (Problem 19.4.2). A non-integral series does better.

Problem 63.1.2. $\partial_s^{pw}\partial_t^{w}e^{s^pt/p}\big|_{(0,0)}=(pw)!/p^w$, of valuation $v_p(w!)$. For $p=3$, $w=2$ this is 80, a unit, while for every $G\in\mathbb{Z}_3[\mathrm{i}][[X_1,X_2]]$, with $X_1=\mathrm{sl}\,s$, $X_2=\mathrm{sl}\,t$, the valuation of $\partial_s^6\partial_t^2G(0,0)$ is at least 2.

For a prime $p\equiv 3 \pmod 8$ and integers $a,w\ge 0$, Theorem 16.3.1 gives in particular $v_p(t(a,w))\ge\sum_{i\ge1,\ i\ \mathrm{odd}}(\lfloor a/p^i\rfloor-w)_+$ for the moments of Section 15.1, where w is the order of the derivative in the partner direction.

Problem 63.1.3. $v_{11}(t(27,1))=v_{11}(t(38,2))=v_{11}(t(49,3))=1$, and in each case the bound of Theorem 16.3.1 at $p=11$ is 1: in these three cases the theta function itself attains the bound.

Problem 63.1.4. At $p=3$: $v_3(t(a,1))=6,6,9$ for $a=11,19,27$, while the bound of Theorem 16.3.1 is $2,5,8$.

So a fixed theta function can miss. For each p and η the proof chooses twelve sections, one on each copy of the variables $(z_\tau)_{\tau\in\Phi}$.

Date: November 26, 2026.

63.2. What the partners take away

From now on we use the data (Definition 33.3.1). Fix a prime p and a ring homomorphism $\eta\colon \mathbb{C} \to \mathbb{C}_p$. Then c_p, I_p and the local prime sum $s_{\mathrm{fin},p}(y,\sigma) = c_p \sum_{e\in I_p}(y/p^e - \kappa([-p^e]\sigma))_+$ are those of Section 48.1. Let $\gamma_p := c_p \sum_{e\in I_p} p^{-e}$ (values in Problem 19.3.1). The *total local prime sum* is

$$s^{\mathrm{tot}}_{\mathrm{fin},p} := \sum_{\tau\in\Phi} s_{\mathrm{fin},p}(\kappa(\tau),\tau). \tag{1}$$

By Problem 19.4.1, $s^{\mathrm{tot}}_{\mathrm{fin},p} \le \gamma_p \sum_\tau \kappa(\tau)$. The difference is what the partners take away.

Problem 63.2.1. $\gamma_p \sum_\tau \kappa(\tau) - s^{\mathrm{tot}}_{\mathrm{fin},p} = c_p \sum_{\tau\in\Phi}\sum_{e\in I_p} \min\bigl(\kappa(\tau)/p^e,\ \kappa([-p^e]\tau)\bigr)$.

At an inert prime the partners enter the theta function through couplings. The proof uses a fixed curve: the lattice $\Lambda = \Omega_0\mathcal{O}_K$, with Ω_0 as in Definition 50.4.3, with t, a_1 and the series y as in Section 19.3; let $\mathrm{area}(\Lambda)$ be the area of $\mathbb{C}/\Lambda$. Let σ_Λ be the odd entire function with $\sigma'_\Lambda(0) = 1$ and $\sigma_\Lambda(z+l) = \epsilon_l \exp\bigl(\pi(\bar l z + |l|^2/2)/\mathrm{area}(\Lambda)\bigr)\sigma_\Lambda(z)$ for $l \in \Lambda$, where $\epsilon_l = 1$ on 2Λ and -1 elsewhere. In this sheet let

$$\mathrm{th}(z) := e^{-\pi z\bar t/\,\mathrm{area}(\Lambda)}\,\frac{\sigma_\Lambda(z+t)}{\sigma_\Lambda(t)},$$

We read its Taylor series in $\mathbb{C}_p$ through η. For linear forms μ_β on $\mathbb{C}_p^\Phi$ and integers $c_\beta \ge 0$ (β in a finite set) put $\mathrm{th}_{\mathrm{fr}}(z) := \prod_\beta \mathrm{th}(\mu_\beta z)^{c_\beta}$, and for odd e let $\Gamma_e := \sum_\tau z_\tau^{p^e} z_{[-p^e]\tau}$ be the coupling of each place with its partner.

Normal form. Let p be inert in K, and let the forms be those of a tight frame (Definition 63.3.1 below). The proof shows that there are $\varpi \in \mathbb{C}_p$ with $\mathrm{val}\,\varpi = 1/(p^2-1)$, integral $\mathfrak{l}_{e,j}$ (e odd, $j \ge 0$) with $\mathfrak{l}_{e,0}$ a unit, and an integral series W in the z_τ, such that

$$\mathrm{th}_{\mathrm{fr}}(\varpi z) = W(z)\exp\Bigl(\frac{\varpi^{p+1}}{p}\sum_{e\ \mathrm{odd}}\sum_{j\ge 0}\mathfrak{l}_{e,j}\,\Gamma_e^{p^j}\Bigr).$$

Status: read from the proof.

Problem 63.2.2. A two-variable model: $K = \mathbb{Q}(\sqrt{-7})$, $p = 13$, variables z_1, z_2, $\mathrm{val}\,\varpi = 1/168$ and $\mathfrak{l}_{1,0}$ a unit. Then 13 is inert in K, $\mathrm{val}(\varpi^{14}/13) = -11/12$, and the coefficient of $z_1^{13}z_2$ in $(\varpi^{14}/13)\mathfrak{l}_{1,0}(z_1/\varpi)^{13}(z_2/\varpi)$ is $\mathfrak{l}_{1,0}/13$, of valuation -1; times $13!\,1!$ it has valuation 0, whereas the rate of one variable in degree 14 is $\gamma_{13}\cdot 14 = 13/12$.

63.3. Six copies along an isotropic vector

Definition 63.3.1. A *tight frame* of length M consists of elements $w_\beta \in E$ and integers $c_\beta \ge 0$, β in a finite set, with $\sum_\beta c_\beta\,\tau'(w_\beta)\overline{\tau(w_\beta)} = M\delta_{\tau'\tau}$ for $\tau,\tau' \in \Phi$, each w_β lying in the lattice $\mathfrak{a}_0 := E \cap \alpha_0\hat{\mathcal{O}}_E$, α_0 the finite idele of the *Weil data* fixed with E in the proof. At η its forms are $\mu_\beta(z) := \sum_{\tau\in\Phi}\eta\bigl(c_{\mathrm{per}}\overline{\tau(w_\beta)}\bigr)z_\tau$, where c_{per} is the period factor of Definition 50.4.3 (not the Ω of Chapter 33). The *twelve copies* are the variables $z_{\tau,i}$, $\tau\in\Phi$, $1 \le i \le 12$, one coordinate of $\mathrm{Hom}(E, E^{12})$ at each infinite place and each of the twelve basis vectors; a multi-index on them is written $\mathbf{h} = (h_{\tau,i})$, and n copies are the variables $z_{\tau,i}$ with $i \le n$.

Tight frames. There is a tight frame of length M with $c_\beta \ge 6fb$ for every β such that for every prime p and every $\eta\colon \mathbb{C} \to \mathbb{C}_p$ some form μ_{β_0} has all its coefficients units. *Status*: read from the proof. Fix one; write $\mathfrak{o}$ for the valuation ring of $\mathbb{C}_p$, and $\mathfrak{o}[[y_{\mathrm{fr}}]]$ for the ring of series $G\big((y(\mu_\beta z))_\beta\big)$, G a power series over $\mathfrak{o}$ in one variable for each β.

Definition 63.3.2. Let $n \in \mathbb{N}$, ν a multi-index on Φ and $\rho \in \mathbb{R}$. We write $\mathrm{lv}_n(\nu) \le \rho$ if there are $H_1, \dots, H_n \in \mathfrak{o}[[y_{\mathrm{fr}}]]$ and multi-indices $\nu_1 + \cdots + \nu_n = \nu$ with $\sum_{i=1}^{n} \mathrm{val}\big([z^{\nu_i}](H_i \,\mathrm{th}_{\mathrm{fr}})\big) \le \rho$.

The next problems use six scalings to make the product of the theta factors a unit of $\mathfrak{o}[[y_{\mathrm{fr}}]]$.
Isotropic scalings. Write $\mathrm{th} = \exp(-g)$ with $g(0) = 0$. For every $\delta \in \mathbb{Z}_p$ the series $\exp\big(\delta^2 g(z) - g(\delta z)\big)$ lies in $\mathfrak{o}[[y]]$. *Status*: read from the proof. For $0 \ne \alpha \in \mathcal{O}_K$, multiplication by α is an isogeny of degree $\alpha\bar{\alpha}$ of $\mathbb{C}/\Lambda$ (complex multiplication; Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*, Ch. II). For every $\alpha \in \mathcal{O}_K$ the proof shows $\mathrm{th}(\alpha z) = \mathrm{th}(z)^{\alpha\bar{\alpha}} v$ with $v \in \mathfrak{o}[[y]]$, that is, $\exp(\alpha\bar{\alpha} g(z) - g(\alpha z)) \in \mathfrak{o}[[y]]$; it then passes to p-adic limits of the pairs $(\alpha, \alpha\bar{\alpha})$, among which are the pairs (δ, δ^2), $\delta \in \mathbb{Z}_p$.

Problem 63.3.1. $1 + 70^2 = 29 \cdot 13^2$; $(1, 70, 0, 0, 0, 0)$ is isotropic modulo 13^2; there is $\delta_2 \in \mathbb{Z}_{13}$ with $\delta_2 \equiv 70 \pmod{169}$ and $\delta_2^2 = -1$. For every prime p there are $\delta_2, \dots, \delta_5 \in \mathbb{Z}_p$ such that $\delta := (1, \delta_2, \delta_3, \delta_4, \delta_5, 0)$ has $\sum_{i=1}^{6} \delta_i^2 = 0$.

Problem 63.3.2. If $\delta \in \mathbb{Z}_p^6$ and $\sum_i \delta_i^2 = 0$, then $\prod_i \mathrm{th}(\delta_i z)$ lies in $\mathfrak{o}[[y]]$ with constant term 1, and $\prod_i \mathrm{th}_{\mathrm{fr}}(\delta_i z)$ is a unit of $\mathfrak{o}[[y_{\mathrm{fr}}]]$.

Problem 63.3.3. If μ_{β_0} has unit coefficients, then $\mathrm{lv}_6(\nu) \le \gamma_p|\nu| - \sum_\tau \mathrm{val}(\nu_\tau!)$ for every ν. For $\nu = (3, 6)$ on two places and $p = 3$: $\binom{9}{3} = 84$, $v_3(9!) = 4$ and $v_3(3!\,6!) = 3$.

Two more six-copy bounds are read from the proof. At an inert prime p, integral combinations of the forms give each coordinate times a unit, and then $\mathrm{lv}_6(\nu) \le 0$ for every ν. At an inert prime $p > 2$, from the normal form: let $\Phi_0 \subseteq \Phi$, odd positive integers e_τ for $\tau \in \Phi_0$ such that no (τ_1, e') with $\tau_1 \in \Phi_0$, $e' \le e_\tau$ an odd positive integer and $(\tau_1, e') \ne (\tau, e_\tau)$ has $[-p^{e'}]\tau_1 = [-p^{e_\tau}]\tau$, integers $j_\tau \ge 0$, $\nu' := \sum_{\tau \in \Phi_0} p^{e_\tau} j_\tau [\tau]$, $\nu'' := \sum_{\tau \in \Phi_0} j_\tau [[-p^{e_\tau}]\tau]$ and $J := \sum_{\tau \in \Phi_0} j_\tau$; then

$$\mathrm{lv}_6(\nu' + \nu'') \le \frac{J}{p-1} - J - \frac{|\nu' + \nu''|}{p^2 - 1} - \mathrm{val}(\nu''!),$$

where $[\tau]$ is the multi-index with a single 1 at τ and $\nu''! := \prod_\tau \nu''_\tau!$.

63.4. Near pairs

We now describe the pairs used at non-split primes $p \le k$. Let $l_0(s)$ be as in Definition 33.3.1.

Definition 63.4.1. Let p be a prime. A pair (τ, e) with $\tau \in \Phi$ is *near* at p if $e \in I_p$, $2e < l_0(s)$, $\tau \in \Phi_b$ and $[-p^e]\tau \in \Phi_b$; its *start* is τ and its *end* is $[-p^e]\tau$.

A model: the group $(\mathbb{Z}/13)^\times$ in place of Φ, $p = 3$ treated as inert, the cutoff $2e < 3$, and the heavy set $\{1, 10\}$ in place of Φ_b.

Problem 63.4.1. The iterates of $[-3]$ of orders 0 to 4 from 1 and from 10 are $(1, 10, 9, 12, 3)$ and $(10, 9, 12, 3, 4)$; the only near pair is $(1, 1)$, with end 10.

Problem 63.4.2. With weight 27 on $\{1, 10\}$ and 1 elsewhere, $\sum_\tau \sum_{e \text{ odd}} (\kappa(\tau)/3^e - \kappa([-3^e]\tau))_+ = 8$, the only nonzero term being $\tau = 10$, $e = 1$; the near pair $(1, 1)$ contributes 0.

Problem 63.4.3. Let $p \le k$ be a prime with $\chi_K(p) \ne 1$. (a) Two distinct near pairs at p have distinct starts and distinct ends, and the end of a near pair is never the start of one. (b) If $p = d$, there are no near pairs. Hence the near pairs at a prime $p \le k$ satisfy the hypothesis on Φ_0 in Section 63.3.

63.5. Twelve copies and the theorem

On twelve copies the proof combines the two kinds of six-copy bounds: at a split prime, Problem 63.3.3 on six copies and the constant coefficient in degree zero on the other six; at an inert $p > k$, every place coupled with its partner for $e = 1$ on six copies and the span bound on six; at a non-split $p \le k$, the near pairs on six copies and Problem 63.3.3 on six. For $\lambda\colon \Phi \to \mathbb{N}$ let $u := \lceil 6b/k \rceil$ and

$$\Pi_\tau := \prod_{i=1}^{u} \big((\lambda(\tau) - u)_+ + i \big),$$

a product of u consecutive integers; the reserved u pays for the rounding. The proof shows: if $\kappa(\tau) \le \lambda(\tau) \le \kappa(\tau) + x^{42}$ for every τ, then at every prime p and every η

$$\mathrm{lv}_{12}(\lambda) \le s^{\mathrm{tot}}_{\mathrm{fin},p} + 2 \sum_\tau \mathrm{val}(\Pi_\tau) - \sum_\tau \mathrm{val}(\lambda(\tau)!).$$

Status: read from the proof. The loss added to $s^{\mathrm{tot}}_{\mathrm{fin},p} - \sum_\tau \mathrm{val}(\lambda(\tau)!)$ is zero at split primes, $\sum_\tau \mathrm{val}(\Pi_\tau)$ at non-split $p \le k$, and $2 \sum_\tau \mathrm{val}(\Pi_\tau)$ at inert $p > k$.

Problem 63.5.1. $12 \cdot 13 \cdot 14 \cdot 15 = 32760$ has $v_{13} = 1$. A product of u consecutive integers has $v_p \ge \lfloor u/p \rfloor$.

Problem 63.5.2. If $\mathrm{lv}_n(\nu) \le \rho$, then the H_i in Definition 63.3.2 may be taken to be monomials $\prod_\beta y(\mu_\beta z)^{e_{i,\beta}}$ with $\sum_\beta e_{i,\beta} \le |\nu|$.

For a modulus $\mathfrak{m}$ of E (Definition 58.2.1) with ideal (π_M) and $y_0 \in (\mathcal{O}_E/\mathfrak{m})^{12}$, let Th_{y_0} be the theta function (the th_φ of Definition 50.4.3; in this sheet th is the theta function of the curve) of the datum on $\mathrm{Hom}(E, E^{12})$ with the Gaussian at infinity, the indicator of y_0 at the places dividing $\mathfrak{m}$, and the vacuum at the other finite places. For a vector F on $\mathrm{Hom}(E, E^{12})$ write $\mathrm{Jet}(F)$ for its jet series at scale $\pi_M c_{\mathrm{jet}}$; for F with the Gaussian at infinity, as the datum of y_0, this is the Taylor series at 0, in the twelve copies, of $z \mapsto \mathrm{Th}_F(\pi_M c_{\mathrm{jet}} z)$, as in Definition 50.4.3. Write Jet_{y_0} for this series for the datum of y_0. Two facts are read from the proof. First, if $3e_{i,\beta} \le c_\beta$ for all $i \le 12$ and all β, the product over the twelve copies of the series $\prod_\beta y(\mu_\beta z)^{e_{i,\beta}} \,\mathrm{th}(\mu_\beta z)^{c_\beta}$ is η applied to $\mathrm{Jet}(F)$ for a vector F on $\mathrm{Hom}(E, E^{12})$ whose values at finite arguments are integral at η and whose theta function is entire and fixed by the signed translations along $\pi_M \mathfrak{a}_0^{12}$, with $\mathfrak{a}_0$ as in Definition 63.3.1. Second, for such F, finite Fourier inversion writes $M^{12f} F$ as a finite sum $\sum_j c_j \cdot$ (translate of the vacuum) such that $|\eta(c_j v_*)| \le 1$ for every value v_* of the vacuum at a finite argument, and each translate is a sum over y_0 of roots of unity times the datum of y_0. *Status*: both are read from the proof; for background on algebraic

theta functions compare Bannai and Kobayashi, Duke Math. J. 153 (2010). Here the integral vacuum of $\mathrm{Hom}(E, E^{12})$ is c_{vac}^{12} times the vacuum (Section 34.8). Also read from the proof: every conjugate under $\mathrm{Aut}(\mathbb{C})$ of a value of the integral vacuum of $\mathrm{Hom}(E, E^{12})$ at a finite argument has absolute value at most $\exp(v_0 q_1^2)^{12}$.

Problem 63.5.3. Let $y_1, \dots, y_N \in \mathbb{C}_p$, $c_1, \dots, c_N$ with $|c_i| \le 1$, and $|\sum_i c_i y_i| \ge \epsilon_0 > 0$. Then $|y_i| \ge \epsilon_0$ for some i. Fix a modulus as above and a value c_* of the integral vacuum of $\mathrm{Hom}(E, E^{12})$ at a finite argument (with $\mathrm{val}(0) = +\infty$). If $\mathrm{lv}_{12}(\lambda) \le \rho$ and $c_\beta \ge 3|\lambda|$ for all β, there are $\mathbf{h}$ with $\sum_i h_{\tau,i} = \lambda(\tau)$ and y_0 with $\mathrm{val}\,\eta\big(c_{\mathrm{vac}}^{12}[z^{\mathbf{h}}]\mathrm{Jet}_{y_0}\big) \le \rho + \mathrm{val}\,\eta(M^{12f} c_*)$.

Fix a nonzero value c_* of the integral vacuum of $\mathrm{Hom}(E, E^{12})$ at a finite argument, before any modulus or prime is chosen, and put $c_{\mathrm{att}} := M^{12f}\, c_* \prod_\tau \Pi_\tau^2$. If $\lambda(\tau) \le \kappa(\tau) + x^{42}$ for every τ, then $|\lambda| \le f(b + x^{42}) \le 2fb$, so $c_\beta \ge 6fb \ge 3|\lambda|$.

Problem 63.5.4. If $\lambda(\tau) \le \kappa(\tau) + x^{42}$ for every τ, then for every $\sigma \in \mathrm{Aut}(\mathbb{C})$

$$\log|\sigma(c_{\mathrm{att}})| \le 12f \log M + 2fu \log(2b + u) + 12 v_0 q_1^2 \le \frac{fmb}{k}.$$

Problems 63.5.2, 63.5.3 and 63.5.4, with the bound on twelve copies (to which Problems 63.2.1, 63.3.3, 63.4.3 and 63.5.1 contribute), the tight frame and the two facts on theta functions, prove the following theorem.

Theorem 63.5.1. *Let $\lambda\colon \Phi \to \mathbb{N}$ satisfy $\kappa(\tau) \le \lambda(\tau) \le \kappa(\tau) + x^{42}$ for every τ. There is $c_{\mathrm{att}} \in \mathbb{C}$, $c_{\mathrm{att}} \ne 0$, with $|\sigma(c_{\mathrm{att}})| \le \exp(fmb/k)$ for every $\sigma \in \mathrm{Aut}(\mathbb{C})$, such that: for every modulus $\mathfrak{m}$ of E with ideal (π_M), every prime p and every ring homomorphism $\eta\colon \mathbb{C} \to \mathbb{C}_p$, there are a multi-index $\mathbf{h} = (h_{\tau,i})$ on the twelve copies with $\sum_i h_{\tau,i} = \lambda(\tau)$ for every τ, and a class $y_0 \in (\mathcal{O}_E/\mathfrak{m})^{12}$, with*

$$\mathrm{val}\ \eta\Big(c_{\mathrm{vac}}^{12}\, c_{\mathrm{att}}^{-1} \prod_{\tau \in \Phi} \lambda(\tau)! \cdot [z^{\mathbf{h}}]\,\mathrm{Jet}_{y_0}\Big) \le s_{\mathrm{fin},p}^{\mathrm{tot}}.$$

For fixed λ the same multiplier c_{att} works for all $\mathfrak{m}$, p and η; the witnesses $\mathbf{h}$, y_0 may depend on all three. Chapter 64 applies the theorem with λ the row λ_P of a critical pair main for j (Definitions 62.2.1 and 62.4.1), which satisfies the hypothesis by Problem 62.4.2.

Taken as given: the normal form, the isotropic scalings, the tight frame, the six-copy span and coupling bounds, the twelve-copy bound, the vacuum bound and the two facts on theta functions. The next sheet needs Theorem 63.5.1 and (1).

In the Lean formalization. In the Lean proof [GL] (readable edition, `BoundAttained.lean`), Theorem 63.5.1 is `Data.exists_rpow_neg_localPrimeSumTotal_le_norm_coeff`, stated with norms, Jet_{y_0} being `twelveTaylor` of `indicatorDatum` and $s_{\mathrm{fin},p}^{\mathrm{tot}}$ `Data.localPrimeSumTotal`. Definitions 63.3.2 and 63.4.1: `CMLattice.LeastValLE`, `Data.IsNearPair`. Normal form: `Data.exists_hasNormalForm_resolutionForms`. Isotropic scalings: `CMLattice.expSubst_sub_rescale_mem`, `CMLattice.prod_rescale_theta_mem`. Tight frame: `Data.exists_isTightFrame`. Coupling bound: `CMLattice.leastValLE_partnerDegree_of_isCo` Twelve copies: `Data.leastValLE_twelve`. The first fact on theta functions is `Data.exists_integral_isThetaFunction_twelveTaylor_eq`; the second is the Fourier expansion (`Space.exists_fourier_coefficients`) in the proof of `Data.exists_norm_le_norm_indicatorDatum`. The coefficient assertion in Problem 63.5.3 is `Data.exists_le_norm_coeff_indicatorDatum`. Further steps: `Data.mul_sum_weight_sub_localPrimeSumTotal`, `Parameters.cmCurve`,

`Parameters.periodFactor`, `Parameters.resolutionForms`, `CMLattice.leastValLE_of_unit_coefficients`, `Data.leastValLE_six_zero_of_inert`, `Data.isCouplingFamily_of_isNearPair`, `CMLattice.LeastValLE.exists_monomial`, `Parameters.norm_ringEquiv_intVacuum_le` and `Data.norm_map_mul_intVacuum_le`.

Hints

§63.1.

63.1.1: Problem 19.1.1, by machine.

63.1.2: Expand the exponential; for the integral series use Problem 19.4.2 and $\mu(6) \geq E_3(6)$.

63.1.3: By machine: the series of $F = \sigma^2 \wp$ through degree 52 from $\wp = \mathrm{sl}^{-2}$ and $(\log \sigma)'' = -\wp$ (Section 15.1), then $F(s+t)F(\zeta(s-t))$.

§63.2.

63.2.1: Compare term by term.

63.2.2: Euler's criterion.

§63.3.

63.3.1: Hensel's lemma at 13; for general p, Lagrange's theorem and the compactness of $\mathbb{Z}_p^4$.

63.3.2: Invert the one-variable product in $\mathfrak{o}[[y]]$, then substitute the forms.

63.3.3: Theorem 19.3.1 in total degree $|\nu|$ along μ_{β_0}, then specialize the six copies along an isotropic vector with first entry 1.

§63.4.

63.4.3: Start with (b): Φ_b lies in one class modulo q_0; compute d^e modulo q_0, using $d \equiv q_0/2 - 1$ and $4 \mid q_0$. For (a) at an inert prime, Problem 19.4.3 for Φ, $[-p]$, Φ_b, $L = l_0(s)$, the sparsity in Definition 33.3.1 and Problem 48.1.1.

§63.5.

63.5.2: As in Problem 19.1.1: truncate, and use the ultrametric inequality.

63.5.3: Separate the case $c_* = 0$. Otherwise apply the first part to the Fourier expansion multiplied by the vacuum value $c_*/c_{\mathrm{vac}}^{12}$, then to the expansion of a translate over the y_0; Problem 63.5.2 for the exponents.

63.5.4: Bound each factor of Π_τ by $2b + u$, and $|\sigma(c_*)|$ by the bound stated before Problem 63.5.3; for the last inequality use $M \leq b^{22}$, $k \leq r$ and the size conditions of Definition 33.3.1.

References

[GL] L. Sernau, *GRH for Dirichlet L-functions, in Lean 4*, a shorter rewriting of the Lean proof, text by Claude, `https://github.com/lsernau/grh-lean`, commit `72fead1`, readable edition `grh/`.

TEST FORMS AND THE HEIGHT OF A HECKE RATIO

Prerequisites. Characters of finite abelian groups; $\mathbb{C}_\ell$, $|\ell|_\ell = 1/\ell$. Chapter 5, Section 5.3: isomorphisms $\iota \mid \ell$, $|x|_\iota := |\iota(x)|_\ell$, families and the height ht, Problems 5.3.2 and 5.3.3, and the Fock norm of Problem 5.4.4. Chapter 29: congruence modules. Chapter 67, for the existence of regular families only. Chapter 33: the data, s_{fin}, s_∞, h_{dir} and the budget $B = U/(mk)$ (Definition 33.4.1). Chapter 34: twists, $\mathcal{M}$, χ_M, υ, c_{vac}, and critical pairs $P = (\nu, z)$ with their ratios $R_P(\xi, \epsilon)$ (Definition 34.10.1). Chapter 48: local prime sums, and forms integral at η (Section 48.3). Chapter 61: false lifts and clearing. Chapter 62: rows λ_P (Definition 62.2.1), main pairs and empty rows (Definition 62.4.1), $\phi_{P,\xi}$, $\mathrm{alg}_P(\xi)$ (Definition 62.3.1) and Theorem 62.4.1. Chapter 63: $s^{\mathrm{tot}}_{\mathrm{fin},p}$, the twelve copies, Theorem 63.5.1.

This chapter closes the cost of one lift, whose statement chapter is Chapter 60. There the height of the family $Z_j(1)/Z_j(\theta_\iota)$, for a regular family θ of m-fold twists, needs among other inputs a height bound for $\iota \mapsto R_P(\vartheta_\iota)^{-1}$, $\vartheta_\iota := \theta_\iota^j$, for the pairs P main for j in the factorization of the Hecke value product. By Theorem 62.4.1, $R_P(\vartheta)^{-1} = (\mathrm{Nm}\, Q_\vartheta)^{2z-1}\|\phi_{P,1}\|^2/\|\phi_{P,\vartheta}\|^2$; the untwisted squared norm has a height bound, and $\mathrm{alg}_P(\vartheta)$ is integral at $\ell \nmid \mathrm{Nm}\, Q_\vartheta$. How does the proof bound $|\|\phi_{P,\vartheta_\iota}\|^2|_\iota$ from below? With *test forms*: the lower bound (1) for their pairings with ϕ_{P,ϑ_ι} combines the sharp jet of Chapter 63 with an auxiliary Hecke ratio. We begin with a line in $\mathbb{C}^2$.

64.1. Two operations on heights

A height bound $\mathrm{ht}(y) \le c$ for a family $y = (y_\iota)$ is as in Section 5.3; products and powers are treated in Problem 5.3.2. We need two more operations.

Problem 64.1.1. Let $H \neq 0$ and $\alpha \in \mathbb{R}$ with $|\sigma H| \le e^\alpha$ for all $\sigma \in \mathrm{Aut}(\mathbb{C})$, and let $e(\ell) \in \mathbb{R}$, of any sign, one for each prime ℓ, with $|Hy_\iota|_\iota \le \exp(e(\ell))$ for all $\iota \mid \ell$ and $\alpha + \sum_{\ell \in F} e(\ell) \le c$ for every finite set F of primes. Then $\mathrm{ht}(y) \le c$.

Problem 64.1.2. If $\mathrm{ht}(y) \le c \le c''$ and $|y''_\iota|_\iota \le |y_\iota|_\iota$ for every $\iota \mid \ell$ and every prime ℓ, then $\mathrm{ht}(y'') \le c''$.

64.2. Two tests and a line

Let V be a finite-dimensional complex inner product space, conjugate-linear in the first variable, let $0 \neq v \in V$, and let pr be the orthogonal projection onto $\mathbb{C}v$.

Problem 64.2.1. For all $\Xi, \Xi' \in V$,

$$\langle \mathrm{pr}\,\Xi, \mathrm{pr}\,\Xi' \rangle = \frac{\langle \Xi, v\rangle\langle v, \Xi'\rangle}{\|v\|^2}.$$

Problem 64.2.2. In $V = \mathbb{C}^2$ with the standard inner product let $v = (1, 2)$, $\Xi = (1, 0)$ and $\Xi' = (0, 1)$. Then $\langle \Xi, v\rangle\langle v, \Xi'\rangle = 2$ and $\langle \mathrm{pr}\,\Xi, \mathrm{pr}\,\Xi'\rangle = 2/5$, so $|\langle \mathrm{pr}\,\Xi, \mathrm{pr}\,\Xi'\rangle|_\iota = 5$ for every $\iota \mid 5$, although v, Ξ and Ξ' have integral coordinates.

Date: November 26, 2026.

So projecting integral vectors to a line can create a denominator, a congruence in the sense of Chapter 29. Given an upper bound for $|\langle \operatorname{pr}\Xi, \operatorname{pr}\Xi'\rangle|_\iota$, a lower bound for $|\langle \Xi, v\rangle\langle v, \Xi'\rangle|_\iota$ gives one for $|\|v\|^2|_\iota$. For a critical pair $P = (\nu, z)$ with $z \geq 2$, Theorem 62.4.1(i) states that for every tame character ξ

$$R_P(\xi) = \frac{\|\phi_{P,\xi}\|^2/(\operatorname{Nm} Q_\xi)^{2z-1}}{\|\phi_{P,1}\|^2}.$$

Problem 64.2.3. Let $P = (\nu, z)$ be a critical pair with $z \geq 2$, ϑ a twist, $\operatorname{pr}_{P,\vartheta}$ the orthogonal projection onto $\mathbb{C}\phi_{P,\vartheta}$, Ξ, Ξ' forms with $\langle \Xi, \phi_{P,\vartheta}\rangle\langle \phi_{P,\vartheta}, \Xi'\rangle \neq 0$, and P' a critical pair with $R_{P'}(\vartheta) \neq 0$. Then

$$R_P(\vartheta)^{-1} = (\operatorname{Nm} Q_\vartheta)^{2z-1} \cdot \|\phi_{P,1}\|^2 \cdot \langle \operatorname{pr}_{P,\vartheta}\Xi, \operatorname{pr}_{P,\vartheta}\Xi'\rangle \cdot R_{P'}(\vartheta)^{-2} \cdot \frac{R_{P'}(\vartheta)^2}{\langle \Xi, \phi_{P,\vartheta}\rangle\langle \phi_{P,\vartheta}, \Xi'\rangle}.$$

In the application P is main for j, $\vartheta = \theta_\iota^j$ for a regular family θ, Ξ and Ξ' are test forms and P' is ramified; Problem 64.4.5 bounds the five factors.

Definition 64.2.1. Let $P = (\nu, z)$ be a critical pair with $z \geq 2$, ϑ a twist and ℓ a prime. A *test form for* ℓ (for P and ϑ) is a form Ξ in the space of forms of $\phi_{P,\vartheta}$, on the definite space of rank $2z$ (Definition 62.2.2), such that:

(1) Ξ is integral at every ring homomorphism $\eta\colon \mathbb{C} \to \mathbb{C}_\ell$ (Section 48.3);
(2) Ξ is orthogonal to the false lifts of the rank-one lift: for every finite place w of E with $\bar{w} \neq w$ that is not a place of the lift or the conjugate of one, Ξ is orthogonal to every form in the image of e_{X-1} that is killed by the Hecke polynomial at w at its test value (as in Definition 61.3.2) and by the descent, the adjoint of the lift. Here e_{X-1} is the idempotent with label $X - 1$ at every chosen place; since the source has rank one, it is the mean over $\prod_{w\in\mathcal{M}} k_w^\times$.

Let $\theta = (\theta_\iota)$ be a family of m-fold twists, one for every prime ℓ and every $\iota \mid \ell$.

Definition 64.2.2. The family θ has *small ratios* if (i) ℓ is prime to $\operatorname{Nm} Q_{\theta_\iota}$ for every $\iota \mid \ell$, and (ii) for every $1 \leq j \leq m$, every ramified critical pair P and $\epsilon = \pm 1$, the family $\iota \mapsto R_P(\theta_\iota^j, \epsilon)^{-1}$ has height at most x_1.

Definition 64.2.3. The family θ is *regular* if it has small ratios and (iii) for every $1 \leq j \leq m$ there are reals $\operatorname{cl}(\ell)$, one for each prime ℓ, with $\sum_{\ell\in F} \operatorname{cl}(\ell) \leq B$ for every finite set F of primes, such that for every $\iota \mid \ell$, with $\vartheta := \theta_\iota^j$: $\operatorname{cl}(\ell)$ clears the projection at (ι, ϑ, j) (Definition 61.3.4); and for every critical pair P main for j and any two test forms Ξ, Ξ' for ℓ for P and ϑ, $|\langle \operatorname{pr}_{P,\vartheta}\Xi, \operatorname{pr}_{P,\vartheta}\Xi'\rangle|_\iota \leq e^{\operatorname{cl}(\ell)}$.

That regular families exist is Theorem 67.2.1.

64.3. A large pairing from characters

Where does a test form with a large pairing come from? In the proof of (1) its pairing with $\phi_{P,\vartheta}$ is a scalar multiple of a normalized character sum of a theta kernel with twelve coordinates at each τ; after scaling, the value of the kernel at the identity is the coefficient estimated in Theorem 63.5.1. Two elementary facts carry the passage.

Problem 64.3.1. Let Cl be a finite abelian group of order N_c, $\operatorname{kn}\colon \mathrm{Cl} \to \mathbb{C}$, and for a character ψ of Cl let $\operatorname{av}_\psi := N_c^{-1} \sum_{g\in\mathrm{Cl}} \psi(g) \operatorname{kn}(g)$. Then $\sum_\psi \operatorname{av}_\psi = \operatorname{kn}(1)$,

the sum over all characters, and for every prime ℓ and every ring homomorphism $\eta\colon \mathbb{C} \to \mathbb{C}_\ell$ some ψ has $|\eta(\mathrm{av}_\psi)| \geq |\eta(\mathrm{kn}(1))|$. If $N_c = 2$ and kn is the indicator of 1, both av_ψ equal $1/2$, of 2-adic absolute value $2 \geq |\mathrm{kn}(1)|_2$.

Problem 64.3.2. Let G be a finite group, $\mathcal{A}_3, \mathcal{A}_1\colon G \to \mathbb{C}$, and $L_* \in \mathbb{C}$ with $L_*^{\#G} = \prod_{\chi \in G} \mathcal{A}_3(\chi)\mathcal{A}_1(\chi)$. Let $\eta\colon \mathbb{C} \to F_0$ be a ring homomorphism into a field with an absolute value. Then for every $\psi \in G$ there are $\chi_3, \chi_1 \in G$ with $\chi_3\chi_1 = \psi$ and $|\eta(\mathcal{A}_3(\chi_3)\mathcal{A}_1(\chi_1))| \geq |\eta(L_*)|$. For $G = \{1, \psi\}$, $\mathcal{A}_3 = (1, 9)$, $\mathcal{A}_1 = (9, 1)$ and $L_* = 9$, exactly one factorization of ψ satisfies the inequality for $|\cdot|_3$.

For a main pair the proof of (1) splits the $2z$ coordinates into blocks of sizes 12, 4, 4 and $2z - 20$: the jet lives on the first block, the twist on the second, and the last two carry auxiliary lifts.

Problem 64.3.3. For an integer $z \geq 2$, $12 + 4 + 4 + \max(2z - 20, 0) = 2z$ if and only if $z \geq 10$. For a pair main for j, $10000 \leq m < z \leq r$ and $4 \leq 2z - 20 \leq t$.

Let P be main for j, $\lambda := \lambda_P$ its row, and $\mathbf{h} = (h_{\tau,i})$ a multi-index on the twelve copies with $\sum_i h_{\tau,i} = \lambda(\tau)$ for every τ (Chapter 63). For the twelve coordinates of the first block the proof uses an integer vector in the Weyl representation of the lift; over every field of characteristic zero it is fixed by every family of invertible matrices fixing those twelve basis vectors at each τ, and its Fock polynomial in these coordinates is $T_{\mathbf{h}} X^{\mathbf{h}}$, with

$$T_{\mathbf{h}} := \prod_{\tau \in \Phi} \frac{\lambda(\tau)!}{\prod_{i=1}^{12} h_{\tau,i}!}.$$

This is read from the code [GL]. Give the polynomials in the $X_{\tau,i}$ the Fock inner product of Problem 5.4.4 in each variable: $\|X^{\mathbf{h}}\|^2 = \prod_{\tau,i} h_{\tau,i}!$, and monomials are orthogonal.

Problem 64.3.4. $T_{\mathbf{h}}$ is the coefficient of $X^{\mathbf{h}}$ in $\prod_\tau (X_{\tau,1} + \cdots + X_{\tau,12})^{\lambda(\tau)}$, and $T_{\mathbf{h}} \in \mathbb{Z}$. For a polynomial $f = \sum_{\mathbf{h}'} a_{\mathbf{h}'} X^{\mathbf{h}'}$, $\langle T_{\mathbf{h}} X^{\mathbf{h}}, f \rangle = \prod_\tau \lambda(\tau)! \cdot a_{\mathbf{h}}$. For one place, $\lambda = 13$ and $\mathbf{h} = (2, 1, \ldots, 1)$, $T_{\mathbf{h}} = 13!/2$.

Theorem 63.5.1, for λ with $\kappa(\tau) \leq \lambda(\tau) \leq \kappa(\tau) + x^{42}$ for every τ, gives $c_{\mathrm{att}} \in \mathbb{C}^\times$ with $|\sigma(c_{\mathrm{att}})| \leq \exp(fmb/k)$ for every $\sigma \in \mathrm{Aut}(\mathbb{C})$ such that for every modulus $\mathfrak{m}$ of E with ideal (π_M), every prime p and every ring homomorphism $\eta\colon \mathbb{C} \to \mathbb{C}_p$ there are $\mathbf{h}$ with $\sum_i h_{\tau,i} = \lambda(\tau)$ for every τ and $y_0 \in (\mathcal{O}_E/\mathfrak{m})^{12}$ with

$$\mathrm{val}\Big(\eta\Big(\frac{c_{\mathrm{vac}}^{12}}{c_{\mathrm{att}}} \prod_{\tau \in \Phi} \lambda(\tau)! \cdot [z^{\mathbf{h}}]\mathrm{Jet}_{y_0}\Big)\Big) \leq s_{\mathrm{fin},p}^{\mathrm{tot}}.$$

For a pair P main for j, the row λ_P satisfies these bounds (Problem 62.4.2).

Now the objects read from the proof [GL]. In this sheet $G_{\mathcal{M}}$ is the finite group of pairs ψ consisting of a continuous unitary character of the norm-one ideles of E, trivial on the norm-one elements of $E^\times$, of weight 0, and its tame part, which is trivial off $\mathcal{M}$; $\psi(g)$ is the value of the character at the norm-one idele given by a finite adelic point g of $U(1)$. For every $\psi \in G_{\mathcal{M}}$ and every even n with $4 \leq n \leq t$ there is a critical pair $(\nu, n/2)$ with empty row, of *rank* n (the rank $2z$ of the space of its lift, Definition 62.2.2), with the tame part of ψ, whose character becomes that of ψ after multiplication by $v^{n/2}$. For a pair $P = (\nu_P, z)$ main for j, let $P_\psi^{(4)}$ and

$P_\psi^{(2z-20)}$ be such pairs of ranks 4 and $2z-20$, and fix L_* with

$$L_*^{\#G_{\mathcal{M}}} = \prod_{\psi \in G_{\mathcal{M}}} \operatorname{alg}_{P_\psi^{(4)}}(1) \operatorname{alg}_{P_\psi^{(2z-20)}}(1).$$

For a pair P_0 with empty row, $\operatorname{alg}_{P_0}(1)$ is a positive real number (Chapter 62), and

$$|\sigma(\operatorname{alg}_{P_0}(1))| \le e^{x^{34}} \qquad \text{for every } \sigma \in \operatorname{Aut}(\mathbb{C});$$

this bound is read from the code [GL] and not proved in this workbook. Hence $L_* \neq 0$ and $|\sigma(L_*)| \le e^{2x^{34}}$ for every $\sigma \in \operatorname{Aut}(\mathbb{C})$. The classes of the finite adelic points of $U(1)$ modulo the rational points and the principal level at the chosen places form a finite abelian group Cl, of order N_c; every character of Cl has the form $g \mapsto \psi(g)$ for some $\psi \in G_{\mathcal{M}}$. Fix representatives g_c of the classes $c \in \mathrm{Cl}$.

The exact pairing. Let P be main for j, P' a critical pair with empty row of rank four, ℓ a prime, $\eta\colon \mathbb{C} \to \mathbb{C}_\ell$ a ring homomorphism and ϑ a twist with $\ell \nmid \operatorname{Nm} Q_\vartheta$. Let $\mathbf{h}$ and y_0 be given by Theorem 63.5.1 for $\lambda = \lambda_P$, (ℓ, η) and the modulus formed by the chosen places, with exponent one, whose ideal is (π_M). Write $\nu_{P'}$ for the character of P' and put $\chi_0 := (\nu_P/\nu_{P'})\, \upsilon^{z-2}$. Let $\mathrm{kn}(g)$ be the scalar theta kernel on the twelve-block, with characters 1 and χ_0, polynomial $X^{\mathbf{h}}$ and the indicator of y_0, evaluated at the point of $U(1)$ with finite part g and trivial archimedean part, and at the identity of $U(12)$. There is a number $c_{\mathrm{kn}} \neq 0$ such that $c_{\mathrm{kn}} \operatorname{kn}(1) = c_{\mathrm{vac}}^{12} c_{\mathrm{att}}^{-1} \prod_\tau \lambda_P(\tau)! \cdot [z^{\mathbf{h}}]\mathrm{Jet}_{y_0}$, so that $|\eta(c_{\mathrm{kn}} \operatorname{kn}(1))| \ge \ell^{-s^{\mathrm{tot}}_{\mathrm{fin},\ell}}$; and for every $\psi \in G_{\mathcal{M}}$, every factorization $\psi = \psi_3\psi_1$ in $G_{\mathcal{M}}$ and every finite adelic point g_0 of $U(1)$ there is a test form Ξ for ℓ for P and ϑ with

$$N_c^2 \langle \Xi, \phi_{P,\vartheta} \rangle = c_{\mathrm{att}} \operatorname{alg}_{P'}(1) \operatorname{alg}_{\psi_3,\psi_1} R_{P'}(\vartheta)\, c_{\mathrm{kn}} \operatorname{av}_{\psi,g_0}, \qquad \operatorname{av}_{\psi,g_0} := \frac{1}{N_c} \sum_{c \in \mathrm{Cl}} \psi(g_c g_0) \operatorname{kn}(g_c g_0),$$

where $\operatorname{alg}_{\psi_3,\psi_1} := \operatorname{alg}_{P_{\psi_3}^{(4)}}(1) \operatorname{alg}_{P_{\psi_1}^{(2z-20)}}(1)$. Here Ξ is a class sum, against the lift of P' at ϑ and the untwisted lifts of the two auxiliary pairs, of a point form with the integer vector above. *Status*: read from the code [GL] (see the remark at the end); not proved in this workbook.

Problem 64.3.5. Let P be main for j and P' a critical pair with empty row of rank four, and put $c_{\mathrm{test}} := c_{\mathrm{att}} \operatorname{alg}_{P'}(1)\, L_*$. Then $c_{\mathrm{test}} \neq 0$, $|\sigma(c_{\mathrm{test}})| \le \exp(fmb/k + 3x^{34})$ for every $\sigma \in \operatorname{Aut}(\mathbb{C})$, and for every prime ℓ, every ring homomorphism $\eta\colon \mathbb{C} \to \mathbb{C}_\ell$ and every twist ϑ with $\ell \nmid \operatorname{Nm} Q_\vartheta$ there is a test form Ξ for ℓ for P and ϑ with

$$|\eta(c_{\mathrm{test}}\, R_{P'}(\vartheta))| \cdot \ell^{-s^{\mathrm{tot}}_{\mathrm{fin},\ell}} \le |\eta\langle \Xi, \phi_{P,\vartheta} \rangle|. \tag{1}$$

64.4. The height of a Hecke ratio

Let θ be regular, $1 \le j \le m$, $P = (\nu, z)$ a critical pair main for j, and put $\vartheta_\iota := \theta_\iota^j$. Fix a ramified critical pair P' with empty row of rank four; the proof takes one whose tame part is that of χ_M and whose character becomes χ_M after multiplication by υ^2. Let c_{test} be as in Problem 64.3.5 for P and P'. The ratio $R_{P'}(\vartheta_\iota)$ is a positive real number.

Problem 64.4.1. Let $\iota \mid \ell$. There are test forms Ξ_ι, Ξ'_ι for ℓ for P and ϑ_ι such that, with $y_\iota := \langle \Xi_\iota, \phi_{P,\vartheta_\iota} \rangle \langle \phi_{P,\vartheta_\iota}, \Xi'_\iota \rangle$,

$$|c_{\mathrm{test}}\, c_{\mathrm{test}}^{-}\, R_{P'}(\vartheta_\iota)^2|_\iota \cdot \ell^{-2s^{\mathrm{tot}}_{\mathrm{fin},\ell}} \le |y_\iota|_\iota;$$

in particular $y_\iota \neq 0$.

For each ι fix such Ξ_ι, Ξ'_ι, and let y_ι be the resulting product.

Problem 64.4.2. For every finite set F of primes,

$$\sum_{p\in F} 2\, s^{\mathrm{tot}}_{\mathrm{fin},p} \log p \le \sum_{\tau\in\Phi} s_{\mathrm{fin}}(\kappa(\tau),\tau).$$

Problem 64.4.3. For the data, $fmb/k + 3x^{34} \le B$ and $x_1 \le B$.

Problem 64.4.4. The family $\iota \mapsto R_{P'}(\vartheta_\iota)^2/y_\iota$ has height at most $2B + \sum_{\tau\in\Phi} s_{\mathrm{fin}}(\kappa(\tau),\tau)$.

Problem 64.4.5. In Problem 64.2.3 at ϑ_ι, with Ξ_ι, Ξ'_ι and P', the five factors have $|(\mathrm{Nm}\, Q_{\vartheta_\iota})^{2z-1}|_\iota = 1$ and, as families in ι, heights at most $B - \sum_\tau s_\infty(\kappa(\tau))$, B, $2x_1$ and $2B + \sum_\tau s_{\mathrm{fin}}(\kappa(\tau),\tau)$ for the last four. The sum of these four bounds is $4B + 2x_1 - h_{\mathrm{dir}} \le 6B - h_{\mathrm{dir}}$.

Problems 64.2.3 and 64.4.1–64.4.5 prove the following.

Theorem 64.4.1. *Let θ be regular, $1 \le j \le m$, and P a critical pair main for j. Then the family $\iota \mapsto R_P(\theta^j_\iota)^{-1}$ has height at most $6B - h_{\mathrm{dir}}$.*

Problem 64.4.6. For the data, $6B < h_{\mathrm{dir}}$. So the bound of Theorem 64.4.1 is negative.

We have proved Theorem 64.4.1 from Theorems 62.4.1 and 63.5.1 and the exact pairing of Section 64.3, taken as an input with the auxiliary pairs, the conjugate bound for their algebraic parts, the integer vector on the twelve-block, and the finite class group Cl with the lifting of its characters to $G_{\mathcal{M}}$; the bounds on ramified ratios and on denominators of projections enter as the definition of regular families. By Problem 62.5.1, at ϑ_ι the inverse ratio of Hecke value products is, up to a unit at ℓ, the square of a product of $k/2$ factors $R_P(\vartheta_\iota)^{-1}$, P main, and $5m$ factors $R_{P'}(\vartheta_\iota,\epsilon)^{-1}$, P' ramified, with signs depending only on j; so its height is at most $k(6B - h_{\mathrm{dir}}) + 10mx_1$ (Problem 60.2.2).

In the Lean formalization. In the Lean proof [GL] (`grh/src/New/`), Theorem 64.4.1 is `Data.heightLe_inv_ratio`, whose proof also chooses P'; (1) is `Data.exists_isTestForm_le_norm_inner_trivialLift`, in whose proof are the group $G_{\mathcal{M}}$, the blocks, the classes Cl and the value $c_{\mathrm{kn}}\,\mathrm{kn}(1)$ (step `h_lower`); its step `h_inner` is the exact pairing for the choices made there. The exact pairing in general follows from `Data.exists_isTestForm_inner_kernelForm_eq`, `Data.modKernel_div_apply` and `LValueData.trivialLift_eq_stdClassSum_translate`. Test forms are `DescentPair.IsTestForm`; Definitions 64.2.2 and 64.2.3 are `Data.HasSmallRatios` and `Data.IsRegularFamily`. The auxiliary pairs come from `Data.exists_hasEmptyRow`, the bound $e^{x^{34}}$ is `Data.CriticalPair.norm_map_integralAlgebraicPart_le`, L_* is from `Data.exists_root_prod_integralAlgebraicPart`, the integer vector is `Rows.exists_int_weylRep_invariant_fockPoly_eq_smul_monomial`, and the lifting of characters of Cl is in `exists_norm_le_norm_twisted_classSum`.

Hints

§64.1.

64.1.1: Only the primes with $e(\ell) > 0$ cost anything.

64.1.2: Keep the multiplier H.

§64.2.

64.2.1: $\operatorname{pr}\Xi = (\langle v, \Xi\rangle/\|v\|^2)\, v$, and the first slot is conjugate-linear.

64.2.3: Theorem 62.4.1(i) at $\xi = \vartheta$, and Problem 64.2.1 for $\|\phi_{P,\vartheta}\|^2$.

§64.3.

64.3.1: $\sum_\psi \psi(g)$ is N_c or 0. For the second statement, $\mathbb{C}_\ell$ is ultrametric.

64.3.2: For fixed ψ, compare the product of $|\eta(\mathcal{A}_3(\psi\chi^{-1})\mathcal{A}_1(\chi))|$ over χ with its largest factor.

64.3.4: The multinomial theorem, and Problem 5.4.4 variable by variable.

64.3.5: Translate the representative of the identity class to 1. Which character and which factorization give the two lower bounds? Use $N_c \in \mathbb{Z}$ to control its local absolute value.

§64.4.

64.4.1: Keep the twist fixed. Which two maps $\mathbb{C} \to \mathbb{C}_\ell$ account for the two orders of the arguments of the inner product?

64.4.2: Problems 48.1.4 and 33.4.2; all terms are nonnegative.

64.4.3: $B = fxb\log^3 b/(mk)$. Use Definition 33.3.1 and Problem 33.3.2: $m^2 \le 4x$, $k \le r \le 3x^5$, $x^{10^6} \le x_1$ and $x_1^{10^6} \le b$.

64.4.4: Problem 64.1.1: which multiplier works at both embeddings? Then Problems 64.4.1, 64.4.2 and 64.4.3.

64.4.5: Match the four factors with Theorem 62.4.1(iii), clause (iii) of Definition 64.2.3 with Problem 5.3.3(a), clause (ii) of Definition 64.2.2 for P' squared (Problem 5.3.2) and Problem 64.4.4; then Problem 64.1.2.

64.4.6: $h_{\mathrm{dir}} \ge b\,\#\Phi_a$ (Problem 33.4.5), $f = \#\Phi_a\,\varphi(q_0)$ (Problem 33.2.2), and compare $6\varphi(q_0)x\log^3 b$ with mk.

References

[GL] L. Sernau, *GRH for Dirichlet L-functions, in Lean 4*, a shorter rewriting of the Lean proof, text by Claude, `https://github.com/lsernau/grh-lean`, commit `72fead1`, readable edition `grh/`.

DENOMINATORS OF PROJECTIONS TO LIFTS

Prerequisites. Discrete valuation rings and lengths of modules; the elementary divisor theorem. The Chebotarev density theorem and the Brauer–Nesbitt theorem [CR, (30.16)]. From Chapter 29, *Congruence modules*: the congruence module $\mathrm{C}(\,\cdot\,;\,\cdot\,)$ and Problems 29.1.1 and 29.1.2. From Chapter 30, *Eisenstein congruences and Selmer classes*: Problem 30.2.2 and Ribet's lemma, Theorem 30.2.1. From Chapter 24, *Hecke operators and theta lifts*: Section 24.4, with Problems 24.4.2 and 24.4.3. From Chapter 32: Section 32.3 on $X_0(11)$ and, for Section 65.4, the Weil data, the eigenforms and the attached representations of Section 32.4. For Section 65.3, Chapters 27 and 28 on Tate twists and odd classes; Chapter 31 is background. For Section 65.4, the data of Chapter 33; the single lifts $u_{\vartheta,j}$, the good forms and the twists of Chapter 34, whose notation we use; Definitions 61.3.2 and 61.3.4; ℓ-adic representations of Galois groups, crystalline representations and their Hodge–Tate weights, at the level of definitions.

To compare lifts at the trivial twist with lifts at a twist chosen for each $\iota \mid \ell$, one needs to control the denominators of the orthogonal projections of integral test forms onto spaces of lifts. How large can they be? In Chapter 29 the exponent of a congruence module gave the scalar denominator of a projection onto an eigenspace, and in Chapter 30 a congruence produced a Galois cohomology class. Here we measure a denominator by the determinant of an operator that clears it. Sections 65.1 and 65.2 are models, the second the smallest example, a class set with two elements; Section 65.3 describes the Galois side; Section 65.4 gives the definitions and the statement. Theorem 65.4.1 is read from the proof [GL]; of its bound, the local loss is developed in Chapter 66.

65.1. Clearing a projection

Let $\mathcal{O}$ be a discrete valuation ring with fraction field K and valuation ord, normalized by $\mathrm{ord}(\varpi) = 1$ for a uniformizer ϖ; we use $\mathrm{ord}(0) = +\infty$. Let V be a finite-dimensional K-vector space with a lattice L, and let $V = \mathcal{F} \oplus \mathcal{F}'$ with projection $\mathrm{pr}\colon V \to \mathcal{F}$ along $\mathcal{F}'$. Write $\mathrm{C}(L;\mathcal{F}) := \mathrm{pr}(L)/(L \cap \mathcal{F})$, as in Chapter 29. An operator $C_\ell \in \mathrm{End}_K(\mathcal{F})$ (the subscript recalls the prime ℓ of the later sections) *clears* pr on a subset $Y \subseteq L$ if $C_\ell(\mathrm{pr}(y)) \in L$ for every $y \in Y$. A scalar c clears pr on L when $c\,\mathrm{pr}(L) \subseteq L$; an operator may clear different directions of $\mathcal{F}$ by different amounts, and we measure it by $\mathrm{ord}(\det C_\ell)$.

Problem 65.1.1. C_ℓ clears pr on L if and only if $C_\ell(\mathrm{pr}(L)) \subseteq L \cap \mathcal{F}$. The least value of $\mathrm{ord}(\det C_\ell)$ over such C_ℓ is $\mathrm{len}_{\mathcal{O}}\,\mathrm{C}(L;\mathcal{F})$.

The operators that clear pr on a given Y form an $\mathcal{O}$-module; the definitions make sense for any valuation ring $\mathcal{O}$ and any $\mathcal{O}$-submodule L of V. The next problem combines clearing operators that are diagonal in one basis.

Problem 65.1.2. Let $\mathcal{O}$ be a valuation ring with infinite residue field and valuation ord, such as the ring of integers of $\bar{\mathbb{Q}}_\ell$ with $\mathrm{ord}(\ell) = 1$, and let $b_1, \dots, b_n$ be a

Date: November 26, 2026.

basis of $\mathcal{F}$. Let $C_\ell^{(1)}, \dots, C_\ell^{(n)}$ clear pr on Y, with $C_\ell^{(j)} b_i = \lambda_{ji} b_i$. Then some $C_\ell = \sum_j u_j C_\ell^{(j)}$ with $u_j \in \mathcal{O}$ has $C_\ell b_i = \mu_i b_i$ with $\operatorname{ord}(\mu_i) \le \operatorname{ord}(\lambda_{ii})$ for every i; it clears pr on Y.

Now let K be a subfield of $\mathbb{C}$ stable under complex conjugation, and $\mathcal{O}$ a discrete valuation ring with fraction field K. Let V carry a positive definite hermitian form $\langle\,,\rangle$, linear in the first variable, let $\mathcal{F}' = \mathcal{F}^\perp$, and let T be a self-adjoint operator on V with $T(L) \subseteq L$, diagonalizable with eigenvalues in $\mathcal{O}$, such that $\mathcal{F} \subseteq \ker(T - \lambda)$. The vectors of $\mathcal{F}^\perp$ with the eigenvalue of $\mathcal{F}$,

$$F_T := \mathcal{F}^\perp \cap \ker(T - \lambda),$$

are the *false lifts* for T. Let $\Pi(X) := \prod_\mu (X - \mu)$, the product over the eigenvalues $\mu \ne \lambda$ of T, each taken once.

Problem 65.1.3. For $y \in L$ orthogonal to F_T, $\Pi(T)\, y = \Pi(\lambda)\operatorname{pr}(y)$. Hence the scalar $\Pi(\lambda)$ clears pr on the $y \in L$ orthogonal to F_T, and the determinant of the scalar $\Pi(\lambda)$ acting on $\mathcal{F}$ has valuation $\dim \mathcal{F} \cdot \operatorname{ord}(\Pi(\lambda))$.

The cost $\operatorname{ord}(\Pi(\lambda)) = \sum_\mu \operatorname{ord}(\lambda - \mu)$ counts congruences between the eigenvalue of $\mathcal{F}$ and the other eigenvalues. The restriction to vectors orthogonal to the false lifts cannot be dropped.

Problem 65.1.4. Let $V = K^2$ with $\langle x, y\rangle = x_1\bar{y}_1 + x_2\bar{y}_2$, $L = \mathcal{O}^2$, $T = \lambda \cdot 1$, $\mathcal{F} = K(1,1)$, and suppose $\operatorname{ord}(2) > 0$. Then $F_T = K(1,-1)$, no unit $c \in \mathcal{O}^\times$ clears pr on L, and $c = 1$ clears it on the $y \in L$ orthogonal to F_T.

65.2. Two classes

We take the class set of Section 24.4 of Chapter 24: the two left ideal classes of a maximal order in the quaternion algebra over $\mathbb{Q}$ ramified at 11 and ∞, indexed by their right orders, with $w_1 = 2$ and $w_2 = 3$. Functions on the two classes are vectors $\varphi = (\varphi(1), \varphi(2))$, with

$$\langle \varphi, \varphi' \rangle := \frac{\varphi(1)\overline{\varphi'(1)}}{w_1} + \frac{\varphi(2)\overline{\varphi'(2)}}{w_2},$$

and the Brandt matrix $B(\ell)$, for a prime $\ell \ne 11$, acts by $(B(\ell)\varphi)(i) = \sum_j B_{ij}(\ell)\varphi(j)$. Recall from that section that $B(\ell)$ has integer entries, that $w_j B_{ij}(\ell) = w_i B_{ji}(\ell)$ and $\sum_j B_{ij}(\ell) = \ell + 1$, and that $B(\ell)$ is the action of T_ℓ on $M_2(\Gamma_0(11))$, which is spanned by an Eisenstein series of T_ℓ-eigenvalue $\ell + 1$ and by the form called f there; we write

$$f_{11} := q \prod_{n \ge 1} (1 - q^n)^2 (1 - q^{11n})^2 = \sum_{n \ge 1} a_n q^n.$$

By Problem 24.4.2, $B(2) = \begin{pmatrix} 1 & 2 \\ 3 & 0 \end{pmatrix}$ and $B(3) = \begin{pmatrix} 2 & 2 \\ 3 & 1 \end{pmatrix}$. The constant function 1 plays the role of the lifts: $\mathcal{F}$ is the line of constant functions, and pr is the orthogonal projection onto $\mathcal{F}$. The integral functions are $L := \mathbb{Z}^2$. To apply Section 65.1 over $\mathbb{Z}_{(\ell)}$, use the lattice $\mathbb{Z}_{(\ell)}^2$ in $\mathbb{Q}^2$. Over $\mathbb{Q}_\ell$ use the lattice $\mathbb{Z}_\ell^2$ and the same bilinear formula without the bar.

Problem 65.2.1. $B(\ell)$ is self-adjoint for $\langle\,,\rangle$, $B(\ell)1 = (\ell+1)1$, and $\varphi_{11} := (2, -3)$ spans $\mathcal{F}^\perp$ and satisfies $B(\ell)\varphi_{11} = a_\ell \varphi_{11}$.

Problem 65.2.2. $\mathrm{pr}(\varphi) = \frac{1}{5}\big(3\varphi(1) + 2\varphi(2)\big) \cdot 1$, and $5\,\mathrm{pr} = B(2) + 2 = B(3) + 1$. Hence $\mathrm{pr}(L) = \frac{1}{5}\mathbb{Z} \cdot 1$ and $\mathrm{C}(L; \mathcal{F}) \cong \mathbb{Z}/5\mathbb{Z}$. The least value of $\mathrm{val}_5(\det C_\ell)$ for C_ℓ clearing pr on $\mathbb{Z}_5^2$ is 1; for $\ell \neq 5$ the identity clears pr on $\mathbb{Z}_\ell^2$. The scalar $\Pi(\lambda)$ of Problem 65.1.3 is 5 both for $T = B(2)$ and for $T = B(3)$.

What congruence do the Brandt eigenvalues satisfy?

Problem 65.2.3. $B(\ell) - a_\ell = (\ell + 1 - a_\ell)\mathrm{pr}$. Hence $a_\ell \equiv 1 + \ell \pmod 5$ for every prime $\ell \neq 11$; for example $a_{13} = 4$ (Problem 32.3.1).

The denominator 5 is the numerator of the mass $1/w_1 + 1/w_2 = (11-1)/12 = 5/6$. The next problem gives the denominator at primes dividing none of the weights.

Problem 65.2.4. Let I be a nonempty finite set with positive integers w_i, let $\langle \varphi, \varphi' \rangle := \sum_i \varphi(i)\varphi'(i)/w_i$ on $\mathbb{Q}_\ell^I$, let $\mathcal{F}$ be the line of constant functions, and let ℓ be a prime dividing no w_i. Then $\mathfrak{m} := \sum_i 1/w_i$ has $\mathrm{val}_\ell(\mathfrak{m}) \geq 0$, and $\mathrm{C}(\mathbb{Z}_\ell^I; \mathcal{F}) \cong \mathbb{Z}/\ell^{\mathrm{val}_\ell(\mathfrak{m})}\mathbb{Z}$.

For the quaternion algebra ramified at a prime p and ∞ the mass is $(p-1)/12$, and Mazur showed that the index of his Eisenstein ideal is the numerator of $(p-1)/12$ [Ma]. There is also an integrality question for the pairing of a cleared form with an integral form.

Problem 65.2.5. In the setting of Problem 65.2.4, drop the condition on ℓ, and let n_0 be a common multiple of the w_i. If C_ℓ clears pr on $Y \subseteq \mathbb{Z}_\ell^I$, then so does $n_0 C_\ell$, and $\langle n_0 C_\ell \mathrm{pr}(y), \varphi' \rangle \in \mathbb{Z}_\ell$ for $y \in Y$ and $\varphi' \in \mathbb{Z}_\ell^I$. In the class set with two elements, $6\langle \varphi, \varphi' \rangle \in \mathbb{Z}$ for $\varphi, \varphi' \in \mathbb{Z}^2$.

65.3. Lifts and the classes they produce

Where does the congruence of Problem 65.2.3 come from? The constant function carries the Galois representation $1 \oplus \chi_{\mathrm{cyc}}$, where χ_{cyc} is the 5-adic cyclotomic character; its trace at an arithmetic Frobenius Frob_ℓ is $1 + \ell$ for $\ell \neq 5$. The form f_{11} carries the representation ρ_{11} of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ on the rational 5-adic Tate module $T_5(X_0(11)) \otimes \mathbb{Q}_5$, whose trace at Frob_ℓ is a_ℓ for $\ell \nmid 55$ (Section 32.3 of Chapter 32). Let ω be the reduction of χ_{cyc} modulo 5.

Problem 65.3.1. The semisimplification of the reduction of ρ_{11} modulo 5 is $1 \oplus \omega$, and $\omega(c) = -1$ for every complex conjugation c.

The representation ρ_{11} is irreducible: it is semisimple and its commutant is $\mathbb{Q}_5$, by Faltings' theorem [Fa], since $X_0(11)$ has no complex multiplication (its j-invariant $-122023936/161051$ is not an integer). Ribet's lemma, Theorem 30.2.1, then gives a nonzero class with values in $\mathbb{F}_5(\omega)$ or $\mathbb{F}_5(\omega^{-1})$, an odd character.

In the general setting a single theta lift takes values in forms on a standard definite unitary space for the CM extension E/E^+. For a main summand R for a pair $\mathfrak{O}_0$ and a family $\mathfrak{s}$, take a pair $\mathfrak{O}$ with the same basis index sets for its two spaces and with character that of $\mathfrak{O}_0$ times a tame character ξ. The normalization S of any representation attached to a lift eigenform for $\mathfrak{s}$ on $\mathfrak{O}$ satisfies $\mathrm{tr}\, S(g) = \hat{\xi}(g)\,\mathrm{tr}\, R(g) + \sum_{0 \leq e < t'} \chi_{\mathrm{cyc}}(g)^{-e}$ for every $g \in \mathrm{Gal}(\bar{\mathbb{Q}}/E)$. Here t' is the rank difference, χ_{cyc} is the ℓ-adic cyclotomic character, and $\hat{\xi}$ is the inverse avatar of ξ (Definitions 65.4.5 and 65.4.8). The constant function above has this shape, with no R and two characters, after a twist by the inverse 5-adic cyclotomic character.

For an extension of $\chi_{\mathrm{cyc}}^{-e'}$ by χ_{cyc}^{-e} modulo ℓ^ν, the extension cocycle takes values in $(\mathcal{O}/\ell^\nu)(-a)$, where $a = e - e'$. On cocycles z of $\mathrm{Gal}(\bar{\mathbb{Q}}/E)$ a complex conjugation c acts by $z^c(g) := z(cgc)$; call z *odd* if $z^c = -z$ and *even* if $z^c = z$.

Problem 65.3.2. Let ℓ be odd and $\mathcal{O}$ the ring of integers of a finite extension of $\mathbb{Q}_\ell$. Every cocycle of $\mathrm{Gal}(\bar{\mathbb{Q}}/E^+)$ with values in $(\mathcal{O}/\ell^\nu)(-a)$ differs by a coboundary from one with $z(c) = 0$. For such z, the restriction to $\mathrm{Gal}(\bar{\mathbb{Q}}/E)$ satisfies $z^c = (-1)^a z$.

For odd ℓ and odd a, restriction from $\mathrm{Gal}(\bar{\mathbb{Q}}/E^+)$ to $\mathrm{Gal}(\bar{\mathbb{Q}}/E)$ therefore gives classes with odd representatives. For the CM field $E \subseteq \mathbb{Q}(\mu_{q_1 d})$ of Chapter 33, let $d_{q_1 d}$ be the exponent of $(\mathbb{Z}/(q_1 d)\mathbb{Z})^\times$. Theorem 27.3.2, proved using Gauss sums as in Chapter 28, gives one positive integer X_{odd} that works simultaneously for every prime ℓ, every ring of integers $\mathcal{O}$ of a finite extension of $\mathbb{Q}_\ell$ containing a primitive $d_{q_1 d}$-th root of unity, every integer $0 \le a < t$ and every integer $\nu \ge 0$. For $a > 0$ the $\mathcal{O}$-length of the module of continuous odd cocycles of $\mathrm{Gal}(\bar{\mathbb{Q}}/E)$ with values in $(\mathcal{O}/\ell^\nu)(-a)$, unramified off ℓ and zero on the kernel of χ_{cyc} in every decomposition group above ℓ, is at most $\mathrm{ord}_{\mathcal{O}}(X_{\mathrm{odd}})$, with a uniformizer of order 1. For $a = 0$ the same bound holds for the everywhere unramified continuous homomorphisms with values in $\mathcal{O}/\ell^\nu$. Definition 65.4.1 contains no order of a group of even classes. A class can be tested by its values at Frobenius elements; here is an example, for a Kummer class.

Problem 65.3.3. Let ℓ be an odd prime, $u \in \mathbb{Q}^\times$ not an ℓ-th power, and kum_u the Kummer class of u in $H^1(\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}), \mu_\ell)$. For a prime $q \equiv 1 \pmod{\ell}$ with $\mathrm{val}_q(u) = 0$, kum_u is unramified at q, and $\mathrm{kum}_u(\mathrm{Frob}_q) = 0$, a condition independent of the choice of Frob_q, if and only if $u^{(q-1)/\ell} \equiv 1 \pmod{q}$. There are infinitely many such q with $\mathrm{kum}_u(\mathrm{Frob}_q) \neq 0$. For $\ell = 3$ and $u = 2$, $q = 7$ detects kum_2 and $q = 31$ does not.

Ribet's lemma needs an element on which the two characters differ (Problem 30.2.2). For the characters χ_{cyc}^{-e}, $0 \le e < t$, with χ_{cyc} the ℓ-adic cyclotomic character, the cost of an element g is the valuations of the differences $\chi_{\mathrm{cyc}}(g)^a - 1$, $0 < a < t$. If $\chi_{\mathrm{cyc}}(g)$ reduces to a generator of $\mathbb{F}_\ell^\times$ and $t \le \ell - 1$, these valuations are 0, by Problem 65.3.4. If g is an arithmetic Frobenius element at a chosen place w not dividing ℓ (Section 34.1), then $\chi_{\mathrm{cyc}}(g) = \#k_w$ and these valuations are at most $\mathrm{val}_\ell(\mathcal{N})$, by Problem 65.3.5 with $n = rt$: the integer $\mathcal{N}$ of that section is a multiple of $\#\mathrm{GL}_{rt}(k_w)$.

Problem 65.3.4. Let $g \in \mathbb{Z}_\ell^\times$ reduce to a generator of $\mathbb{F}_\ell^\times$. Then $g^a - 1 \in \mathbb{Z}_\ell^\times$ for $0 < a < \ell - 1$.

Problem 65.3.5. Let q be a prime power and $1 \le a \le n$. Then $q^a - 1$ divides $\#\mathrm{GL}_n(\mathbb{F}_q) = q^{n(n-1)/2} \prod_{i=1}^n (q^i - 1)$.

65.4. The statement

We use the data of Chapter 33: the CM field E with f infinite places, the rank r, $t = 5r$, the numbers m and k, the level primes p_0, p_1 with $M = p_0 p_1$, the level N, the moduli q_1 and d, and the budget B of Definition 33.4.1. From Chapter 34 we use the chosen places $\mathcal{M}$, labels, the good idempotent e_0 and the integer $\mathcal{N}$ (Section 34.1), the gap $\Delta = 2r^8$ and the weights κ_j of the lifts (Section 34.2), tame

characters ξ and twists ϑ with their sets Q_ξ, Q_ϑ (Section 34.6), and the single lifts $u_{\vartheta,j}$ on good forms (Section 34.9).

Fix a prime ℓ and a ring isomorphism $\iota\colon \mathbb{C} \simeq \bar{\mathbb{Q}}_\ell$. As in Chapter 34, val is the valuation of $\bar{\mathbb{Q}}_\ell$ with $\mathrm{val}(\ell) = 1$ and $\mathrm{val}(0) = \infty$, read through ι on complex numbers, and $\mathrm{val}_+ := \max(\mathrm{val}, 0)$. A form y is *integral at* ι if for every finite adelic point g the gauge of $y(g)$ at g is at most 1. To compute this gauge, use ι followed by $\bar{\mathbb{Q}}_\ell \subset \mathbb{C}_\ell$ on the weight coordinates, apply g^{-1} in the representation of that weight, and take the largest ℓ-adic absolute value of a resulting coordinate. At an infinite place τ with chosen CM-type embedding Φ_τ, the adelic action is read through $x \mapsto \iota(\Phi_\tau(\bar{x}))$ at the induced ℓ-adic place. The field E is embedded in $\bar{\mathbb{Q}}$, and $G_E := \mathrm{Gal}(\bar{\mathbb{Q}}/E)$; with c the complex conjugation of $\bar{\mathbb{Q}}$ fixed in the proof, $g^c := cgc$ for $g \in G_E$; and χ_{cyc} is the ℓ-adic cyclotomic character. For a place of $\bar{\mathbb{Q}}$ above a finite place w of E not dividing ℓ, s_w denotes its distinguished generator of tame inertia; it depends on the place of $\bar{\mathbb{Q}}$.

A *coefficient ring* $\mathcal{O}$ is the ring of integers of a finite Galois extension of $\mathbb{Q}_\ell$ in $\bar{\mathbb{Q}}_\ell$, and a statement holds *for all large* $\mathcal{O}$ if it holds for all coefficient rings containing a fixed one. The *normalized length* of an $\mathcal{O}$-module of finite length is its length divided by the ramification index $e_\mathcal{O}$ of $\mathcal{O}$ over $\mathbb{Z}_\ell$; so $\mathcal{O}/\ell$ has normalized length 1, and the normalized length does not change when $\mathcal{O}$ is enlarged and the module extended. An $\mathcal{O}$-module of infinite length has normalized length $+\infty$.

Definition 65.4.1. Let $n_\ell := \mathrm{val}_\ell(\mathcal{N})$ and $o_\ell := \mathrm{val}_\ell(X_{\mathrm{odd}})$, where X_{odd} is the integer that the proof fixes for the length bound of Section 65.3, with $0 < X_{\mathrm{odd}} \le 2^{4(q_1 d+t+3)^{27}} h_E$ and h_E the class number of E. Let $\mathrm{loc}_\ell = 4f\,\mathrm{defect}_\ell$ be the local loss of Definition 66.1.1, and put

$$\mathrm{tw}_\ell := (4f+3)\,r\,n_\ell + 2^{-\ell}, \qquad \varepsilon_\ell := t\,o_\ell + 8ft\,n_\ell + 2n_\ell + \big((4t+1)(\Delta/2)^{22} + \Delta/2\big)n_\ell.$$

The *clearing bound* is $\mathrm{cl}_\ell := \mathrm{loc}_\ell + (1+2t)\,\mathrm{tw}_\ell + \varepsilon_\ell + n_\ell$.

Definition 65.4.2. A *descent pair* $\mathfrak{D}$ has two finitely indexed families of finite places of E, chosen places and twist places; all their entries are distinct, and none is the conjugate of any entry. It has a hermitian space W of rank r' with signs on its basis indices and a specified adelic frame in which its Gram matrix is the diagonal matrix of the signs at every infinite place and the identity at every finite place, a natural number assigned to each index, an injection of those indices into the basis indices of the standard definite space $V = I_{n'}$ with $r' < n'$ (its image is the set of *selected* indices), column multiplicities $k^{\pm}(\tau, i)$ at each infinite place τ and height $i \ge 0$, and a continuous unitary character μ of $U(1)(\mathbb{A})$, trivial on rational points, with specified integral weight at each infinite place and specified tame part, a character ψ_w of $k_w^\times$ at each finite place w, trivial off the two families. Write K_0 for the stabilizer of the standard integral lattice of V in the finite adelic group. The *level* of $\mathfrak{D}$ consists of the elements of K_0 whose reductions fix the selected basis vectors at the chosen places and preserve the span of the other basis vectors at the twist places. Its *level character* is the product over the twist places w of ψ_w^{-1} applied to the determinant of the block on the selected indices. Its forms $\mathcal{A}(\mathfrak{D})$ are the algebraic forms on V on which the level acts through the level character, of the weight with column multiplicities $k^+(\tau, i) + k^-(\tau, n' - i)$ at τ and each height $0 \le i < n'$, and with determinant exponent $-\sum_{1 \le i < n'} k^-(\tau, i)$ at τ. We write $t' := n' - r'$ for its rank difference.

Definition 65.4.3. Let e_1 be an element of the complex group algebra of $\prod_w \mathrm{GL}_{r'}(k_w)$ over the chosen places of $\mathfrak{O}$, and $A \subseteq \mathcal{A}(\mathfrak{O})$ a subspace. A tuple $g = (g_w)_w$ of this group acts on $\mathcal{A}(\mathfrak{O})$ by right translation by an element of K_0 that reduces to g_w on the selected block and to the identity on the other block at each chosen place w, and to the identity at the twist places, multiplied by $\prod_w \psi_w(\det g_w)$; write $\mathrm{im}(e_1)$ for the image of the operator by which e_1 then acts. In this sheet υ_E is the splitting character of the Weil data on the ideles of E (Section 32.4), and υ is its restriction to the norm-one ideles, as in Section 34.7. For a character a of the norm-one ideles and a natural number $N_0 \geq 0$, the *Frobenius value* of a in rank N_0 at a finite place w is $q_w^{N_0/2}$ times the value, at the finite idele with the chosen uniformizer at w and 1 elsewhere, of the Hecke character $x \mapsto a(x/\bar{x})\,\upsilon_E(x)^{-N_0}$; here $q_w = \#k_w$. For a split place w such that neither w nor $\bar{w}$ is a place of $\mathfrak{O}$, the *false lifts* at w are the forms in $\mathrm{im}(e_1) \cap A$ killed by the Hecke polynomial operator of $\mathfrak{O}$ at w at the value $\left(\nu_w q_w^{n'-r'-1}\right)^{-1}$ expected of a lift, where ν_w is the Frobenius value at w of υ^{r_-} in rank r', with r_- the number of negative signs of W. A form is *orthogonal to the false lifts* for $(\mathfrak{O}, e_1, A)$ if it is orthogonal to the false lifts at every such w.

Definition 65.4.4. Let e_1 be as in Definition 65.4.3, $\mathcal{F} \subseteq \mathcal{A}(\mathfrak{O})$ a subspace, with orthogonal projection pr, and $\mathrm{den} \in \mathbb{R}$. The projection onto $\mathcal{F}$ has *denominator at most* den at ι if some operator C_ℓ on $\mathcal{F}$ has $|\iota(\det C_\ell)|_\ell \geq \exp(-\dim \mathcal{F} \cdot r' \cdot \mathrm{den})$ and, for every form y integral at ι and orthogonal to the false lifts for $(\mathfrak{O}, e_1, \mathcal{F}^\perp)$, $C_\ell(\mathrm{pr}(y))$ is integral at ι and $|\iota\langle C_\ell(\mathrm{pr}(y)), y'\rangle|_\ell \leq 1$ for every form y' integral at every ring map $\mathbb{C} \to \mathbb{C}_\ell$. Here $\langle\,,\rangle$ is the class sum of the pointwise Gram inner products, linear in the first variable; each term is weighted by the reciprocal of the order of the stabilizer of its double-coset representative.

For a twist ϑ and $1 \leq j \leq m$, take the j-th descent pair of ϑ, $e_1 = e_0$ and $\mathcal{F}$ the image of $u_{\vartheta,j}$. Then the false lifts are those of Definition 61.3.2, and the condition of Definition 65.4.4, without the bound on the pairings $\langle C_\ell(\mathrm{pr}(y)), y'\rangle$, says that den clears the projection at (ι, ϑ, j) in the sense of Definition 61.3.4.

Definition 65.4.5. The *inverse avatar* of a tame character ξ is the ℓ-adic avatar $\hat{\xi}\colon G_E \to \bar{\mathbb{Q}}_\ell^\times$, through ι, of the base change of ξ^{-1} to E: the continuous character with $\hat{\xi}(\mathrm{Art}\, x) = \iota\big(\xi(x/\bar{x})\big)^{-1}$ for every finite idele x of E, where Art is the Artin map. We use the Artin map of the proof, with values in the topological abelianization G_E^{ab} and with a local uniformizer mapping to geometric Frobenius modulo inertia. A character of G_E is evaluated there through the induced character. Let $\mathrm{ram} \in [0, \infty]$. A twist ϑ is *auxiliary with ramification at most* ram (at ι) if:

(a) every place of Q_ϑ has prime norm, and neither it nor its conjugate divides ℓMN (its conjugate is not in Q_ϑ, as for every tame character);
(b) $\hat{\vartheta}$ is locally constant, and there is a character η of the finite ideles of E, with values in $\bar{\mathbb{Q}}_\ell^\times$, such that $\hat{\vartheta}(\mathrm{Art}\, x) = \eta(x/\bar{x})$ for every finite idele x, and η is trivial on $E^\times$ and on every idele that is a unit at the places not above ℓ and is congruent to 1 at the places of Q_ϑ;
(c) for some choice of a place of $\bar{\mathbb{Q}}$ above each $w \in Q_\vartheta$, with tame generators s_w, $\sum_{w \in Q_\vartheta} \mathrm{val}_+\big(\hat{\vartheta}(s_w) - 1\big) \leq \mathrm{ram}$.

Definition 65.4.6. Let r' and t' be natural numbers. A family $\mathrm{HT} = (\mathrm{HT}_\sigma)$ of finite multisets of integers, one for each embedding $\sigma\colon E \to \mathbb{C}$, is *admissible for* (r', t') if:

(i) $1 \le r' \le r$ and $t' \le t$;
(ii) there is one $0 \le j \le m$ such that, for every σ, every $u \in \mathrm{HT}_\sigma$ satisfies $\Delta/4 \le |u| \le 2m\Delta$ or $|s_\sigma u + \kappa_j([\sigma])| \le t$; here $[\sigma]$ is the infinite place of σ, and $s_\sigma = \pm 1$ is the sign of σ for the CM type, that is, $\sigma(\sqrt{-d}) = s_\sigma\sqrt{-d}$;
(iii) $k \cdot \#\{u \in \mathrm{HT}_\sigma : |u| \le 2(\Delta/2)^2\} \le r'm$ for every σ, the members counted with multiplicity;
(iv) HT_σ and $\mathrm{HT}_{\bar\sigma}$ together have at most r' negative members, for every σ.

The members of HT_σ are called *jumps*.

Definition 65.4.7. Let $t' \ge 0$ be an integer, HT a family as in Definition 65.4.6, and $R\colon G_E \to \mathrm{GL}_{r'}(\bar{\mathbb{Q}}_\ell)$ a homomorphism. A *lattice of R over $\mathcal{O}$* is a homomorphism $G_E \to \mathrm{GL}_{r'}(\mathcal{O})$ conjugate to R by an element of $\mathrm{GL}_{r'}(\bar{\mathbb{Q}}_\ell)$. The representation R is *main-summand-like for* (t', HT) if:

(a) R is continuous, the trace pairing on the span of its image is nondegenerate, and $\operatorname{tr} R(g^c) = \chi_{\mathrm{cyc}}(g)^{-\max(t'-1,0)} \operatorname{tr} R(g^{-1})$ for every $g \in G_E$;
(b) at every place A of $\bar{\mathbb{Q}}$ above every finite place w of E: if $w \nmid \ell$, R is trivial on the elements of the inertia group in a neighbourhood of 1; if $w \mid \ell$, the restriction of R to the decomposition group is potentially crystalline for every local datum at A, that is, every embedding e of $\bar{\mathbb{Q}}$ in $\bar{\mathbb{Q}}_\ell$ inducing A, with the induced embedding of its decomposition group into $\mathrm{Gal}(\bar{\mathbb{Q}}_\ell/\mathbb{Q}_\ell)$, and for every such datum and every $g \in \mathrm{Gal}(\bar{\mathbb{Q}}_\ell/\mathbb{Q}_\ell)$ its Hodge–Tate jumps at the coefficient embedding induced by g are, with multiplicity, the multiset HT_σ for $\sigma = \iota^{-1} \circ g^{-1} \circ e|_E$; and if $w \nmid M$, R is unramified ($w \nmid \ell$), respectively crystalline for every local datum ($w \mid \ell$);
(c) HT is admissible for (r', t');
(d) at every place of $\bar{\mathbb{Q}}$ above every $w \mid M$ with $w \nmid \ell$ there are an element δ of the inertia group and a natural number n_w prime to the residue characteristic such that $R(s^{n_w}) = 1$ for every inertia element s there, δ is the tame generator s_w if $w \in \mathcal{M}$, and $\operatorname{val}_+ \det(R(\delta) - 1) \le r'n_\ell$, $\operatorname{val}_+ \det\bigl(R((\delta^c)^{-1}) - 1\bigr) \le r'n_\ell$;
(e) for all large $\mathcal{O}$, the image of every lattice of R over $\mathcal{O}$ spans $M_{r'}(\mathcal{O})$ over $\mathcal{O}$; and for all large $\mathcal{O}$ and every lattice of R over $\mathcal{O}$, some $g \in G_E$ with $\chi_{\mathrm{cyc}}(g) \in \{p_0^{r'}, p_1^{r'}\}$ acts on it by a scalar;
(f) some element of an inertia group above a place dividing M and not dividing ℓ acts through R by a scalar y with $|y^{\ell^a j} - 1|_\ell = 1$ for all integers $a \ge 0$ and $1 \le j \le 4r' + 2$.

The Hodge–Tate jumps are taken in the convention of the proof, in which the cyclotomic character has jump -1.

Definition 65.4.8. Let $\mathfrak{s} = (\mathfrak{s}(w, i))$ be a family of complex numbers indexed by the finite places w of E and the integers $i \ge 0$. A form $y \in \mathcal{A}(\mathfrak{O})$ *lifts* $\mathfrak{s}$ if, at every split place w such that neither w nor $\bar w$ is a place of $\mathfrak{O}$, it is spherical and for every $T \in \mathbb{C}$ the Hecke polynomial operator at w at the value T sends y to y multiplied

by

$$\prod_{0\le i<t'} \bigl(1-q_w^i\,\nu_W T\bigr)\cdot H_{\mathfrak{s}(w)}\bigl(q_w^{t'}\nu_W T/\nu_V\bigr), \qquad H_{\mathfrak{s}(w)}(T) := \sum_{i=0}^{r'} (-T)^i q_w^{i(i-1)/2}\,\mathfrak{s}(w,i),$$

where ν_W and ν_V are the Frobenius values at w of υ^{r_-} in rank r' and of $\mu\,\upsilon^{\lfloor n'/2\rfloor}$ in rank n', respectively, as in Definition 65.4.3. A homomorphism $R\colon G_E \to \mathrm{GL}_{r'}(\bar{\mathbb{Q}}_\ell)$ is a *main summand* for a descent pair $\mathfrak{O}_0$ of ranks $r' < n'$ and $\mathfrak{s}$ if it is main-summand-like for $(n'-r', \mathrm{HT})$ for some HT, and

$$\operatorname{tr} S(g) = \hat{\xi}(g)\operatorname{tr} R(g) + \sum_{0\le e<n'-r'} \chi_{\mathrm{cyc}}(g)^{-e} \qquad (g\in G_E)$$

for every tame character ξ, every descent pair $\mathfrak{O}$ with the same basis index sets for W and for V as $\mathfrak{O}_0$ and with character μ that of $\mathfrak{O}_0$ times ξ, every form in $\mathcal{A}(\mathfrak{O})$ lifting $\mathfrak{s}$, every family P of polynomials for which that form is an eigenform, and every representation attached to P (Section 32.4). Here S, the *normalization* of that representation for $\mathfrak{O}$, is its twist by the ℓ-adic avatar, through ι, of the Hecke character $x \mapsto \upsilon^{-r_-}(x/\bar{x})\,\upsilon_E(x)^{r'}\,|x|^{r'/2}$, with r_- taken for $\mathfrak{O}$ and $|x|$ the idelic norm.

Definition 65.4.9. Let $R\colon G_E \to \mathrm{GL}_{r'}(\bar{\mathbb{Q}}_\ell)$ be a homomorphism, ξ a tame character, $g_*\in G_E$ and $\mathrm{sel}\in[0,\infty]$. Let L be a lattice of R over a coefficient ring $\mathcal{O}$ containing the values of $\hat{\xi}$, and L_{tw} the module $\mathcal{O}^{r'}$ on which $g\in G_E$ acts by $\hat{\xi}(g)L(g)$. For each $v\mid\ell$, let G_v be the decomposition group of the chosen place above v and use the local embedding of G_v into $\mathrm{Gal}(\bar{\mathbb{Q}}_\ell/\mathbb{Q}_\ell)$ fixed in the proof. In the crystalline relations below, an integral crystalline cocycle means a function $z_0\colon G_v\to L_{\mathrm{tw}}$ for which some $b_0\in B_{\max}\otimes_{\mathbb{Z}_\ell} L_{\mathrm{tw}}$ satisfies $1\otimes z_0(g) = gb_0 - b_0$ for every $g\in G_v$. Here $B_{\max}$ is the crystalline period ring of the proof, and G_v acts on the tensor product through its local embedding on $B_{\max}$ and through L_{tw} on the second factor. Then $\mathrm{Sel}(L_{\mathrm{tw}}, g_*)$ is the $\mathcal{O}$-module of locally constant maps $z\colon G_E\to L_{\mathrm{tw}}\otimes_{\mathcal{O}}(\mathrm{Frac}(\mathcal{O})/\mathcal{O})$ such that: $z(gh) = z(g) + g\,z(h)$ for all g,h; z vanishes on the inertia groups above the finite places of E that neither divide ℓM nor lie in $Q_\xi\cup\bar{Q}_\xi$; z satisfies the *crystalline relations*, that is, for each $v\mid\ell$ and every finite family of $g_i\in G_v$ and $a_i\in M_{r'}(\mathcal{O})$ such that $\sum_i a_i\,z_0(g_i)=0$ for every integral crystalline cocycle $z_0\colon G_v\to L_{\mathrm{tw}}$, also $\sum_i a_i\,z(g_i)=0$; and $z(g_*)=0$. The twist $\hat{\xi}R$ *has Selmer bound* sel if there are an element g_* of an inertia group above a place of E not dividing ℓ and an integer ζ of $\bar{\mathbb{Q}}_\ell$ such that, for all large $\mathcal{O}$, there is a lattice L of R over $\mathcal{O}$ for which $\zeta\in\mathcal{O}$, $\zeta-1\in\mathcal{O}^\times$, g_* acts on L_{tw} by the scalar ζ, and $\mathrm{Sel}(L_{\mathrm{tw}}, g_*)$ has normalized length at most sel.

Definition 65.4.10. A descent pair $\mathfrak{O}$ with a tuple of polynomials over the residue fields of its chosen places is in *lift setting* for ϑ if its indexed chosen and twist places agree with those of the data and of ϑ; its tame part is the j-th power of the tame part of χ_M from Section 34.7, times the tame part of ϑ, for some $1\le j\le m$; r' and $n'-r'$ are odd, with $r'\le r$ and $n'-r'\le t$; each polynomial is a label of degree r' (Section 34.1), and none of its roots becomes 1 on multiplication by the element of $k_w^\times$ naming the inverse tame character of $\mathfrak{O}$ at its place w; and above each p_i one polynomial is primitive with $r'=r$, or equal to $X-1$ with $r'=1$.

Definition 65.4.11. Let ϑ be a twist, $\mathfrak{O}$ a descent pair, e_1 as in Definition 65.4.3, $\mathcal{F} \subseteq \mathcal{A}(\mathfrak{O})$ a subspace and $\mathrm{sel} \in [0,\infty]$. A *lift generator* for $(\vartheta, \mathfrak{O}, e_1, \mathcal{F})$ with Selmer bound sel is a form $y \in \mathcal{F}$ such that:

(a) y lies in the range of the idempotent of a tuple of polynomials with which $\mathfrak{O}$ is in lift setting for ϑ (Definition 65.4.10), and the whole range of this idempotent is contained in $\mathrm{im}(e_1)$;

(b) y lifts a family $\mathfrak{s}$ for which there are a descent pair $\mathfrak{O}_0$ with the same basis index sets for W and for V as $\mathfrak{O}$, whose character μ times ϑ is that of $\mathfrak{O}$, and a main summand R for $\mathfrak{O}_0$ and $\mathfrak{s}$ such that $\hat{\vartheta}R$ has Selmer bound sel (Definition 65.4.9).

Theorem 65.4.1. *Let ℓ and ι be as above, and let ϑ be a twist that is auxiliary with ramification at most tw_ℓ. Let $\mathfrak{O}$ be a descent pair of ranks $r' < n'$, e_1 an element of the complex group algebra of $\prod_w \mathrm{GL}_{r'}(k_w)$ over its chosen places, and $\mathcal{F} \subseteq \mathcal{A}(\mathfrak{O})$ a subspace contained in the span of the lift generators for $(\vartheta, \mathfrak{O}, e_1, \mathcal{F})$ with Selmer bound tw_ℓ. Then the projection onto $\mathcal{F}$ has denominator at most $\mathrm{cl}_\ell \log \ell$ at ι, in the sense of Definition 65.4.4.*

Status: read from the proof [GL]; not proved here. The next three problems are arithmetic of the clearing bound and of determinants.

Problem 65.4.1. Let r', t' be integers with $1 \le r' \le r$ and $0 \le t' \le t$, and let $0 \le \mathrm{sel}, \mathrm{ram} \le \mathrm{tw}_\ell$. Then

$$\mathrm{sel} + 2t'\,\mathrm{ram} + r'\,\mathrm{loc}_\ell + \varepsilon_\ell + n_\ell \le r'\mathrm{cl}_\ell.$$

Problem 65.4.2. Let $\mathcal{F}$ be a finite-dimensional complex vector space, $n_0 \ge 0$ an integer, $u_0 \ge 0$, and $C_\ell \in \mathrm{End}_{\mathbb{C}}(\mathcal{F})$ with $\mathrm{val}(n_0\iota(\mu)) \le u_0$ for every eigenvalue μ of C_ℓ. Then, with $|\ell|_\ell = \ell^{-1}$, $|\iota(\det(n_0 C_\ell))|_\ell \ge \exp(-\dim \mathcal{F} \cdot u_0 \log \ell)$.

Problem 65.4.3. The sum of $2^{-\ell}\log\ell$ over all primes ℓ is $0.3776\ldots$, and for every finite set P_0 of primes, $\sum_{\ell\in P_0} \mathrm{tw}_\ell \log\ell \le (4f+3)\, r \log \mathcal{N} + 0.378$.

The clearing bounds of all primes together fit the budget B: the proof bounds by B the sum in Problem 65.4.4. Let C_1 be the number of $U(1)$ double cosets at the chosen level. In Chapter 67 the allowance for the pairing on the rank-one lifts is $(\mathrm{cl}_\ell + \mathrm{val}_\ell(C_1))\log\ell$ (Section 67.2). With x the length of the prime sum and b the weight scale of Chapter 33, consider the following five comparisons.

$$\log\bigl(2^{4(q_1 d+t+3)^{27}} h_E\bigr) \le x^{2000}, \qquad (4f+3)\, r \log\mathcal{N} + 2 \le x^{999}, \qquad \log C_1 \le x^{30},$$

$$t\, x^{2000} + \bigl(8ft + 2 + (4t+1)(\Delta/2)^{22} + \Delta/2\bigr)\log\mathcal{N} \le x^{4000},$$

$$4\cdot 10^6 e^{180} f\, \frac{m}{k}\, b\log b + (1+2t)\, x^{999} + x^{4000} + \log\mathcal{N} + x^{30} \le B.$$

Problem 65.4.4. Granting the five displayed inequalities, for every finite set P_0 of primes

$$\sum_{\ell\in P_0} \bigl(\mathrm{cl}_\ell + \mathrm{val}_\ell(C_1)\bigr)\log\ell \;\le\; 4\cdot 10^6 e^{180} f\, \frac{m}{k}\, b\log b + (1+2t)\, x^{999} + x^{4000} + \log\mathcal{N} + x^{30} \;\le\; B.$$

By Theorem 61.3.1(b), for a twist ϑ of modulus prime to ℓ, a real $\mathrm{cl}(\ell)$ that clears the projection at (ι, ϑ, j) bounds the ℓ-adic norm, through ι, of the determinant of the compression of a comparison operator to the image of $u_{\vartheta,j}$ by $\exp(\dim_{\mathbb{C}} H_g(W_j)\cdot r\cdot \mathrm{cl}(\ell))$. For $1 \le j \le m$, $e_1 = e_0$ and $\mathcal{F}$ the image of $u_{\vartheta,j}$, so that $r' = r$, the proof

deduces from Theorem 65.4.1 that every real $\mathrm{cl}(\ell) \geq \mathrm{cl}_\ell \log \ell$ clears the projection at (ι, ϑ, j) in the sense of Definition 61.3.4, provided ϑ is auxiliary with ramification at most tw_ℓ and every eigensystem occurring in a nonzero good form on W_m has a main summand, for the j-th descent pair of the trivial twist, whose twist by $\hat{\vartheta}$ has Selmer bound tw_ℓ. Chapter 67 chooses an m-fold twist θ_ι for each $\iota \mid \ell$, and at index j one takes $\vartheta = \theta_\iota^j$. Of the terms of cl_ℓ, Chapter 66 develops the local loss loc_ℓ and proves the bound for its sum (Theorem 66.4.1); Theorem 65.4.1 itself is taken from the proof.

In the Lean formalization. In the Lean proof [GL] (`grh/src/`, with the namespace `New.` omitted), Definition 65.4.1 is `Selmer.clearingBound`, with X_{odd} the integer `Selmer.oddClassBound`; Definitions 65.4.2–65.4.4 are `DescentPair`, `DescentPair.falseLiftsAt` (the value at the chosen uniformizer is `HeckeChar.atUniformizer`) and `Selmer.DenominatorLe`; Definitions 65.4.5–65.4.11 are `Selmer.IsAuxTwist` for `Selmer.badPlaces`, Q_ϑ and $\hat{\vartheta}$, with `Data.TameChar.invAvatar` and its formula `Selmer.invAvatar_eq_of_artinMap_eq` for the Artin map `artinMap`, `Selmer.IsMainSummandWeights`, `Selmer.IsMainSummandLike` (the jumps are those of `Period.jump`), `Selmer.IsMainSummand` (its eigenform and attachment conditions are `IsEigenform` and `GaloisRep.Attached`), the existential closure in g_*, ζ of `Selmer.HasDivisibleSelmerLengthLe` with modulus Q_ξ, `Selmer.IsLiftSetting` and `Selmer.IsLiftGenerator`. The module in Definition 65.4.9 has ordinary length `Selmer.crystallineSelmerLength` and uses `Selmer.crysRelations`; its local embedding and period ring are those of `Selmer.localChart` and `Period.crysCocycles`. Theorem 65.4.1 is `Selmer.denominatorLe_clearingBound`, and the good-lift case is `Selmer.denominatorLe_range_goodLift`, followed by `Selmer.DenominatorLe.clearsProjection` for the passage to $\mathrm{cl}(\ell) \geq \mathrm{cl}_\ell \log \ell$. The two inequalities of Problem 65.4.4 occur in the calculation of `Selmer.sum_clearingBound_add_padicValNat_le`, which states the bound by B for all admissible data and all finite sets of primes.

Hints

§65.1.

65.1.1: C_ℓ maps $\mathcal{F}$ to $\mathcal{F}$. For the minimum, $\mathrm{pr}(L)$ and $L \cap \mathcal{F}$ are lattices in $\mathcal{F}$; use elementary divisors.

65.1.2: Choose the u_j generically modulo the maximal ideal.

65.1.3: Decompose y into eigenvectors of T; $\ker(T-\lambda) = \mathcal{F} \oplus F_T$ is orthogonal to the other eigenspaces.

§65.2.

65.2.1: Apply the balance and row-sum identities to the two orthogonal lines.

65.2.2: Apply the projection onto constants to the coordinate functions; then Problem 65.1.1.

65.2.3: Compare both sides on a basis.

65.2.4: Compute pr on the indicator functions.

65.2.5: Inspect each weight in the class sum.

§65.3.

65.3.1: The characteristic polynomial of $\rho_{11}(\mathrm{Frob}_\ell)$ is $X^2 - a_\ell X + \ell$ for $\ell \nmid 55$ (Section 32.3 of Chapter 32). Reduce on the lattice $T_5(X_0(11))$; ρ_{11} is

unramified outside 55. Use Problem 65.2.3, the Chebotarev density theorem and the Brauer–Nesbitt theorem for characteristic polynomials.

65.3.2: Evaluate the cocycle relation on $c\cdot c = 1$ and on $c\cdot g\cdot c$, using $\chi_{\mathrm{cyc}}(c) = -1$.

65.3.3: $\mathrm{kum}_u(\mathrm{Frob}_q)$ is read off from the action of Frob_q on $u^{1/\ell}$ modulo a prime above q. Since u is not an ℓ-th power, $[\mathbb{Q}(u^{1/\ell}) : \mathbb{Q}] = \ell$, so $\mathbb{Q}(\mu_\ell, u^{1/\ell})/\mathbb{Q}(\mu_\ell)$ has degree ℓ, as $\gcd(\ell, \ell-1) = 1$; apply the Chebotarev density theorem to its nontrivial elements.

§65.4.

65.4.1: Use $r' \geq 1$ and $t' \leq t$.

65.4.3: Use the factorization of $\mathcal{N}$. For the prime sum, sum through 31 and bound the rest by $\sum_{k>31} k\,2^{-k}$.

65.4.4: Sum the four terms of cl_ℓ separately. For loc_ℓ use Theorem 66.4.1; for tw_ℓ, Problem 65.4.3; for ε_ℓ, n_ℓ and $\mathrm{val}_\ell(C_1)$, the inequality $\sum_{\ell\in P_0} \mathrm{val}_\ell(n)\log\ell \leq \log n$ for an integer $n \geq 1$, with the bound for X_{odd} of Definition 65.4.1.

References

[CR] C. W. Curtis and I. Reiner, *Representation Theory of Finite Groups and Associative Algebras*, Interscience, 1962.

[Fa] G. Faltings, *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern*, Invent. Math. **73** (1983), 349–366.

[GL] L. Sernau, *GRH for Dirichlet L-functions, in Lean 4*, a shorter rewriting of the Lean proof, text by Claude, `https://github.com/lsernau/grh-lean`, commit `72fead1`, readable edition `grh/`.

[Ma] B. Mazur, *Modular curves and the Eisenstein ideal*, Publ. Math. IHÉS **47** (1977), 33–186.

THE LOCAL LOSS AND THE SPARSE PLACES

Prerequisites. Local fields: decomposition groups, the degree $[E_v : \mathbb{Q}_\ell] = e_v f_v$, Frobenius elements [SLF, Ch. I, IV]; Legendre's formula $\mathrm{val}_\ell(n!) = \sum_{i\ge1}\lfloor n/\ell^i\rfloor$. From Chapter 33: Definition 33.3.1 (the sparse set Φ_b, $l_0(s)$), Problems 33.1.1, 33.1.2, 33.2.1 and 33.5.4, and the budget B of Definition 33.4.1; the construction of Φ_b in Chapter 4. Theorem 31.4.1. From Chapter 65: coefficient rings $\mathcal{O}$ and normalized lengths (Section 65.4), Definitions 65.4.6, 65.4.7 and 65.4.1. p-adic Hodge theory enters only through three results stated in the text.

The clearing bound cl_ℓ of Definition 65.4.1, which controls the denominators of projections onto lifts in Chapter 65, contains the term loc_ℓ, counted per unit of rank; a main summand of rank r' pays $r'\mathrm{loc}_\ell$ (Problem 65.4.1): the price of asking that the cocycles produced by a congruence be crystalline above ℓ. Why is this price the valuation of one integer, and why is the sum of $\mathrm{loc}_\ell \log \ell$ over all primes ℓ only of size $f(m/k)\, b \log b$, far below B? The bound at one place above ℓ is taken from the proof. What this sheet proves is the arithmetic around it: the sum over the places and rows, the integer whose valuation is the loss, the sparse places that keep the small primes cheap, and the sum over ℓ. For a prime ℓ and a positive integer n we write $\mathrm{val}_\ell(n)$ for the exponent of ℓ in n, the valuation val at ℓ.

66.1. The loss at one place

We use the data and the notation of Chapter 33: the field E with f infinite places, the scales, m, r, $k = r + 1 - m$, $t = 5r$, $M = p_0p_1$, the gap $\Delta = 2r^8$, so $\Delta/2 = r^8$.

Definition 66.1.1. Let Int_b be the product of the integers i with $\max(0, b - 30(\Delta/2)^3) < i \le b + 30(\Delta/2)^3$. For a prime ℓ put

$$\mathrm{crys}_\ell := \mathrm{val}_\ell\big((2b)!\,\mathrm{Int}_b^{(\Delta/2)^3}\big), \qquad \mathrm{defect}_\ell := 10^6\,\frac{m}{k}\,\big(b\ \mathrm{val}_\ell(M) + \mathrm{crys}_\ell\big),$$

and $\mathrm{loc}_\ell := 4f\,\mathrm{defect}_\ell$.

Fix a prime ℓ, an isomorphism $\iota\colon \mathbb{C} \simeq \overline{\mathbb{Q}}_\ell$, and $G_{\mathbb{Q}_\ell} := \mathrm{Gal}(\overline{\mathbb{Q}}_\ell/\mathbb{Q}_\ell)$. For a place $v \mid \ell$ of E choose an embedding $\jmath\colon E \to \overline{\mathbb{Q}}_\ell$ inducing v, and let $\Gamma_v \subseteq G_{\mathbb{Q}_\ell}$ be the subgroup fixing $\jmath(E)$, the Galois group of the completion E_v; thus $[G_{\mathbb{Q}_\ell} : \Gamma_v] = [E_v : \mathbb{Q}_\ell]$. In the proof of the denominators theorem, a congruence produces cocycles that obey the relations among the $U_i(g) - 1$; by Theorem 31.4.1 such a cocycle is the second coordinate of an integral cocycle on a lattice. It need not be crystalline above ℓ. The failure is priced on the dual side, and a finite model shows why the price is the same on both sides.

Problem 66.1.1. Let $F_1 \times F_2 \to \mathbb{Q}/\mathbb{Z}$ be a perfect pairing of finite abelian groups and $F_0 \subseteq F_1$ a subgroup. Its orthogonal $F_0^\perp \subseteq F_2$ has index $\#F_0$. For $F_1 = F_2 = \mathbb{Z}/9$ with $\langle y_1, y_2\rangle = y_1y_2/9$ and F_0 generated by 3, $F_0^\perp = \{0, 3, 6\}$, of index 3: one equation costs length 1 on either side.

Date: November 26, 2026.

For a lattice with continuous action of Γ_v, write $Z_f(\cdot)$ for its integral crystalline cocycles. The proof uses three results of p-adic Hodge theory. (i) *Local duality in index form.* Let L, L' be potentially crystalline $\mathbb{Z}_\ell$-lattices with Γ_v-action in perfect equivariant duality $L' \times L \to \mathbb{Z}_\ell(1)$, let $n \geq 1$, red: $L \to L/\ell^n L$, and let $\mathcal{Q}$ be a group of maps $\Gamma_v \to L'$ whose cup products modulo ℓ^n with $\mathrm{red} \circ y$ for all $y \in Z_f(L)$, and with all members of a group $\mathcal{S}$ of continuous cocycles $\Gamma_v \to L/\ell^n L$, are coboundaries. Then $[\mathcal{S} : \mathcal{S} \cap \mathrm{red}\, Z_f(L)]$ divides $[Z_f(L') : Z_f(L') \cap \mathcal{Q}]$. The finite statement behind it is local Tate duality [SGC, II, §5.2, Thm. 2], [ADT, I.2.3]; the crystalline subgroups are exact annihilators of each other [BK, Prop. 3.8]. *Status*: classical in these forms; the integral form stated is read from the proof. (ii) *Bloch–Kato.* For a potentially crystalline $\mathbb{Z}_\ell$-lattice L with Γ_v-action, $Z_f(L)$ is a finite free $\mathbb{Z}_\ell$-module of rank $\mathrm{rk}_{\mathbb{Z}_\ell} L + [G_{\mathbb{Q}_\ell} : \Gamma_v] \cdot n^-$, where n^- is the number of negative Hodge–Tate jumps of L at the inclusion $\mathbb{Q}_\ell \subset \mathbb{C}_\ell$, counted with multiplicity [BK, §3]. *Status*: classical; the integral form is read from the proof. (iii) The bound (1) below. It rests on integral p-adic Hodge theory [Ki], [BMS, §4], and is read from the proof.

Definition 66.1.2. Let $\mathcal{O}$ be a coefficient ring, $\mathcal{C}$ a class of $\mathcal{O}$-lattices with continuous Γ_v-action, and L' such a lattice. In this sheet let $\mathcal{C}^\perp(L')$ be the $\mathcal{O}$-module of maps $c\colon \Gamma_v \to L'$ such that for every $\tilde{L} \in \mathcal{C}$, every $n \geq 0$, every pairing $\langle\,,\rangle\colon \tilde{L} \times L' \to \mathbb{Z}/\ell^n(1)$ obtained from an $\mathcal{O}$-linear form $\psi\colon \tilde{L} \otimes L' \to \mathcal{O}(1)$ whose coboundary $g \mapsto g\psi - \psi$ is ℓ^n times an integral crystalline cocycle, followed by a $\mathbb{Z}_\ell$-linear map $\mathcal{O} \to \mathbb{Z}_\ell$ and reduction modulo ℓ^n, and every $y \in Z_f(\tilde{L})$, the cochain $(g,h) \mapsto \langle y(g), g\,c(h)\rangle$, with values in the roots of unity of $\overline{\mathbb{Q}}_\ell$, is the coboundary of a continuous cochain $\Gamma_v \to \overline{\mathbb{Q}}_\ell^{\times}$. The *dual defect* of L' for $\mathcal{C}$ is the length of $Z_f(L')/(Z_f(L') \cap \mathcal{C}^\perp(L'))$. The *dual defect at* v of a lattice L is the dual defect of its Tate dual $L^*(1)$, in normalized length.

Let R be main-summand-like for (t', HT) (Definition 65.4.7). The *rows* at v are a Γ_v-stable $\mathcal{O}$-lattice L_0 in R, of rank r' and jumps HT, and the characters $\mathcal{O}(-e) = \chi_{\mathrm{cyc}}^{-e}$ for $0 \leq e < t'$, of rank 1. Let $\mathcal{C}$ be a class adapted to the rows: its lattices have jumps among those of the rows, and it consists of crystalline lattices or, when $\ell \in \{p_0, p_1\}$, of lattices of a fixed tame type. The proof shows: given R and v, for all large $\mathcal{O}$, for every choice of the rows at v over $\mathcal{O}$ and every class $\mathcal{C}$ of $\mathcal{O}$-lattices adapted to them, every row L in $\mathcal{C}$ has dual defect at v at most

$$[G_{\mathbb{Q}_\ell} : \Gamma_v]\ \mathrm{rk}(L)\, \mathrm{defect}_\ell / t_L, \qquad t_L = 1 \text{ for } L = L_0, \quad t_L = t \text{ for a character.} \quad (1)$$

Problem 66.1.2. $\sum_{v|\ell} [G_{\mathbb{Q}_\ell} : \Gamma_v] = [E : \mathbb{Q}] = 2f$. In $\mathbb{Q}(i)$ (a model, with 1 in place of f) the pairs (e_v, f_v) are $(1,2)$ above 3 and $(1,1), (1,1)$ above 5; the sum is 2 both times.

Problem 66.1.3. Let $r' \geq 1$ and $0 \leq t' \leq t$. The bounds (1) for the main row and the t' character rows, summed over the rows and the places $v \mid \ell$, total at most $4fr'\,\mathrm{defect}_\ell = r'\mathrm{loc}_\ell$.

In the proof these dual defects, added over the rows and the places above ℓ, bound what the crystalline relations above ℓ cost, and Problem 66.1.3 is the bound used for the sum. This is the term $r'\mathrm{loc}_\ell$ of the bound $\mathrm{sel} + 2t'\,\mathrm{ram} + r'\mathrm{loc}_\ell + \varepsilon_\ell + n_\ell \leq r'\mathrm{cl}_\ell$ of Problem 65.4.1.

66.2. The crystalline loss of one prime

Why the factorial and the interval? Each supplies one property of crys_ℓ that the local estimates need.

Problem 66.2.1. $\lfloor 2b/\ell \rfloor \le \mathrm{crys}_\ell$, so $2b < \ell(\mathrm{crys}_\ell + 1)$. If ℓ divides an integer of the interval of Definition 66.1.1, then $\mathrm{crys}_\ell \ge (\Delta/2)^3$.

Problem 66.2.2. Formally take $\Delta/2 = 1$ and $b = 32$ (no data have these values). The integer of Definition 66.1.1 is $64! \prod_{3 \le i \le 62} i$, and its valuations at $\ell = 2, 3, 5, 31, 61, 67$ are $119, 58, 28, 4, 2, 0$.

The bound (1) is proved by cases, which we only describe. If the class is tame (so $\ell \in \{p_0, p_1\}$), the cost is paid by the term $b\ \mathrm{val}_\ell(M)$, as $\mathrm{val}_\ell(M) \ge 1$. Otherwise the class is crystalline, the allowed jumps lie in a low window around 0 and in far windows of bounded width starting near $\pm b$ (at thick letters, Section 66.3) or near $\pm\lfloor a/x_1 \rfloor$, and there are three cases: $\ell \le kt$, where the thick letters are sparse (Section 66.3); $\ell > kt$ with $\mathrm{crys}_\ell \ge (\Delta/2)^3$; and $\ell > kt$ with $\mathrm{crys}_\ell < (\Delta/2)^3$. In the first two a power of ℓ bounded through $\lfloor 2\mathrm{crys}_\ell/(kt) \rfloor$ kills the quotient defining the dual defect, and (ii) bounds the number of generators. In the third, by Problem 66.2.1, ℓ divides no integer of the interval, so no nonzero multiple of ℓ lies near 0 or near the starts of the far windows, and the following estimate, read from the proof, applies. In this sheet let $\lambda, \lambda_0, \lambda_1 \ge 1$ be integers, $[-\lambda_0, \lambda_0]$ the low window and λ_1 the width of the far windows. At an unramified place with $\ell \ge 5$, group the embeddings of $\mathcal{O}$ by the root of unity of order $\ell^{f_v} - 1$ that they give (the letters of the chart of E_v), and attach to each such letter i a start fs_i and a sign $\mathrm{sg}_i = \pm 1$. Suppose $\mathrm{fs}_i + \lambda_1 + \lambda_0 \le (\ell - 3)\lambda$ and $6(\lambda + \lambda_0 + \lambda_1) < \mathrm{fs}_i$, and that ℓ divides no nonzero integer within $6(\lambda + \lambda_0 + \lambda_1)$ of 0 or $\pm\mathrm{fs}_i$. Let $\mathcal{C}$ be the class of crystalline lattices with jumps in given sets $\mathcal{J}$, and let L' be crystalline with jumps in sets $\mathcal{J}'$, where over each letter i the set $\mathcal{J}$ lies in $[-\lambda_0, \lambda_0] \cup -\mathrm{sg}_i[\mathrm{fs}_i, \mathrm{fs}_i + \lambda_1]$ and $\mathcal{J}'$ lies in $[-\lambda_0, \lambda_0] \cup \mathrm{sg}_i[\mathrm{fs}_i, \mathrm{fs}_i + \lambda_1]$. Then the dual defect of L' for $\mathcal{C}$ vanishes if no member of $\mathcal{J}$ or of $\mathcal{J}'$ lies in $[-\lambda, 0)$, or if $\mathcal{J}'$ lies in $[-\lambda_0, 0]$; and if at most n_{low} jumps of L' lie in $[-\lambda_0, \lambda_0]$ at each embedding, it is at most $11 f_v (n_{\mathrm{low}}(\lambda + 1) + \mathrm{rk}(L')(\lambda_1 + 1))$ in normalized length.

Problem 66.2.3. For $\ell = 101$, $\lambda = \lambda_0 = \lambda_1 = 1$ and one start $\mathrm{fs}_1 = 42$, the numerical hypotheses of this estimate hold: $44 \le 98$, the radius $6(\lambda + \lambda_0 + \lambda_1) = 18$ is less than 42, and no nonzero multiple of 101 lies within 18 of 0 or ± 42.

66.3. Thick letters

For $\ell \le kt$ no estimate uses ℓ large, and what keeps the loss small is the position of the places of weight b. Fix $\jmath\colon E \to \overline{\mathbb{Q}}_\ell$. For $g \in G_{\mathbb{Q}_\ell}$ let $\sigma_g := \iota^{-1} \circ g^{-1} \circ \jmath$, a complex embedding of E, with place $[\sigma_g] \in \Phi$. For a complex embedding σ its sign $s_\sigma = \pm 1$ for the CM type (as in Definition 65.4.6) is given by $\sigma(\sqrt{-d}) = s_\sigma \sqrt{-d}$, with $K \subset \mathbb{C}$ as in Chapter 33; if $\zeta \in \mathbb{C}$ is the image of ζ_{q_1} under the fixed embedding $E \to \mathbb{C}$ over K, the class of $[\sigma]$ in $(\mathbb{Z}/q_1)^\times$ is the u with $\sigma(\zeta_{q_1}) = \zeta^{s_\sigma u}$.

Definition 66.3.1. The embeddings σ_g, $g \in G_{\mathbb{Q}_\ell}$, are the *letters* over $\jmath$. A letter is *thick* if its place lies in Φ_b.

Problem 66.3.1. Let $\zeta_\jmath := \jmath(\zeta_{q_1})$, $h, n \ge 0$, and $g, g' \in G_{\mathbb{Q}_\ell}$ with $(g'g^{-1})(\zeta_\jmath^{\ell^h}) = \zeta_\jmath^{\ell^{h+n}}$. For every $q' \mid q_1$ prime to ℓ, the class of $[\sigma_g]/[\sigma_{g'}]$ modulo q' is $s_{\sigma_g} s_{\sigma_{g'}}\, \ell^n$.

For $\ell = 2$ and 31 in place of q', the powers of ℓ form the cycle $1, 2, 4, 8, 16$, which does not contain -1.

A lift $\mathrm{Fr}_\ell \in G_{\mathbb{Q}_\ell}$ of the Frobenius of the residue field raises every root of unity of order prime to ℓ to its ℓ-th power. So the letters $\sigma_{\mathrm{Fr}_\ell^n g}$, $n \in \mathbb{Z}$, form a cycle along which the classes of the places move by $\pm\ell^{-1}$ modulo the prime-to-ℓ part of q_1. The sparse condition of Definition 33.3.1(3) is designed for this cycle.

Problem 66.3.2. Let $\ell \le kt$, let ℓ^h be the largest power of ℓ dividing q_1, and let $1 \le i, j \le \lfloor \log_\ell(\Delta/2)^3 \rfloor$. Then $\lfloor \log_\ell(\Delta/2)^3 \rfloor \le 12s$, so $i + j < l_0(s)$. If $g_0, g_1, g_2 \in G_{\mathbb{Q}_\ell}$, $g_2 g_0^{-1}$ raises $\zeta_j^{\ell^h}$ to the power ℓ^{i+j}, $g_2 g_1^{-1}$ raises it to the power ℓ^j, and σ_{g_0}, σ_{g_2} are thick, then σ_{g_1} is not thick.

So along the cycle no three thick letters occur at two successive gaps of at most $\lfloor \log_\ell(\Delta/2)^3 \rfloor$, the gaps used by the local estimate for $\ell \le kt$.

Problem 66.3.3. In the cycle of Problem 66.3.1, call a set of elements of the cycle allowed if it contains no σ, τ, ρ with $\tau/\sigma \equiv \pm 2^i$, $\rho/\sigma \equiv \pm 2^j$ and $0 < i < j < 5$. Then $\{1, 2\}$ is allowed, $\{1, 2, 8\}$ is not, and an allowed set has at most 2 letters. With the true size $l_0(s) \ge 81$ in place of 5, no nonempty set is allowed: a cycle of length 5 is far shorter than any that data produce.

Which far window a thick letter uses depends on its sign. For $\ell \nmid q_1 d$ the field $E \subseteq \mathbb{Q}(\zeta_{q_1 d})$ is unramified at ℓ, and $\ell \ge 13$ since every prime below 13 divides q_0; there the proof reads the sign of each letter separately. For $\ell \mid q_1 d$ the proof needs that the thick letters have one sign, and this has two cases.

Problem 66.3.4. If $\ell \mid q_1$, then $s_{\sigma_g} = s_{\sigma_{g'}}$ for all $g, g' \in G_{\mathbb{Q}_\ell}$; in particular two thick letters have the same sign.

Problem 66.3.5. $d^2 \equiv 1$ and $d \not\equiv \pm 1 \pmod{q_0}$, so $d^n \not\equiv -1 \pmod{q_0}$ for every $n \ge 0$. Hence two thick letters over $\ell = d$ have the same sign. For $q_0 = 18480$ and $d = 9239$, $d^2 \bmod q_0 = 1$.

66.4. The sum over the primes

The number defect_ℓ is $10^6(m/k)$ times a combination of valuations at ℓ of two integers, M^b and $(2b)!\,\mathrm{Int}_b^{(\Delta/2)^3}$. Summed with weights $\log \ell$, valuations give back logarithms.

Problem 66.4.1. For an integer $n \ge 1$ and a finite set A of primes, $\sum_{\ell \in A} \mathrm{val}_\ell(n) \log \ell \le \log n$. For the integer of Problem 66.2.2 the sum over $\ell \le 67$ is $401.34123\ldots$, its logarithm.

Problem 66.4.2. $\mathrm{Int}_b \le (b + 30(\Delta/2)^3)^{60(\Delta/2)^3}$. For data,

$$b \log M + \log\Big((2b)!\,(b + 30(\Delta/2)^3)^{60(\Delta/2)^6}\Big) \le 26\, b \log b.$$

Problem 66.4.3. For every finite set A of primes, $\sum_{\ell \in A} \mathrm{defect}_\ell \log \ell \le 26 \cdot 10^6\,(m/k)\, b \log b$.

Since $26 \le e^{180}$, Problem 66.4.3 gives the following theorem; Problems 66.4.1–66.4.3 prove it.

Theorem 66.4.1. *For all data and every finite set A of primes,*

$$\sum_{\ell\in A} \mathrm{loc}_\ell \log \ell \le 4\cdot 10^6 e^{180}\, f\, \frac{m}{k}\, b \log b.$$

The proof states the theorem with the constant e^{180}, which it obtains by a general comparison of the sizes of the data.

Problem 66.4.4. The right side of Theorem 66.4.1 is at most $16\cdot 10^6 e^{180}\, B/(\log b)^2$.

So the local loss uses a fraction $O((\log b)^{-2})$ of the budget B. Proved here: Problems 66.1.3 and 66.2.1, the spacing and signs of thick letters, and Theorem 66.4.1. Taken as given: local duality, the Bloch–Kato rank, and the bound (1) at one place with its case analysis. Problem 65.4.4 adds Theorem 66.4.1 to the bounds for the other terms of cl_ℓ, summed with weights $\log \ell$, to fit the budget B.

In the Lean formalization. In the Lean proof [GL] (`grh/src/`; the prefixes `New.Selmer`, `New.Lift` and `New.Period` are omitted), Definition 66.1.1 is `crystallineLoss`, `defectBound` (`New/Congruences/LocalLoss/Basic.lean`) and `localDefectBound` (`New/Congruences/FirstOrder/TraceRelations.lean`). The cocycles that obey the relations and their graph are `ribetCocyclesIn` and `ribetCocycles.exists_graph_subrepresentation` (`LocalLoss/Basic.lean`). Definition 66.1.2 is `dualDefect` (`Lib/ClassField/LocalDuality/CrystallineDuality.lean`), where (i) is `IsPotentiallyCrystalline.relIndex_dvd_of_orthogonal`; (ii) is `crysCocycles.finrank_eq` (`Lib/PadicHodge/BlochKato.lean`); the frame behind (iii) is in `Lib/PadicHodge/Kisin/`. The bound (1) is `summand_defect_le_at_place` (`LocalLoss/CrystallineDefect.lean`); its case analysis is `normLength_dualDefect_le_of_crystallineSizes` (`LocalLoss/CrystallineCocycles.lean`) and, for a tame class, `normLength_dualDefect_le_defectBound_of_isTameType` with `two_mul_tame_exponent_le_defectBound`; the estimate before Problem 66.2.3 is `KummerChart.dualDefect_eq_zero_and_dualDefect_le` (`New/Congruences/Lifting/CupOrthogonalityBounds.lean`); the letters, their thickness and signs as the local estimates use them are `eventually_exists_lettersReadThick`. The dual defects summed over rows and places are bounded by $r'\mathrm{loc}_\ell$ in `eventually_exists_inClass_sum_dualDefect_le`, and $r'\mathrm{loc}_\ell$ is a term of `liftValuationBound` (`FirstOrder/DenominatorBound.lean`). Problem 66.1.3 is `sum_index_mul_defectBound_le`, whose step `h_degrees` proves the form with $\le$ of Problem 66.1.2, stated here with equality. Problem 66.2.1 is `two_mul_lt_mul_crystallineLoss_succ` and `cube_le_crystallineLoss_of_dvd`, its first inequality being a step in the proof of the former. Problem 66.3.1 is `placeClass_eq_cmSign_mul_pow`; Problem 66.3.2 is `notMem_bPlaces_of_short_arc`, with the bound on the gaps from `notMem_bPlaces_of_coefficientEmbedding_eq_pow`. Problems 66.3.4 and 66.3.5 are the two branches of `cmSign_eq_of_mem_bPlaces`, whose branch $\ell \mid q_1$ does not use that the letters are thick, with `New.Parameters.d_pow_ne_neg_one` (`New/Reduction/Data/FieldsAndPlaces.lean`) for the first assertion of Problem 66.3.5. Problem 66.4.1 is `sum_padicValNat_mul_log_le`, the first part of Problem 66.4.2 is `prod_Ioc_natB_le_pow`, and Theorem 66.4.1 is `sum_localDefectBound_mul_log_le` (`New/Congruences/FitTwistsExist.lean`).

The comparison of sizes that gives e^{180} is `New.Data.le_of_hasLogBound`, and the sum of the clearing bounds is `sum_clearingBound_add_padicValNat_le`. The constant 26, Problems 66.1.1, 66.2.2, 66.2.3, 66.3.3 and 66.4.4, and the numerical examples in Problems 66.1.2, 66.3.1, 66.3.5 and 66.4.1 are ours.

Hints

§66.1.

66.1.1: The pairing identifies F_2 with the dual of F_1; describe $F_0^{\perp}$ in these terms.

66.1.2: The places above ℓ correspond to the double cosets of the embeddings; use $\sum_v e_v f_v = [E : \mathbb{Q}]$ [SLF, Ch. I, §4, Prop. 10] and $[E_v : \mathbb{Q}_\ell] = e_v f_v$ [SLF, Ch. II, §3]. -1 is a square modulo 5, not modulo 3.

66.1.3: Sum first over the places, by Problem 66.1.2.

§66.2.

66.2.1: Legendre's formula for $(2b)!$; the integer divides Int_b.

66.2.2: Legendre's formula, plus the multiples of ℓ in $[3, 62]$.

§66.3.

66.3.1: Write $g(y) = y^{u_g}$ on roots of unity of order q_1 in $\overline{\mathbb{Q}}_\ell$, for $g \in G_{\mathbb{Q}_\ell}$, and compare $\sigma_g(\zeta_{q_1})$ with $\sigma_{g'}(\zeta_{q_1})$.

66.3.2: $r \le 3x^5$ and $2^s = m^{22} \ge x^{11}$; then Problem 33.2.1 and Problem 66.3.1.

66.3.3: For three letters, read their exponents relative to one of them. For the last assertion, σ, τ, ρ need not be distinct.

66.3.4: Consider $\theta_K = (1 + \sqrt{-d})/2$ and Problem 33.1.2.

66.3.5: $d + 1$ is an odd multiple of $q_0/2$. For the second assertion, $d \nmid q_1$, and every element of $G_{\mathbb{Q}_d}$ raises the roots of unity of order q_1 to a power d^n; use Problem 66.3.1 with $q' = q_0$ and the class of Φ_b modulo q_0.

§66.4.

66.4.1: Factor n.

66.4.2: Count the factors. Then Problem 33.5.4, $(2b)! \le (2b)^{2b}$, and $(\Delta/2)^6 = r^{48}$, which is tiny compared with b by Definition 33.3.1.

66.4.3: Problem 66.4.1 for $n = M^b$ and $n = (2b)!\,\mathrm{Int}_b^{(\Delta/2)^3}$.

66.4.4: $B = fxb\log^3 b/(mk)$ and $m \le 2\sqrt{x}$.

References

[ADT] J. S. Milne, *Arithmetic Duality Theorems*, 2nd ed., BookSurge, 2006.

[BK] S. Bloch and K. Kato, *L-functions and Tamagawa numbers of motives*, in: The Grothendieck Festschrift I, Progr. Math. 86, Birkhäuser, 1990, 333–400.

[BMS] B. Bhatt, M. Morrow and P. Scholze, *Integral p-adic Hodge theory*, Publ. Math. IHÉS **128** (2018), 219–397.

[GL] L. Sernau, *GRH for Dirichlet L-functions, in Lean 4*, a shorter rewriting of the Lean proof, text by Claude, `https://github.com/lsernau/grh-lean`, commit `72fead1`, readable edition `grh/`.

[Ki] M. Kisin, *Crystalline representations and F-crystals*, in: Algebraic Geometry and Number Theory, Progr. Math. 253, Birkhäuser, 2006, 459–496.

[SGC] J.-P. Serre, *Galois Cohomology*, Springer, 1997.

[SLF] J.-P. Serre, *Local Fields*, Grad. Texts in Math. 67, Springer, 1979.

TWISTS WITH FEW CONGRUENCES

Prerequisites. Valuations on $\bar{\mathbb{Q}}_\ell$ [Ne, Ch. II]; roots of unity of prime power order [Wa, Ch. 1–2]; inertia groups and tame inertia at a finite place. Chapter 68, *Roots of unity for many polynomials*: Theorem 68.2.1 and Problems 68.2.7 and 68.2.5. Chapter 65, *Denominators of projections to lifts*: Section 65.4 with its definitions (coefficient rings and normalized lengths, auxiliary twists, main-summand-like representations, Selmer bounds, the numbers tw_ℓ and cl_ℓ) and Theorem 65.4.1. The data of Chapter 33; twists and critical pairs (Chapter 34, Section 34.6 and Definition 34.10.1); heights of families (Section 5.3) and the twist at each prime of Chapter 6; regular families (Definitions 64.2.2 and 64.2.3). As background: Stickelberger elements (Chapter 26) and Selmer groups (Chapter 30).

Chapter 65 bounds the denominator of a projection to lifts through the Selmer groups of twisted Galois representations, and the cost of comparing a lift at two twists involves ratios of Hecke L-values (Chapter 60). For each prime ℓ and each $\iota \mid \ell$, can one twist bound the Selmer lengths for a prescribed finite family satisfying the hypotheses of Theorem 67.1.2 and the valuations of the ratios for every ramified critical pair and both signs? The proof reduces both to values of polynomials at points $(\zeta_w - 1)_w$, with ζ_w roots of unity of ℓ-power order. The lemma that chooses the roots of unity is proved in Chapter 68; Section 67.1 states the polynomial input, deduces the existence of small twists (Theorem 67.1.1) and states the twisting theorem; Section 67.2 provides the regular families used in Chapters 60 and 54.

Throughout, ℓ is a prime and val is the valuation of $\bar{\mathbb{Q}}_\ell$ with $\mathrm{val}(\ell) = 1$ and $\mathrm{val}(0) = \infty$, as in Chapter 68; $\mathrm{val}_+ := \max(\mathrm{val}, 0)$, and val_ℓ is the ℓ-adic valuation of integers. Coefficient rings $\mathcal{O}$ and normalized lengths are those of Section 65.4.

67.1. The twisting theorem

Fix a CM field $E \subseteq \bar{\mathbb{Q}}$, with $G_E := \mathrm{Gal}(\bar{\mathbb{Q}}/E)$ and $g^c := cgc$ for the complex conjugation c of Section 65.4, a finite set Σ_0 of finite places of E containing those above ℓ, and an element g_0 of inertia at a place of Σ_0 prime to ℓ. Fix finitely many Selmer data and finitely many Stickelberger systems for (Σ_0, g_0), defined in the next paragraphs. Chapter 30 gives examples of Selmer classes arising from congruences, and Chapter 26 treats the classical cyclotomic Stickelberger element.

The Selmer data T_{Sel} have a common coefficient ring $\mathcal{O}$. A *Selmer datum* for (Σ_0, g_0) is a free $\mathcal{O}$-module T_{Sel} of finite rank $\mathrm{rk}\, T_{\mathrm{Sel}} \geq 1$ with a continuous $\mathcal{O}$-linear action of G_E, unramified outside a set $\Sigma(T_{\mathrm{Sel}}) \subseteq \Sigma_0$ containing the places above ℓ; write $T_{\mathrm{Sel}}(g)$ for the action of g. The endomorphisms $T_{\mathrm{Sel}}(g)$, $g \in G_E$, span $\mathrm{End}_{\mathcal{O}}(T_{\mathrm{Sel}})$ over $\mathcal{O}$. For each finite place w of E fix a place of $\bar{\mathbb{Q}}$ above w, and write G_w for its decomposition group. For each $w \mid \ell$ the datum supplies a finitely generated $\mathcal{O}$-module Z_w of cocycles $G_w \to T_{\mathrm{Sel}}$ containing the coboundaries, with $\sum_{w|\ell}(\mathrm{rk}\, Z_w - \mathrm{rk}\, T_{\mathrm{Sel}}) \leq f_E\, \mathrm{rk}\, T_{\mathrm{Sel}}$, where f_E is the number of infinite places of E. The *local relations* at w are the relations $\sum_j a_j z(g_j) = 0$, with finitely many $g_j \in G_w$ and $a_j \in \mathrm{End}_{\mathcal{O}}(T_{\mathrm{Sel}})$, satisfied by all $z \in Z_w$. The datum also supplies an

Date: November 26, 2026.

element $\gamma(T_{\mathrm{Sel}})$ of inertia at a place of $\Sigma(T_{\mathrm{Sel}})$ prime to ℓ and a scalar $\lambda \in \mathcal{O}$ with $\lambda^2 - 1 \in \mathcal{O}^\times$; both $\gamma(T_{\mathrm{Sel}})$ and $(\gamma(T_{\mathrm{Sel}})^c)^{-1}$ act on T_{Sel} by λ.

A datum has three terms, in the nonnegative extended integers. For $0 \neq a \in \mathcal{O}$ write $\bar{T}_a := T_{\mathrm{Sel}}/aT_{\mathrm{Sel}}$, and $\bar{T}_a^{*c}$ for the additive dual $\mathrm{Hom}_{\mathbb{Z}}(\bar{T}_a, \mathbb{Q}/\mathbb{Z})$, on which $\mathcal{O}$ acts by precomposition and $g \in G_E$ acts by $y \mapsto y \circ \big(\chi_{\mathrm{cyc}}(g^c)\, T_{\mathrm{Sel}}((g^c)^{-1})\big)$, with χ_{cyc} the ℓ-adic cyclotomic character. The global term $\mathrm{glob}(T_{\mathrm{Sel}})$ is the supremum, over $0 \neq a \in \mathcal{O}$, of the $\mathcal{O}$-length of the module of $\mathcal{O}$-linear G_E-equivariant maps $\bar{T}_a \to \bar{T}_a^{*c}$. At a place $v \in \Sigma(T_{\mathrm{Sel}})$ prime to ℓ, the local term is the supremum over the same a of the excess, taken to be 0 if negative, of the length of the module of restrictions to G_v of the locally constant cocycles $G_E \to \bar{T}_a$ over the length of $\bar{T}_a$; $\mathrm{plc}(T_{\mathrm{Sel}})$ is the sum of these local terms over the places $v \in \Sigma(T_{\mathrm{Sel}})$ prime to ℓ. The third term is $\mathrm{inr}(T_{\mathrm{Sel}}) := \sum_g \mathrm{ord}_{\mathcal{O}} \det(T_{\mathrm{Sel}}(g) - 1)$, the sum over $g = g_0$ and $g = (g_0^c)^{-1}$, where $\mathrm{ord}_{\mathcal{O}}$ gives a uniformizer the value 1. For a datum, $\mathrm{glob}(T_{\mathrm{Sel}})$ and $\mathrm{plc}(T_{\mathrm{Sel}}) + \mathrm{inr}(T_{\mathrm{Sel}})$ are finite. Write $\mathrm{bd}(T_{\mathrm{Sel}}) := (\mathrm{glob}(T_{\mathrm{Sel}}) + \mathrm{plc}(T_{\mathrm{Sel}}) + \mathrm{inr}(T_{\mathrm{Sel}}))/e_{\mathcal{O}}$, with $e_{\mathcal{O}} := \mathrm{ord}_{\mathcal{O}}(\ell)$.

For a finite set Q of finite places and a character $\chi\colon G_E \to \bar{\mathbb{Q}}_\ell^\times$, a bound $\mathrm{len}\,\mathrm{Sel}_Q(T_{\mathrm{Sel}}\chi) \leq d$ means that for every sufficiently large coefficient ring $\mathcal{O}' \supseteq \mathcal{O}$ there is an $\mathcal{O}'$-valued model of χ for which the following module has normalized length at most d: the locally constant cocycles with coefficients in the extended twisted lattice tensored over $\mathcal{O}'$ with $\mathrm{Frac}(\mathcal{O}')/\mathcal{O}'$ that are unramified outside $\Sigma(T_{\mathrm{Sel}}) \cup Q \cup \bar{Q}$, satisfy the local relations with coefficients extended to $\mathcal{O}'$, and vanish at $\gamma(T_{\mathrm{Sel}})$.

A finite set Q of finite places is *auxiliary* for Σ_0 if its places have prime norm, and Q, its conjugate $\bar{Q}$ and Σ_0 are pairwise disjoint. For a finite set Q of finite places, write Cl_Q for the group of finite ideles u of E with $u\bar{u} = 1$, modulo the subgroup generated by those that are principal and those that are units at every place and congruent to 1 at every place of Q. Every class of Cl_Q is represented by $y/\bar{y}$ for a finite idele y. Let $\chi\colon G_E \to \bar{\mathbb{Q}}_\ell^\times$ be a locally constant character coming by $y \mapsto y/\bar{y}$ from a finite idele class character of tame level Q trivial above ℓ. Its value at the class of $y/\bar{y}$ is $\chi(\mathrm{Art}\, y)$, where Art is the Artin map; it depends only on the class. Extend this evaluation linearly to $\bar{\mathbb{Z}}_\ell[\mathrm{Cl}_Q]$.

A *Stickelberger system* St for (Σ_0, g_0) comprises a continuous character $\alpha\colon G_E \to \bar{\mathbb{Q}}_\ell^\times$ unramified outside Σ_0 with $\alpha(g_0) \neq 1$, a finite list L of integer exponents, and an element $\mathrm{St}_Q \in \bar{\mathbb{Z}}_\ell[\mathrm{Cl}_Q]$ for each finite set Q of finite places, such that $1(\mathrm{St}_\varnothing) \neq 0$, where 1 denotes the trivial character. If $v \notin Q$ and $Q \cup \{v\}$ is auxiliary for Σ_0, then

$$\chi(\mathrm{St}_{Q\cup\{v\}}) = \chi(\mathrm{St}_Q) \prod_{e\in L} \prod_{\epsilon=\pm 1} \big(1 - (\alpha(\mathrm{Fr}_v)\chi(\mathrm{Fr}_v))^\epsilon\, (\#k_v)^{-e}\big)$$

for every locally constant χ coming by $y \mapsto y/\bar{y}$ from a finite idele class character of tame level Q trivial above ℓ, and every arithmetic Frobenius element Fr_v at any place of $\bar{\mathbb{Q}}$ above v; here k_v is the residue field at v, and the product over L counts entries with multiplicity. The finite number attached to the system is

$$\mathrm{bd}(\mathrm{St}) := \mathrm{val}\big(1(\mathrm{St}_\varnothing)\big) + 2\,\#L\ \mathrm{val}\big(\alpha(g_0) - 1\big),$$

where $\#L$ counts entries with multiplicity.

The polynomial input below is read from the proof; it follows by descent, which we do not treat. It holds for any finite Σ_0 with g_0 inertial at a place of Σ_0 prime to ℓ, subject to the hypotheses on the data, systems and c_{tor} below. We use it with Σ_0 containing the places above ℓ. Fix a natural number c_{tor}, a *torsion level*: for

every datum, $\mathrm{bd}(T_{\mathrm{Sel}}) + 1 < c_{\mathrm{tor}}$ and $2 \operatorname{rk} T_{\mathrm{Sel}} \operatorname{ord}_{\mathcal{O}}(\ell^{c_{\mathrm{tor}}}) + 1 < \#k_{\mathcal{O}}$, where $k_{\mathcal{O}}$ is the residue field and $\operatorname{ord}_{\mathcal{O}}$ gives a uniformizer the value 1. There is an integer $s_0 \geq 1$ such that for every rational $\rho > 0$ with $s_0\rho < 1$ and every sufficiently large h_1 there are:

(1) an auxiliary set Q of at most $s_0/2$ places, and for each $w \in Q$ a locally constant homomorphism $\lg_w \colon G_E \to \mathbb{Z}/\ell^{h_1}$, onto on inertia at w, coming by $y \mapsto y/\bar{y}$ from a finite idele class character of tame level $\{w\}$ trivial above ℓ; thus it is anticyclotomic, unramified outside w and $\bar{w}$, and trivial on the decomposition groups above ℓ;
(2) for each datum and each system a polynomial F over $\bar{\mathbb{Z}}_\ell$ in variables X_w, $w \in Q$, and a point with coordinates of valuation at least ρ at which $\mathrm{val}(F) \leq \mathrm{bd} + s_0\rho$, where bd is $\mathrm{bd}(T_{\mathrm{Sel}})$ or $\mathrm{bd}(\mathrm{St})$;
(3) for ℓ^{h_1}-th roots of unity ζ_w, with $\chi_\zeta := \prod_{w\in Q} \zeta_w^{\lg_w}$ and $x := (\zeta_w - 1)_w$: for a system, $F(x) = \chi_\zeta(\mathrm{St}_Q)$; for a datum with $\mathrm{val}(F(x)) < \mathrm{bd}(T_{\mathrm{Sel}}) + 1$, $\operatorname{len} \mathrm{Sel}_Q(T_{\mathrm{Sel}}\chi_\zeta) \leq \mathrm{val}(F(x))$.

Problem 67.1.1. For $\chi_\zeta = \prod_w \zeta_w^{\lg_w}$ and $n \geq 1$, $\chi_\zeta^n = \prod_w (\zeta_w^n)^{\lg_w}$, and $\chi_\zeta^{\ell^{h_1}} = 1$. For $w \in Q$ some g in an inertia group at w has $\chi_\zeta(g) = \zeta_w$.

Problem 67.1.2. Let $0 < \rho < 1$ and $m \geq 1$, and let the ζ_w, $w \in Q$, be ℓ^{h_1}-th roots of unity with $\mathrm{val}(\zeta_w - 1) \leq \rho/m$. Then $\mathrm{val}\big(\chi_\zeta^n(s_{w'}) - 1\big) \leq \rho$ for every $1 \leq n \leq m$, every $w' \in Q \cup \bar{Q}$ and every generator $s_{w'}$ of tame inertia at a place of $\bar{\mathbb{Q}}$ above w'. Hence $\sum_{w'\in Q\cup\bar{Q}} \mathrm{val}\big(\chi_\zeta^n(s_{w'}) - 1\big) \leq 2\,\#Q\,\rho$.

Problem 67.1.3. Let $0 < \varepsilon < 1$ and $m \geq 1$. There are auxiliary data as in the input and a character $\chi_\zeta = \prod_w \zeta_w^{\lg_w}$ such that, for all $1 \leq n \leq m$, $\operatorname{len} \mathrm{Sel}_Q(T_{\mathrm{Sel}}\chi_\zeta^n) \leq \mathrm{bd}(T_{\mathrm{Sel}}) + \varepsilon$ for every datum, $\mathrm{val}(\chi_\zeta^n(\mathrm{St}_Q)) \leq \mathrm{bd}(\mathrm{St}) + \varepsilon$ for every system, χ_ζ^n is ramified at every place of Q, and $\sum_{w'\in Q\cup\bar{Q}} \mathrm{val}\big(\chi_\zeta^n(s_{w'}) - 1\big) \leq \varepsilon$ for any generators $s_{w'}$ of tame inertia.

Theorem 67.1.1 (small twists)**.** *Let Σ_0, g_0, finitely many Selmer data over one coefficient ring $\mathcal{O}$, finitely many Stickelberger systems and a torsion level c_{tor} be as above, and let $m \geq 1$ be an integer and $\varepsilon > 0$ real. There are a finite set Q of places, auxiliary for Σ_0, and a character $\chi \colon G_E \to \bar{\mathbb{Q}}_\ell^\times$ such that for every $1 \leq n \leq m$:*

(1) *χ^n is locally constant, of ℓ-power order, comes by $y \mapsto y/\bar{y}$ from a finite idele class character of tame level Q trivial above ℓ, and is ramified at every place of Q;*
(2) *$\operatorname{len} \mathrm{Sel}_Q(T_{\mathrm{Sel}}\chi^n) \leq \mathrm{bd}(T_{\mathrm{Sel}}) + \varepsilon$ for every datum, and $\mathrm{val}(\chi^n(\mathrm{St}_Q)) \leq \mathrm{bd}(\mathrm{St}) + \varepsilon$ for every system;*
(3) *$\sum_{w'\in Q\cup\bar{Q}} \mathrm{val}\big(\chi^n(s_{w'}) - 1\big) \leq \varepsilon$ for any generators $s_{w'}$ of tame inertia at any places of $\bar{\mathbb{Q}}$ above the w'.*

Problems 67.1.1–67.1.3 give Theorem 67.1.1 for $0 < \varepsilon < 1$. The proof uses the same reduction to the polynomial input.

For the data of Chapter 33 the proof applies Theorem 67.1.1, with $\varepsilon = 2^{-\ell}$, to Selmer data on lattices in given representations and to one Stickelberger system for each ramified critical pair and sign. We use the notation of Chapters 33 and 34 (f, r, t, m, b, p_0, p_1, $M = p_0p_1$, N, the chosen places $\mathcal{M}$, the integer $\mathcal{N}$, m-fold twists ϑ with their sets Q_ϑ), the critical pairs $P = (\nu, z)$, their ratios $R_P(\vartheta, \epsilon)$, $\epsilon = \pm 1$,

and ramified pairs of Definition 34.10.1, and the number of Definition 65.4.1,

$$\mathrm{tw}_\ell := (4f+3)\, r\ \mathrm{val}_\ell(\mathcal{N}) + 2^{-\ell}.$$

For a twist ϑ and $\iota\colon \mathbb{C} \simeq \bar{\mathbb{Q}}_\ell$, $\hat{\vartheta}$ is the inverse avatar of Definition 65.4.5.

Theorem 67.1.2 (twisting theorem)**.** *Let $\iota\colon \mathbb{C} \simeq \bar{\mathbb{Q}}_\ell$, and let $R_1, \dots, R_n$ ($n \geq 0$) be ℓ-adic representations of G_E such that each R_i is main-summand-like for (t_i', HT_i), for some integer $t_i' \geq 0$ and some family HT_i (Definition 65.4.7). There is an m-fold twist ϑ such that for every $1 \leq j \leq m$:*

1. *the twist ϑ^j is auxiliary with ramification at most tw_ℓ (Definition 65.4.5);*
2. *for each i, the twist $\widehat{\vartheta^j} R_i$ has Selmer bound tw_ℓ (Definition 65.4.9);*
3. *for each ramified critical pair P and each sign ϵ, $\mathrm{val}_+\big(\iota(R_P(\vartheta^j, \epsilon))\big) \leq \mathrm{tw}_\ell$.*

Status: read from the proof [GL]; not proved here. The proof applies Theorem 67.1.1 with Σ_0 the places dividing ℓMN. The hypothesis on the R_i (Definition 65.4.7) imposes, at each place of $\bar{\mathbb{Q}}$ above a chosen place away from ℓ, the determinant bounds for the distinguished tame generator; it does not include the trace identity of Definition 65.4.8. The orders of finite general linear groups enter tw_ℓ through $\mathcal{N}$. The next problem uses the same group-order formula in a numerical example.

Problem 67.1.4. $\#\mathrm{GL}_3(\mathbb{F}_7) = 33784128 = 2^6 \cdot 3^4 \cdot 7^3 \cdot 19$, and $\mathrm{val}_3(7^e - 1) = 1, 1, 2$ for $e = 1, 2, 3$, with sum $4 = \mathrm{val}_3(\#\mathrm{GL}_3(\mathbb{F}_7))$.

Problem 67.1.5. For an integer $n \geq 1$ and a finite set P_0 of primes, $\sum_{\ell \in P_0} \mathrm{val}_\ell(n) \log \ell \leq \log n$. Moreover $\sum_\ell 2^{-\ell} \log \ell = 0.3776\ldots$, the sum over all primes. Hence $\sum_{\ell \in P_0} \mathrm{tw}_\ell \log \ell \leq (4f+3)\, r \log \mathcal{N} + 1$.

67.2. Regular families

As in Chapter 6, the twist may depend on the prime: it is chosen for every $\iota \mid \ell$, and families $y = (y_\iota)$ are measured by their heights (Section 5.3). Regular families and small ratios are those of Definitions 64.2.3 and 64.2.2; the denominators are measured against the budget $B = U/(mk)$, $U = fa \log^3 b$.

Problem 67.2.1. Let $e_\ell \geq 0$ be reals with $\sum_{\ell \in P_0} e_\ell \log \ell \leq c$ for every finite set P_0 of primes. If $\|\iota(y_\iota)\| \leq \ell^{e_\ell}$ for every $\iota \mid \ell$, then y has height at most c.

Problem 67.2.2. If $y \in \mathbb{C}$ and $\mathrm{val}_+(\iota(y)) \leq c$ for a real $c \geq 0$, then $y \neq 0$ and $\|\iota(y^{-1})\| \leq \ell^c$.

Problem 67.2.3. If Q is auxiliary for a set Σ_0 containing the places above ℓ, then ℓ does not divide the product of the norms of the places of Q.

The clearing bound cl_ℓ of Definition 65.4.1 contains the local loss $\mathrm{loc}_\ell = 4f\, \mathrm{defect}_\ell$ of Definition 66.1.1, in which Int_b is the product of the positive integers in $(b - 30(\Delta/2)^3, b + 30(\Delta/2)^3]$ and $\Delta/2 = r^8$. For the data, $m \geq 1$, $k \geq 1$ and $b > 1$.

Problem 67.2.4. For every finite set P_0 of primes, $\sum_{\ell \in P_0} \mathrm{defect}_\ell \log \ell \leq 10^6 \frac{m}{k} \big(b \log M + \log\big((2b)!\, (b + 30(\Delta/2)^3)^{60(\Delta/2)^6}\big)\big)$.

By Theorem 66.4.1, $\sum_{\ell \in P_0} \mathrm{loc}_\ell \log \ell \leq 4 \cdot 10^6 e^{180} f \frac{m}{k}\, b \log b$ for every finite set P_0 of primes.

Problem 67.2.5. $4 \cdot 10^6 e^{180} f \frac{m}{k} b \log b \le B$ if and only if $4 \cdot 10^6 e^{180} m^2 \le x \log^2 b$. In particular this holds if $m^2 \le 4x$ and $\log^2 b \ge 16 \cdot 10^6 e^{180}$.

Problem 67.2.5 compares the upper bound for the sum of the local losses with the budget. The data have $x \le m^2 \le 4x$, by Definition 33.3.1. Problem 65.4.4 bounds $\sum_{\ell \in P_0} (\mathrm{cl}_\ell + \mathrm{val}_\ell(C_1)) \log \ell$ by B for every finite set P_0 of primes, with C_1 the number of $U(1)$ double cosets at the chosen level.

Theorem 67.2.1. *For all data D there is a regular family $\theta = (\theta_\iota)$ of m-fold twists.*

Status: read from the proof [GL]. The next two problems give the clause on small ratios and one step of the clause on denominators. For the hypothesis of the first: the comparison of sizes displayed before Problem 65.4.4 gives $(4f+3)\, r \log \mathcal{N} + 2 \le x^{999}$, and $x^{999} \le x_1$ by Definition 33.3.1, so by Problem 67.1.5 the sum of $\mathrm{tw}_\ell \log \ell$ over every finite set of primes is at most x_1.

Problem 67.2.6. Assume $\sum_{\ell \in P_0} \mathrm{tw}_\ell \log \ell \le x_1$ for every finite set P_0 of primes. If each θ_ι satisfies the conclusions of Theorem 67.1.2 at ι, then θ has small ratios.

Problem 67.2.7. Let $C_1 \ge 1$ be an integer, $y \in \mathbb{C}$ and c real. If $\|\iota(C_1 y)\| \le e^c$, then $\|\iota(y)\| \le e^{c + \mathrm{val}_\ell(C_1) \log \ell}$.

For the denominator clause of regularity, the proof uses the ramification and Selmer bounds of Theorem 67.1.2. It takes one main summand for each lift index and each eigensystem occurring on the good forms of W_m, and one rank-one main summand for the untwisted lift from $U(1)$ for each main pair and its lift index. At $\vartheta = \theta_\iota^j$ it applies Theorem 65.4.1 to the image of the good-form lift from W_j and to the line of the twisted lift of the constant function for each main pair for j. The $U(1)$ stabilizers at the chosen level are trivial. The logarithmic allowance for the pairing of the projections of two test forms onto that line is $(\mathrm{cl}_\ell + \mathrm{val}_\ell(C_1)) \log \ell$; the class number enters as in Problem 67.2.7. This allowance also suffices for clearing the good-form projection. Its sum over every finite set of primes is at most B by Problem 65.4.4.

This chapter has deduced the small twists from the polynomial input and the lemma on roots of unity, and the small ratios of a regular family from the twisting theorem. Taken as given: the polynomial input, the twisting theorem (Theorem 67.1.2), Theorem 65.4.1 and the existence of main summands used in the denominator clause, all read from the proof. Chapter 54 uses Theorem 67.2.1.

In the Lean formalization. In the Lean proof [GL] (`grh/src/`, namespace `New.Selmer` unless stated), the input of Section 67.1 is a specialization of `exists_twistPolynomials`, its objects are `SelmerDatum` and `StickelbergerSystem`, and the length bound is `SelmerDatum.TwistedLengthLe`. Theorem 67.1.1 is `exists_anticyclotomic_twist`, with conclusions `IsSmallTwist`; Theorem 67.1.2 is `exists_mFoldTwist_hasDivisibleSelmerLengthLe`; Theorem 67.2.1 is `New.exists_isRegularFamily`. Its clause on denominators is the field `New.Data.IsRegularFamily.exists_denominator_bound`; the proof uses `exists_mFoldTwist_hasDenominatorsLe` at each ι, and the sum over the primes is that of Problem 65.4.4. The selection of main summands, the two applications of Theorem 65.4.1 and the pairing estimate described in Section 67.2 are the steps of the proof of `exists_mFoldTwist_hasDenominatorsLe`; the main summands are supplied by `exists_isMainSummand_descentPair` and

`exists_isMainSummand_mainPair`. The passage from the values of a Stickelberger system to the ratios of a ramified critical pair is `exists_stickelbergerSystem_ellVal_ratio_le`.

Hints

Section 67.1.

67.1.1: For the last claim, the $\lg_{w'}$ with $w' \neq w$ are unramified at w because Q is auxiliary.

67.1.2: $\lg_w$ is trivial on wild inertia, and a generator of tame inertia at w maps to a generator of $\mathbb{Z}/\ell^{h_1}$; so $\chi_\zeta(s_w) = \zeta_w^a$ with a prime to ℓ, and ζ_w^{an}, ζ_w^n have the same order. At $\bar{w}$ use $\lg_w(g^c) = -\lg_w(g)$. Then Problem 68.2.5.

67.1.3: Choose s_0 as in the input, then a rational $\rho > 0$ with $s_0\rho \leq \varepsilon/2$, then h_0 by Problem 68.2.7 with the bounds $\mathrm{bd} + 1 \geq 0$ (note $0 \leq \mathrm{val}(F) \leq \mathrm{bd} + s_0\rho$) and $\varepsilon/2$, then a sufficiently large $h_1 \geq h_0$ and the auxiliary data at level ℓ^{h_1}. Use Problem 67.1.1; for the ramification, Problem 68.2.5; for the last sum, Problem 67.1.2 and $2\,\#Q \leq s_0$.

Theorem 67.1.1: Take $\chi = \chi_\zeta$ for $0 < \varepsilon < 1$. For $\varepsilon \geq 1$, apply the case $\varepsilon = 1/2$.

67.1.5: Factor n; for the last claim take $n = \mathcal{N}$.

Section 67.2.

67.2.1: Which multiplier leaves the local inequalities unchanged?

67.2.3: A place of Q has prime norm and does not lie above ℓ.

67.2.4: Problem 67.1.5, and count the factors of Int_b.

67.2.5: Write $a = xb$.

67.2.6: Problems 67.2.3, 67.2.2 and 67.2.1.

67.2.7: $\|\iota(C_1)\| = \ell^{-\mathrm{val}_\ell(C_1)}$.

References

[GL] L. Sernau, *GRH for Dirichlet L-functions, in Lean 4*, a shorter rewriting of the Lean proof, text by Claude, `https://github.com/lsernau/grh-lean`, commit `72fead1`, readable edition `grh/`.

[Ne] J. Neukirch, *Algebraic Number Theory*, Grundlehren Math. Wiss. 322, Springer, 1999.

[Wa] L. C. Washington, *Introduction to Cyclotomic Fields*, 2nd ed., Grad. Texts in Math. 83, Springer, 1997.

ROOTS OF UNITY FOR MANY POLYNOMIALS

Prerequisites. Valuations on $\bar{\mathbb{Q}}_\ell$ [Ne, Ch. II]; roots of unity of prime power order [Wa, Ch. 1–2]. No earlier chapter.

Chapter 67, *Twists with few congruences*, describes how the proof bounds Selmer lengths and the valuations of ratios of Hecke L-values at each prime ℓ through values of polynomials at points $(\zeta_w - 1)_w$, with the ζ_w of ℓ-power order. Suppose finitely many integral polynomials have starting points whose coordinates have valuation at least a fixed rational $\rho > 0$, and the sum of their starting valuations is bounded. Can one replace all the points by one tuple $(\zeta_w - 1)_w$ while increasing each valuation by at most a prescribed $\varepsilon > 0$? Theorem 68.2.1 gives a level depending only on the prime, the bound on the number of variables, ρ, the sum bound and ε. Problem 68.2.7 treats the first m powers simultaneously.

Throughout, ℓ is a prime, val is the valuation of $\bar{\mathbb{Q}}_\ell$ with $\mathrm{val}(\ell) = 1$ and $\mathrm{val}(0) = \infty$, $\|y\| = \ell^{-\,\mathrm{val}(y)}$, and $\bar{\mathbb{Z}}_\ell = \{y : \mathrm{val}(y) \geq 0\}$. For $h \geq 0$ put

$$\rho_h := 1/\varphi(\ell^h),$$

with Euler's function φ. For a polynomial $g = \sum_i y_i Y^i \in \bar{\mathbb{Q}}_\ell[Y]$ and a rational $\rho \geq 0$, the *Gauss valuation* is $v_\rho(g) := \min_i\big(\mathrm{val}(y_i) + \rho i\big)$, and $R_\rho(g)$ is the multiset of roots of g in $\bar{\mathbb{Q}}_\ell$ of valuation exactly ρ, counted with multiplicity; for the zero polynomial $v_\rho(0) = \infty$ and $R_\rho(0) = \varnothing$. Below, g denotes a nonzero polynomial in $\bar{\mathbb{Z}}_\ell[Y]$. "Of order ℓ^h" means of exact order ℓ^h. We write ζ_d for a root of unity of exact order d.

68.1. One variable

Given g and a point x of positive valuation, can one replace x by $\zeta - 1$, with ζ a root of unity of ℓ-power order, without making g much more divisible?

Problem 68.1.1. If $h \geq 1$ and ζ has order ℓ^h, then $\mathrm{val}(\zeta - 1) = \rho_h$. For $\ell = 3$ the radii ρ_1, ρ_2, ρ_3 are $1/2, 1/6, 1/18$; for $\ell = 2$ they are $1, 1/2, 1/4$. The ρ_h with $h \geq 1$ are distinct and tend to 0.

Problem 68.1.2. Let $0 \neq g \in \bar{\mathbb{Z}}_\ell[Y]$, and write $g = c\prod_k (Y - \alpha_k)$ in $\bar{\mathbb{Q}}_\ell[Y]$. For rational $\rho \geq 0$,

$$v_\rho(g) = \mathrm{val}(c) + \sum\nolimits_k \min\big(\mathrm{val}(\alpha_k), \rho\big).$$

Hence $v_\rho(g_1 g_2) = v_\rho(g_1) + v_\rho(g_2)$, and $\rho \mapsto v_\rho(g)$ is nondecreasing.

Problem 68.1.3. (a) If $\mathrm{val}(x) \geq \rho$, then $\mathrm{val}(g(x)) \geq v_\rho(g)$. (b) If $\mathrm{val}(y) = \rho$, then

$$\mathrm{val}(g(y)) = v_\rho(g) + \sum\nolimits_{\alpha \in R_\rho(g)} \big(\mathrm{val}(y - \alpha) - \rho\big).$$

Problem 68.1.4. Let $\ell = 3$ and $g = Y^2 + 3Y + 3$. Then $v_\rho(g) = \min(1, 2\rho)$, and for ζ of order 3^h the valuation $\mathrm{val}(g(\zeta - 1))$ is ∞ if $h = 1$ and $2\rho_h = v_{\rho_h}(g)$ if $h \geq 2$.

Date: November 26, 2026.

We bound the root counts on the radii $\rho_h \le \rho$, each weighted by ρ_h. For a rational $\rho > 0$ and an integer $h_0 \ge 1$, let $H(\rho, h_0)$ be the set of h with $1 \le h \le h_0$ and $\rho_h \le \rho$.

Problem 68.1.5. $\sum_{h \in H(\rho,h_0)} \#R_{\rho_h}(g) \cdot \rho_h \le v_\rho(g)$.

Problem 68.1.6. Let $\delta > 0$ and $\beta \ge 0$, with $\beta < \delta \sum_{h \in H(\rho,h_0)} 1/(h+1)$. If $v_\rho(g) \le \beta$, then some $h \in H(\rho, h_0)$ has $\#R_{\rho_h}(g) \cdot \rho_h \le \delta/(h+1)$.

Next, how close can the $\zeta - 1$ of a given order be to a fixed point?

Problem 68.1.7. Let $\alpha \in \bar{\mathbb{Z}}_\ell$ with $\mathrm{val}(\alpha) > 0$, and $h \ge 1$. Then

$$\sum\nolimits_\zeta \min\bigl(\mathrm{val}(\zeta - 1 - \alpha), 1\bigr) \le h + 1,$$

the sum over the ζ of order ℓ^h. For $\ell = 3$, $h = 1$ and $\alpha = \zeta_0 - 1$, with ζ_0 of order 3, the sum is $3/2$.

Problem 68.1.8. For $\ell = 3$, $h = 2$ and $\alpha = \zeta_9 - 1$, the six terms $\min(\mathrm{val}(\zeta - 1 - \alpha), 1)$, for $\zeta = \zeta_9^e$ with $e = 1, 2, 4, 5, 7, 8$, are $1, \frac{1}{6}, \frac{1}{2}, \frac{1}{6}, \frac{1}{2}, \frac{1}{6}$; their sum is $\frac{5}{2} \le h + 1$.

Problem 68.1.9. Let R be a finite multiset of elements of $\bar{\mathbb{Z}}_\ell$ of positive valuation, and $h \ge 1$. Some ζ of order ℓ^h has $\sum_{\alpha \in R} \min\bigl(\mathrm{val}(\zeta - 1 - \alpha), 1\bigr) \le \#R \cdot \rho_h(h+1)$.

Problem 68.1.10. Let $0 < \delta < 1$, $\rho > 0$ rational, and $\beta < \delta \sum_{h \in H(\rho,h_0)} 1/(h+1)$. If $v_\rho(g) \le \beta$, then for some $h \in H(\rho, h_0)$ and some ζ of order ℓ^h,

$$\mathrm{val}\bigl(g(\zeta - 1)\bigr) \le v_{\rho_h}(g) + \delta.$$

Problem 68.1.11. For rational $\rho > 0$, real $\delta > 0$ and $\beta \ge 0$, some h_0 has $\beta < \delta \sum_{h \in H(\rho,h_0)} 1/(h+1)$. For $\ell = 2$, $\rho = \delta = 1/2$ and $\beta = 1$, the least such h_0 is 18.

Problem 68.1.12. Let δ, ρ, β, h_0 be as in Problem 68.1.10. If $\mathrm{val}(x) \ge \rho$ and $\mathrm{val}(g(x)) \le \beta$, then some ζ with $\zeta^{\ell^{h_0}} = 1$ and $\mathrm{val}(\zeta - 1) \le \rho$ has $\mathrm{val}(g(\zeta - 1)) \le \mathrm{val}(g(x)) + \delta$.

68.2. Several variables and several powers

Let $\rho > 0$ be rational, and $\mathcal{V}$ and I finite sets. For $i \in I$ let $F_i \in \bar{\mathbb{Z}}_\ell[X_j : j \in \mathcal{V}]$, and let $x_i \in \bar{\mathbb{Z}}_\ell^{\mathcal{V}}$ be a point. We seek one tuple of roots of unity that works for every i.

Problem 68.2.1. Fix $j \in \mathcal{V}$, and assume $\mathrm{val}(x_{ij}) \ge \rho$ for all i (the other coordinates are only integral). Let $0 < \delta < 1$, $\beta < \delta \sum_{h \in H(\rho,h_0)} 1/(h+1)$, and $\sum_i \mathrm{val}(F_i(x_i)) \le \beta$. There is ζ with $\zeta^{\ell^{h_0}} = 1$ and $\mathrm{val}(\zeta - 1) \le \rho$ such that, if the coordinate x_{ij} is replaced by $\zeta - 1$ for every i, each $\mathrm{val}(F_i(x_i))$, and also their sum, grows by at most δ.

Problem 68.2.2. Let $0 < \delta < 1$, $\#\mathcal{V} \cdot \delta \le 1$, $\beta + 1 < \delta \sum_{h \in H(\rho,h_0)} 1/(h+1)$, $\mathrm{val}(x_{ij}) \ge \rho$ for all i, j, and $\sum_i \mathrm{val}(F_i(x_i)) \le \beta$. There are ζ_j, $j \in \mathcal{V}$, with $\zeta_j^{\ell^{h_0}} = 1$, $\mathrm{val}(\zeta_j - 1) \le \rho$, and $\mathrm{val}\bigl(F_i((\zeta_j - 1)_j)\bigr) \le \mathrm{val}(F_i(x_i)) + \#\mathcal{V} \cdot \delta$ for all i.

Problem 68.2.3. Let $\ell = 3$, $F_1 = X + Y$, $F_2 = XY + 3$, $F_3 = X^2 + 3X + 3$, with starting points $(3, 0)$, $(0, 3)$, $(0, 0)$, at which each F_i has valuation 1. For $\zeta = \zeta_{27}$, the common point $(\zeta - 1, \zeta^2 - 1)$ gives $\mathrm{val}(F_i) = \frac{1}{9}$ for $i = 1, 2, 3$.

The following theorem is proved by the problems of this section. In Theorem 68.2.1, the level h_0 depends only on $\ell, s_0, \rho, \beta, \varepsilon$.

Theorem 68.2.1. *Let $s_0 \geq 0$ be an integer, $\rho > 0$ rational, $\beta \geq 0$ and $\varepsilon > 0$. There is h_0 with the following property. Let $\mathcal{V}$, I be finite sets with $\#\mathcal{V} \leq s_0$, let $F_i \in \bar{\mathbb{Z}}_\ell[X_j : j \in \mathcal{V}]$ and $x_i \in \bar{\mathbb{Z}}_\ell^{\mathcal{V}}$ for $i \in I$, with $\operatorname{val}(x_{ij}) \geq \rho$ for all i, j and $\sum_i \operatorname{val}(F_i(x_i)) \leq \beta$. Then there are $\zeta_j \in \bar{\mathbb{Z}}_\ell$, $j \in \mathcal{V}$, with*

$$\zeta_j^{\ell^{h_0}} = 1, \quad \operatorname{val}(\zeta_j - 1) \leq \rho \quad (j \in \mathcal{V}), \qquad \operatorname{val}\big(F_i((\zeta_j - 1)_j)\big) \leq \operatorname{val}\big(F_i(x_i)\big) + \varepsilon \quad (i \in I).$$

A twist will be used through its first m powers at once, so the roots of unity must also serve for $\zeta_j^n - 1$, $1 \leq n \leq m$.

Problem 68.2.4. Let $n \geq 1$ and $x \in \bar{\mathbb{Z}}_\ell$ with $\operatorname{val}(x) \geq \rho$. Some $x' \in \bar{\mathbb{Z}}_\ell$ has $(1 + x')^n = 1 + x$ and $\operatorname{val}(x') \geq \rho/n$.

Problem 68.2.5. Let $0 < \rho < 1$, $1 \leq n \leq m$, and let ζ have ℓ-power order and $\operatorname{val}(\zeta - 1) \leq \rho/m$. Then $\operatorname{val}(\zeta^n - 1) \leq \rho$; in particular $\zeta^n \neq 1$. For $\ell = 2$, ζ of order 8, $m = n = 2$ and $\rho = 1/2$, equality holds.

Problem 68.2.6. Let $\ell = 3$ and $\Phi_3(Y) = Y^2 + Y + 1$. The values $\operatorname{val}(\Phi_3(\zeta_n^j))$ for $j = 1, 2, 3$ are $\frac{1}{3}, \frac{1}{3}, \infty$ for $n = 9$; $\frac{1}{9}, \frac{1}{9}, \frac{1}{3}$ for $n = 27$; and $\frac{1}{27}, \frac{1}{27}, \frac{1}{9}$ for $n = 81$. For $m = 3$, $\rho = 1/2$, one variable, $F(X) = \Phi_3(1 + X)$, $x = 0$ and $\beta = 1$, no root of order 9 satisfies the conclusion of Problem 68.2.7, for any $\varepsilon > 0$.

Problem 68.2.7. Let integers $s_0 \geq 0$, $m \geq 1$, a rational $\rho > 0$, $\varepsilon > 0$, a finite set I and numbers $\beta_i \geq 0$, $i \in I$, be given. There is h_0 such that, for every finite set $\mathcal{V}$ with $\#\mathcal{V} \leq s_0$, all $F_i \in \bar{\mathbb{Z}}_\ell[X_j : j \in \mathcal{V}]$ and all $x_i \in \bar{\mathbb{Z}}_\ell^{\mathcal{V}}$ satisfying $\operatorname{val}(x_{ij}) \geq \rho$ for every i, j and $\operatorname{val}(F_i(x_i)) \leq \beta_i$ for every i, some ζ_j with $\zeta_j^{\ell^{h_0}} = 1$ and $\operatorname{val}(\zeta_j - 1) \leq \rho/m$ satisfy

$$\operatorname{val}\big(F_i((\zeta_j^n - 1)_j)\big) \leq \operatorname{val}\big(F_i(x_i)\big) + \varepsilon \qquad (i \in I,\ 1 \leq n \leq m).$$

The exercises derive Theorem 68.2.1 and Problem 68.2.7 from the stated prerequisites and the divergence of the harmonic series. Chapter 67 states the polynomial input and uses Problem 68.2.7 to construct the twist and bound its powers.

In the Lean formalization. In the Lean proof [GL], Theorem 68.2.1 is `New.Selmer.exists_rootsOfUnity_ellVal_eval_le_add` (`New/Congruences/Selmer/RootsOfUnity.lean`); two one-variable steps, used in Problems 68.1.6 and 68.1.10, are `New.Selmer.exists_card_rootsOfValuation_mul_le` and `New.Selmer.exists_rootOfUnity_eval_le_gaussVal_add` in the same file; the form for powers, Problem 68.2.7, is `New.Selmer.exists_rootsOfUnity_ellVal_eval_le` (`New/Congruences/Selmer/GeneralTheorem.lean`). The truncated valuation $\max(\mathrm{val}, 0)$ is `New.ellVal`. The polynomial input and the use of the first m powers of one twist are `New.Selmer.exists_twistPolynomials` (`New/Congruences/Selmer/Line.lean`) and the proof of `New.Selmer.exists_anticyclotomic_twist` (`New/Congruences/Selmer/GeneralTheorem.lean`). The passage from a Stickelberger value to a bound on a Hecke L-value ratio uses `New.Selmer.exists_stickelbergerSystem_ellVal_ratio_le` (`New/Congruences/Selmer/LValueSystems.lean`).

Hints

Section 68.1.

68.1.1: The conjugates of $\zeta - 1$ have product $\pm\Phi_{\ell^h}(1) = \pm\ell$.

68.1.2: For $\rho = 0$ reduce modulo the maximal ideal of $\bar{\mathbb{Z}}_\ell$; for $\rho = \mathrm{val}(\pi)$ substitute $Y = \pi Z$.

68.1.3: For (b), factor g and use $\mathrm{val}(y-\alpha) = \min(\mathrm{val}(\alpha), \rho)$ when $\mathrm{val}(\alpha) \neq \rho$.

68.1.4: $g(Y) = ((1+Y)^3 - 1)/Y$.

68.1.5: By Problem 68.1.1 a root lies in at most one R_{ρ_h}; compare with Problem 68.1.2, using $v_0(g) \geq 0$.

68.1.7: The $\zeta - 1 - \alpha$ are roots of $(1+\alpha+Y)^{\ell^h} - 1$; look at its coefficient of Y and use Problem 68.1.2 with $\rho = 1$.

68.1.8: $\zeta_9^e - \zeta_9 = \zeta_9(\zeta_9^{e-1} - 1)$; Problem 68.1.1.

68.1.9: Sum Problem 68.1.7 over R and average over the $1/\rho_h$ choices of ζ.

68.1.10: Choose the radius by Problem 68.1.6 and ζ by Problem 68.1.9.

68.1.11: The harmonic series diverges.

68.1.12: Problem 68.1.3(a) and the monotonicity in Problem 68.1.2.

Section 68.2.

68.2.1: Apply Problem 68.1.10 to the product of the one-variable polynomials $g_i(Y)$ obtained by freeing the coordinate j; for each i separately, use $\mathrm{val}(g_i(\zeta - 1)) \geq v_{\rho_h}(g_i)$.

68.2.2: Induction on the number of coordinates moved, with Problem 68.2.1, keeping the running sum at most $\beta + 1$. For Theorem 68.2.1 take $\delta = \min(\varepsilon, 1)/(s_0 + 2)$ and h_0 from Problem 68.1.11 with $\beta + 1$ in place of β.

68.2.3: Factor F_1 and F_3 at the point; Problem 68.1.1.

68.2.4: The roots of $(1+Y)^n - 1 - x$ have product $\pm x$.

68.2.5: First compare m with $\varphi(\ell^h)$, where ℓ^h is the order of ζ. What is the order of ζ^n?

68.2.6: $\Phi_3(y) = (y^3 - 1)/(y - 1)$; Problem 68.1.1.

68.2.7: Theorem 68.2.1 with radius ρ/m, after the substitution $X_j \mapsto (1 + X_j)^n - 1$; Problem 68.2.4.

References

[GL] L. Sernau, *GRH for Dirichlet L-functions, in Lean 4*, a shorter rewriting of the Lean proof, text by Claude, `https://github.com/lsernau/grh-lean`, commit `72fead1`, readable edition `grh/`.

[Ne] J. Neukirch, *Algebraic Number Theory*, Grundlehren Math. Wiss. 322, Springer, 1999.

[Wa] L. C. Washington, *Introduction to Cyclotomic Fields*, 2nd ed., Grad. Texts in Math. 83, Springer, 1997.

THE SIGN-ONLY PROOF OF THE RIEMANN HYPOTHESIS FOR CURVES

Prerequisites. Finite fields and their additive characters. The formalism of ℓ-adic cohomology with compact supports for schemes of finite type over a finite field, as summarized in [SGA4$\frac{1}{2}$, Rapport]: the Grothendieck–Lefschetz trace formula [SGA4$\frac{1}{2}$, Rapport, Théorème 3.2], the Künneth formula, Poincaré duality, Tate twists, Artin's vanishing theorem, and the long exact sequence of an open subscheme and its closed complement; see also [Mil]. Noether normalization. The Artin–Schreier sheaf, whose trace function is the additive character e of §S1.1 [SGA4$\frac{1}{2}$, Sommes trig.]. One theorem of weak Lefschetz type, stated in §S1.3. No earlier chapter is used. The sequel, *Deligne's bound by the sign-only method*, extends the argument to all dimensions.

S1.1. The identity $qN = M^k + R$

How large is a weighted count of the zeros of a quadratic form, and which part of it has square-root size? Alpöge's note sketches a "$qN = M^k + R$ sign-only proof of Weil and Deligne" using the form $x_1x_2 + \cdots + x_{k-1}x_k$ [Alp, p. 2 and footnote 3], without defining t, M, N or R. We follow the reading of [Dup, §§2.8–2.9] and the proof written out in [Ald]. That text reports that its proof was produced by an AI model from Alpöge's sketch and checked by two others, and that no human has checked it. D. Zhang has since written out the same proof for lisse sheaves on the affine line [Zh]. His note is the primary source for §S1.3 wherever it applies, and the text says where [Ald] goes further.

Let $q = p^f$, and let $e(y) := \exp\bigl(2\pi i \operatorname{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(y)/p\bigr)$ for $y \in \mathbb{F}_q$. For $h \in \mathbb{F}_q$ let K_h be the $q \times q$ matrix with entries $K_h(x, y) := e(hxy)$.

Problem S1.1.1. Every additive character of $\mathbb{F}_q$ is $y \mapsto e(ay)$ for a unique $a \in \mathbb{F}_q$, and $\sum_{h \in \mathbb{F}_q} e(hy)$ equals q if $y = 0$ and 0 otherwise.

Problem S1.1.2. If $h \neq 0$, then $K_h K_h^* = q$. So K_h has operator norm $\sqrt{q}$.

Problem S1.1.3. Let $t(x) := e(x)$ for $x \neq 0$ and $t(0) := 0$. Then $\sum_x t(x) = -1$ and $\sum_x t(x)\, e(x\xi) = q\, \delta_{\xi,-1} - 1$.

Let $k \geq 2$, let $Q(x) := x_1x_2 + x_2x_3 + \cdots + x_{k-1}x_k$ be the quadratic form of the path with vertices $1, \ldots, k$, and let $Z \subset \mathbb{A}^k$ be the quadric $Q = 0$. For $t\colon \mathbb{F}_q \to \mathbb{C}$ let

$$N := \sum_{x \in Z(\mathbb{F}_q)} t(x_1) \cdots t(x_k), \qquad M := \sum_{x \in \mathbb{F}_q} t(x),$$

$$R := \sum_{h \neq 0} \sum_{x \in \mathbb{F}_q^k} t(x_1) \cdots t(x_k)\, e\bigl(hQ(x)\bigr).$$

Problem S1.1.4. $qN = M^k + R$.

Date: November 24, 2026.

The identity holds for every t. Its content is that R is controlled by Fourier analysis, and N and M^k by cohomology. Let D_t be the diagonal matrix with entries $t(x)$, and regard t as a column vector.

Problem S1.1.5. For every h,

$$\sum_{x\in\mathbb{F}_q^k} t(x_1)\cdots t(x_k)\, e(hQ(x)) = t^{\mathsf{T}} K_h D_t K_h D_t \cdots D_t K_h\, t,$$

with $k-1$ factors K_h and $k-2$ factors D_t.

Problem S1.1.6. If $|t| \le T$ and $h \neq 0$, the sum in Problem S1.1.5 has absolute value at most $T^k q^{(k+1)/2}$. Hence $|R| \le T^k q^{(k+3)/2}$.

The trivial bound is $|R| \le T^k q^{k+1}$. If M has the hoped-for size $\sqrt{q}$, then M^k has size $q^{k/2}$, and Problem S1.1.6 exceeds it by $q^{3/2}$ for every k. After a k-th root the loss $q^{3/(2k)}$ tends to 1. In §S1.3 the weights vary with the variable and the field.

Problem S1.1.7. Let E be a finite field with r elements, ψ a nontrivial additive character of E, and $t_1,\dots,t_k\colon E\to\mathbb{C}$ functions bounded by T. For $h\in E^\times$ and $c\in E$, $\bigl|\sum_{x\in E^k} t_1(x_1)\cdots t_k(x_k)\,\psi\bigl(hQ(x)+hc\bigr)\bigr| \le T^k r^{(k+1)/2}$.

This is [Zh, Lemma 2.6] and [Ald, Lemma 3]. For $k=2$ it is a finite-field form of Vinogradov's bilinear bound [Zh, Remark 2.7]. The path is what matters. For odd q and $t(x) := e(-x^2/2)$, completing the square gives $|\sum_{x,y} t(x)t(y)\,e(xy)| = q^{3/2}$. So with k even and the disjoint pairs $x_1x_2 + x_3x_4 + \cdots + x_{k-1}x_k$ in place of Q, the sum can reach $q^{3k/4}$, and the loss after a k-th root does not tend to 1 [Zh, Remark 2.7].

Problem S1.1.8. Let t be as in Problem S1.1.3. Then $N = 1-q$ for $k=3$, and $N = q-2$ for $k=4$.

S1.2. The sign under a vanishing hypothesis

Problem S1.1.6 bounds R, but qN and M^k may each be much larger than R. Why can they not cancel? The note's answer is that their Frobenius eigenvalues sit in adjacent cohomological degrees, "one off" [Alp, footnote 3].

Let $U\subset \mathbb{A}^1_{\mathbb{F}_q}$ be a nonempty open subset with $0\notin U$, and $\mathcal{F}$ a lisse $\overline{\mathbb{Q}}_\ell$-sheaf on U of rank ρ, pointwise pure of weight 0 for a fixed embedding $\iota\colon \overline{\mathbb{Q}}_\ell\to\mathbb{C}$. Let $t(x)$ be the trace of Frobenius on the stalk at $x\in U(\mathbb{F}_q)$, and $t(x) := 0$ for $x\notin U$; then $|t|\le\rho$. Over $\mathbb{F}_{q^n}$ write M_n, N_n, R_n for the sums of §S1.1. Cohomology is taken over $\overline{\mathbb{F}}_q$, and Fr is the geometric Frobenius. Let $\mathcal{F}_k := \mathcal{F}^{\boxtimes k}$ on U^k and $Z_k := Z\cap U^k$. By the trace formula $M_n = \sum_i (-1)^i \operatorname{Tr}(\mathrm{Fr}^n \mid H^i_c(U,\mathcal{F}))$ and $N_n = \sum_i (-1)^i \operatorname{Tr}(\mathrm{Fr}^n \mid H^i_c(Z_k,\mathcal{F}_k))$. Following [Dup, §2.10], assume:

(H1) $H^i_c(U,\mathcal{F}) = 0$ for $i\neq 1$;
(H2) for infinitely many k, $H^i_c(Z_k,\mathcal{F}_k)=0$ for $i\neq k-1$.

Let $\alpha_1,\dots,\alpha_d$ be the eigenvalues of Fr on $H^1_c(U,\mathcal{F})$, and $\alpha_I := \alpha_{i_1}\cdots\alpha_{i_k}$ for $I=(i_1,\dots,i_k)$. Under (H1), $M_n = -\sum_j \alpha_j^n$.

Problem S1.2.1. If $\mathcal{F}$ has rank one and is geometrically nonconstant, then (H1) holds.

Problem S1.2.2. $H^i_c(U^k,\mathcal{F}_k) = 0$ for $i<k$, and $H^k_c(U^k,\mathcal{F}_k) = H^1_c(U,\mathcal{F})^{\otimes k}$. Under (H1) it vanishes also for $i>k$, and $M_n^k = (-1)^k \sum_I \alpha_I^n$.

Problem S1.2.3. Z_k is smooth, of pure dimension $k-1$ or empty. Hence $H^i_c(Z_k, \mathcal{F}_k) = 0$ for $i < k-1$.

Let $\beta_1, \dots, \beta_e$ be the eigenvalues of Fr on $H^{k-1}_c(Z_k, \mathcal{F}_k)$.

Problem S1.2.4. Under (H1), and (H2) for the given k, $R_n = (-1)^{k-1}\big(\sum_j (q\beta_j)^n + \sum_I \alpha_I^n\big)$ for all $n \geq 1$.

Every eigenvalue enters R_n with the same sign: M^k comes from degree k, and qN from degree $k-1$.

Problem S1.2.5. Let $\gamma_1, \dots, \gamma_s \in \mathbb{C}$ be distinct and nonzero, and $m_1, \dots, m_s \in \mathbb{C}$ nonzero. If $|\sum_i m_i \gamma_i^n| \leq A\, C^n$ for all $n \geq 1$, then $|\gamma_i| \leq C$ for all i.

In Problem S1.2.4 the coefficients are positive integers after equal eigenvalues are collected, so no α_I is cancelled by a $q\beta_j$. Problems S1.1.6, S1.2.4 and S1.2.5 with $I = (j, \dots, j)$ give $|\alpha_j|^k \leq q^{(k+3)/2}$, and letting $k \to \infty$ proves:

Theorem S1.2.1 ([Dup, Theorem 2.10.2])**.** *Under (H1) and (H2), every eigenvalue α of* Fr *on $H^1_c(U, \mathcal{F})$ satisfies $|\alpha| \leq \sqrt{q}$, and $|\sum_{x \in \mathbb{F}_q} t(x)| \leq d\sqrt{q}$.*

Hypothesis (H1) is harmless: as in Problem S1.2.1, it holds whenever $\mathcal{F}$ has no nonzero geometrically constant quotient. Hypothesis (H2) is not, and [Dup] does not prove it.

Problem S1.2.6. Let $U = \mathbb{A}^1 \smallsetminus \{0\}$ and $\mathcal{F}$ the Artin–Schreier sheaf, with trace function t as in Problem S1.1.3. Then $\mathcal{F}$ is geometrically nonconstant, (H1) holds with $d = 1$ and $\alpha_1 = 1$, and the vanishing in (H2) fails for $k = 3$ and for $k = 4$.

Replacing Q by $\sum_i a_i x_i x_{i+1}$ with $a_i \neq 0$ dilates the weight in each variable, by different factors. For a given sheaf this can matter: in Problem S1.2.6 with $k = 3$, the cohomology of $a_1x_1x_2 + a_2x_2x_3 = 0$ in U^3 is concentrated in degree 2 when $a_1 \neq a_2$. But (H2) asks for infinitely many k, and the proof below does not rest on a choice of coefficients. What is wanted is a hypersurface in U^k whose cohomology above the middle degree is forced to match that of U^k. This is a weak Lefschetz property, and it holds for a generic hyperplane section, which has linear terms as well as quadratic ones.

S1.3. Weak Lefschetz in place of (H2)

The argument of [Ald] and [Zh] keeps the identity and the estimate, and replaces (H2) by a weak Lefschetz theorem. The higher cohomology of the hypersurface cancels against that of U^k, and what survives is the trace on an actual vector space.

Duality and the Gysin map. Let X be smooth of pure dimension D over a finite field $\mathbb{F}_r$, and $\mathcal{G}$ lisse on X. Poincaré duality pairs $H^i_c(X, \mathcal{G})$ perfectly with $H^{2D-i}(X, \mathcal{G}^\vee)(D)$, compatibly with Frobenius, and the twist (-1) multiplies Frobenius eigenvalues by r. If X is affine, Artin's theorem and duality give $H^i_c(X, \mathcal{G}) = 0$ for $i < D$. Let $Y \subset X$ be smooth and closed of pure dimension $D-1$, or empty. The transpose of restriction $H^a(X, \mathcal{G}^\vee) \to H^a(Y, \mathcal{G}^\vee)$ is the Gysin map $H^j_c(Y, \mathcal{G})(-1) \to H^{j+2}_c(X, \mathcal{G})$, $j = 2D - 2 - a$. We say that Y has property (WL) for $\mathcal{G}$ if this restriction is bijective for $a < D-1$ and injective for $a = D-1$.

Problem S1.3.1. If Y has property (WL) for $\mathcal{G}$, the Gysin map $H^j_c(Y, \mathcal{G})(-1) \to H^{j+2}_c(X, \mathcal{G})$ is bijective for $j > D-1$ and surjective for $j = D-1$.

Now let U be a smooth affine curve over $\mathbb{F}_r$, $\mathcal{F}$ lisse on U, $X := U^k$, $D = k$, and $\mathcal{F}_k := \mathcal{F}^{\boxtimes k}$. Let $Y \subset X$ be as above, with property (WL) for $\mathcal{F}_k$. Let M_n and N_n be the sums of the traces of Frobenius on the stalks of $\mathcal{F}$ over $U(\mathbb{F}_{r^n})$ and of $\mathcal{F}_k$ over $Y(\mathbb{F}_{r^n})$, let $R_n := r^n N_n - M_n^k$, and let K be the kernel of the Gysin map $H_c^{k-1}(Y, \mathcal{F}_k)(-1) \to H_c^{k+1}(X, \mathcal{F}_k)$.

Problem S1.3.2. For all $n \geq 1$, $(-1)^{k-1} R_n = \mathrm{Tr}\big(\mathrm{Fr}^n \mid H_c^1(U, \mathcal{F})^{\otimes k}\big) + \mathrm{Tr}\big(\mathrm{Fr}^n \mid K\big)$.

This is [Ald, Proposition 4]. In [Zh, Lemma 2.2 and Definition 2.3] the right side is the trace on the single group $H_c^k(X, Rj_*j^*\mathcal{F}_k)$, where j is the inclusion of $X \smallsetminus Y$. That group is an extension of K by $H_c^k(X, \mathcal{F}_k)$, and property (WL) says that it is the only nonzero one. Up to one global sign, R_n is the trace of Frobenius on an actual vector space, so Problem S1.2.5 applies with positive integer coefficients. Nothing is assumed about the higher cohomology of U or of Y.

Problem S1.3.3. Let $U = \mathbb{A}^1$, $\mathcal{F} = \overline{\mathbb{Q}}_\ell$, $k = 2$, and Y the conic $xy + ax + by + c = 0$ with $ab \neq c$. Then $N_n = r^n - 1$ and $-R_n = r^n$; here $H_c^1(\mathbb{A}^1, \overline{\mathbb{Q}}_\ell) = 0$, and K has dimension one and eigenvalue r.

The following theorem supplies hypersurfaces with property (WL).

Theorem S1.3.1 (Deligne; [Kat93, Appendix, Corollary A.5])**.** *Let V be smooth of pure dimension D over $\overline{\mathbb{F}}_q$, let $f\colon V \to \mathbb{P}^m$ be quasi-finite, and let $\mathcal{G}$ be lisse on V. For H in a dense open subset of the space of hyperplanes of $\mathbb{P}^m$, restriction $H^a(V, \mathcal{G}) \to H^a(f^{-1}H, \mathcal{G})$ is bijective for $a < D - 1$ and injective for $a = D - 1$.*

Katz states this for a perverse sheaf $\mathcal{K}$, in degrees $a < -1$ and $a = -1$. The case above is $\mathcal{K} = \mathcal{G}[D]$, which is perverse because V is smooth of pure dimension D [Kat93, proof of Corollary 3.4.1]. The proof uses generic base change, duality and Artin's theorem, and no weights.

Problem S1.3.4. Let V be smooth and affine of pure dimension D over $\mathbb{F}_q$, let $\Gamma = (y_1, \ldots, y_m)\colon V \to \mathbb{A}^m$ be a closed immersion, and let $\mathcal{G}$ be lisse on V. For (λ, μ) in a dense open subset of the affine space over $\overline{\mathbb{F}}_q$ of parameters with $\lambda_m = 1$, let $Y := \{\sum_i \lambda_i y_i + \mu = 0\}$. (a) Restriction $H^a(V, \mathcal{G}) \to H^a(Y, \mathcal{G})$ is bijective for $a < D - 1$ and injective for $a = D - 1$. (b) Y is smooth, of pure dimension $D - 1$ or empty.

This is the form used below. It is [Ald, Lemma 8], and for $V = \mathbb{A}^n$ it is [Zh, Theorem 2.4 and Construction 2.5].

Let U be a smooth affine curve over $\mathbb{F}_q$, and $\mathcal{F}$ lisse on U with $|\iota\,\mathrm{Tr}(\mathrm{Fr}_u \mid \mathcal{F}_{\bar{u}})| \leq C$ for all n and $u \in U(\mathbb{F}_{q^n})$. Choose a finite morphism $\pi\colon U \to \mathbb{A}^1$ of degree B, and generators $z_1, \ldots, z_s$ of the $\mathbb{F}_q$-algebra $\mathcal{O}(U)$. For $a = (a_{ij}) \in \mathbb{A}^{ks}$ and $c \in \mathbb{A}^1$ let $Y_{a,c} \subset U^k$ be the zero set of

$$P_{a,c}(u_1, \ldots, u_k) := \sum_{i=1}^{k-1} \pi(u_i)\,\pi(u_{i+1}) + \sum_{i=1}^{k} \sum_{j=1}^{s} a_{ij}\, z_j(u_i) + c.$$

Problem S1.3.5. The map $u \mapsto \big(z(u_1), \ldots, z(u_k), \sum_i \pi(u_i)\pi(u_{i+1})\big)$ is a closed immersion $U^k \to \mathbb{A}^{ks+1}$, and the $Y_{a,c}$ are its hyperplane sections with last coefficient 1.

By Problem S1.3.4 with $\mathcal{G} = \mathcal{F}_k^\vee$, there are $e \geq 1$ and (a, c) with coordinates in $\mathbb{F}_r$, $r := q^e$, for which $Y := Y_{a,c}$ has property (WL) for $\mathcal{F}_k$. Over the field E with r^n elements, let ψ be a nontrivial additive character and $\tau(u)$ the trace of Frobenius at $u \in U(E)$, and for $h, x \in E$ let

$$t_{i,h}(x) := \sum_{u \in U(E),\ \pi(u)=x} \tau(u)\, \psi\Big(h \sum_j a_{ij} z_j(u)\Big).$$

Problem S1.3.6. $r^n N_n = \sum_{h \in E} \psi(hc) \sum_{x \in E^k} t_{1,h}(x_1) \cdots t_{k,h}(x_k)\, \psi\big(hQ(x)\big)$, and the term $h = 0$ is M_n^k.

Problem S1.3.7. $|t_{i,h}| \leq BC$, and $|R_n| \leq (BC)^k\, r^{n(k+3)/2}$.

So the weights of §S1.1 reappear, twisted by additive characters that depend on h. It remains to let k and the field vary.

Problem S1.3.8. Let L be a finite-dimensional $\overline{\mathbb{Q}}_\ell$-vector space with an automorphism Φ, and a real. Suppose that for infinitely many k there are $e_k \geq 1$, a finite-dimensional space K_k with an automorphism Φ_k, a sign ε_k, and constants $C_k > 0$, $c_k \geq 0$ with $c_k/k \to 0$, such that for all $n \geq 1$

$$\varepsilon_k R_{k,n} = \iota \operatorname{Tr}\big(\Phi^{e_k n} \mid L^{\otimes k}\big) + \iota \operatorname{Tr}\big(\Phi_k^n \mid K_k\big), \qquad |R_{k,n}| \leq C_k\, q^{e_k n(ka + c_k)}.$$

Then every eigenvalue α of Φ satisfies $|\iota\alpha| \leq q^a$.

This is [Ald, Lemma 2]. Problems S1.3.2, S1.3.5, S1.3.6, S1.3.7 and S1.3.8, with $a = 1/2$ and $c_k = 3/2$, together with Problem S1.3.4, prove:

Theorem S1.3.2 ([Ald, Theorem 9], $d = 1$; for U open in $\mathbb{A}^1$, [Zh, Theorem 1.1 and Remark 1.2])**.** *Let U be a smooth affine curve over $\mathbb{F}_q$, and $\mathcal{F}$ a lisse sheaf on U with bounded traces as above. Then every eigenvalue α of* Fr *on $H_c^1(U, \mathcal{F})$ satisfies $|\iota\alpha| \leq \sqrt{q}$.*

[Zh] treats a lisse sheaf on an open subset of $\mathbb{A}^1$, with weights at most w in place of bounded traces. That case is enough for curves. Let C be a smooth projective geometrically connected curve of genus g over $\mathbb{F}_q$. Choose $x \in \mathbb{F}_q(C)$ such that $\mathbb{F}_q(C)$ is finite and separable over $\mathbb{F}_q(x)$, let $V \subset \mathbb{A}^1$ be a nonempty open subset over which x is finite and étale, and let $U := x^{-1}(V) \subset C$.

Problem S1.3.9. $H^1(C, \overline{\mathbb{Q}}_\ell)$ is a quotient of $H_c^1(U, \overline{\mathbb{Q}}_\ell)$, compatibly with Fr. Moreover $H_c^1(U, \overline{\mathbb{Q}}_\ell) = H_c^1(V, x_*\overline{\mathbb{Q}}_\ell)$, and $x_*\overline{\mathbb{Q}}_\ell$ is lisse on V with traces of Frobenius between 0 and the degree of x.

Problem S1.3.10. If α is an eigenvalue of Fr on $H^1(C, \overline{\mathbb{Q}}_\ell)$, so is q/α.

Theorem S1.3.2 for $x_*\overline{\mathbb{Q}}_\ell$ on V, and Problems S1.3.9 and S1.3.10, give the Riemann hypothesis for C: every eigenvalue of Fr on $H^1(C, \overline{\mathbb{Q}}_\ell)$ has absolute value $\sqrt{q}$. This is Weil's theorem [Wei48]. The route is that of [Ald], after [Alp], and it uses Theorem S1.3.2 only in the case of [Zh, Theorem 1.1 and Remark 1.2].

Problem S1.3.11. $|\#C(\mathbb{F}_{q^n}) - q^n - 1| \leq 2g\, q^{n/2}$.

Nothing in this section used $\dim U = 1$ except the degrees of the cohomology groups, the finite map π to $\mathbb{A}^1$ and the shape of the coupling $\pi(u_i)\pi(u_{i+1})$. Replacing it by a nondegenerate bilinear form on $\mathbb{A}^d$ is the note's "vectorize to go up dimensions", and leads to Deligne's bound. We do not know for which sheaves and which k hypothesis (H2) holds for the plain quadric $Q = 0$ [Dup, Question 2.10.10]; it is no longer needed.

Hints

§S1.1.

S1.1.1: For $y \neq 0$, $h \mapsto e(hy)$ is a nontrivial character, because the trace is onto $\mathbb{F}_p$. Count the characters.
S1.1.2: The (x, x') entry of $K_h K_h^*$ is a sum over y of a character of y.
S1.1.3: Problem S1.1.1, applied to $\sum_{x \in \mathbb{F}_q} e(x(1+\xi))$.
S1.1.4: Sum over h first, using Problem S1.1.1. Then split off $h = 0$.
S1.1.5: Sum over x_1, then x_2, and so on.
S1.1.6: The operator norm of K_h is $\sqrt{q}$, that of D_t at most T, and $\|t\| \leq T\sqrt{q}$.
S1.1.7: As in Problem S1.1.6, with the matrices $\psi(hxy)$ and the diagonal matrices of the t_i.
S1.1.8: For $k = 4$, sum over x_1 and x_4 first, and use Problem S1.1.3.

§S1.2.

S1.2.1: U is geometrically connected. On an affine curve H_c^0 of a lisse sheaf vanishes; $H_c^2(U, \mathcal{F})$ is the space of coinvariants of the geometric monodromy, twisted by (-1).
S1.2.2: Apply the Künneth formula.
S1.2.3: The gradient of Q has first coordinate x_2. For the vanishing, combine Poincaré duality with Artin's theorem on the affine scheme Z_k.
S1.2.4: Write $q^n N_n$ and M_n^k by the trace formula and Problems S1.2.2 and S1.2.3.
S1.2.5: Compare $\sum_n (\sum_i m_i \gamma_i^n) z^n$ with $\sum_i m_i \gamma_i z/(1 - \gamma_i z)$ in $|z| < 1/C$.
S1.2.6: Problems S1.2.1 and S1.1.8 over $\mathbb{F}_{q^n}$. Compare with the form that (H2) prescribes; by Problem S1.2.5, applied to the difference of two power sums, the coefficients of a power sum are unique.

§S1.3.

S1.3.1: Dualize the hypothesis on restriction, using Poincaré duality on X and on Y.
S1.3.2: Write $r^n N_n$ and M_n^k by the trace formula on Y and X. The first statement of Problem S1.2.2 holds for every smooth affine curve. Then use Problem S1.3.1.
S1.3.3: Translate x and y to factor the equation of Y.
S1.3.4: (a) Theorem S1.3.1 for $V \to \mathbb{A}^m \subset \mathbb{P}^m$; the hyperplanes with $\lambda_m \neq 0$ can be scaled to $\lambda_m = 1$. (b) Bound the dimension of the set of pairs (v, H) with H containing the tangent space of $\Gamma(V)$ at $\Gamma(v)$.
S1.3.5: The first ks coordinates already give a closed immersion.
S1.3.6: Problem S1.1.1, then group the u_i by $x_i = \pi(u_i)$.
S1.3.7: A fibre of π over a point of E is the spectrum of an algebra of dimension at most B. Then apply Problem S1.1.7.
S1.3.8: Problem S1.2.5.
S1.3.9: Use the exact sequence of the open subscheme U and its finite complement. For the rest, x is finite, and the stalk of $x_* \overline{\mathbb{Q}}_\ell$ at a geometric point is the sum over its fibre.
S1.3.10: Use Poincaré duality on C.
S1.3.11: The trace formula on C, and $\dim H^1(C, \overline{\mathbb{Q}}_\ell) = 2g$.

References

[Ald] *A short proof of Deligne's bound for Frobenius eigenvalues, after Alpöge*, contributed by F. Alderliefste, deposit hexagon:2611.00789v1, 21 November 2026, `https://hexagonmath.org/2611.00789v1`.

[Alp] L. Alpöge, untitled note announcing a proof of the Riemann hypothesis, 20 November 2026, `https://alpo.ge/remark.pdf`.

[Dup] *Notes on Alpöge's proof of the Riemann hypothesis*, printed by T. Dupuy, AI generated, 21 November 2026, `https://tdupu.github.io/riemann-public/riemann-book.pdf`.

[Kat93] N. M. Katz, *Affine cohomological transforms, perversity, and monodromy*, J. Amer. Math. Soc. **6** (1993), 149–222.

[Mil] J. S. Milne, *Étale Cohomology*, Princeton, 1980.

[SGA4$\frac{1}{2}$] P. Deligne, *Cohomologie étale* (SGA $4\frac{1}{2}$), Lecture Notes in Math. **569**, Springer, 1977.

[Wei48] A. Weil, *Sur les courbes algébriques et les variétés qui s'en déduisent*, Hermann, 1948.

[Zh] D. Zhang, *On an elementary proof of Weil II*, arXiv:2611.30749, 23 November 2026 (listed as *Notes on an elementary proof of Weil II from Hexagon*), `https://arxiv.org/abs/2611.30749`.

DELIGNE'S BOUND BY THE SIGN-ONLY METHOD

Prerequisites. Chapter S1, *The sign-only proof of the Riemann hypothesis for curves*, whose notation, background and results are used throughout. Constructible ℓ-adic sheaves [SGA4$\frac{1}{2}$, Rapport], [Mil]. Noether normalization, and generic smoothness of a reduced scheme of finite type over a perfect field.

S2.1. The lowest degree

Nothing in §S1.3 used $\dim U = 1$ except the degrees of the cohomology groups, the finite map π to $\mathbb{A}^1$ and the shape of the coupling $\pi(u_i)\pi(u_{i+1})$. What does the sign-only method give for U of dimension d? Fix $\iota\colon \overline{\mathbb{Q}}_\ell \to \mathbb{C}$. A constructible sheaf $\mathcal{F}$ on X has *weights at most* w if at every closed point x all eigenvalues of the local Frobenius have absolute value at most $|\kappa(x)|^{w/2}$. It is *pure of weight* w if all these absolute values equal $|\kappa(x)|^{w/2}$.

Theorem S2.1.1 (Deligne)**.** *Let X be separated of finite type over $\mathbb{F}_q$, and $\mathcal{F}$ a constructible $\overline{\mathbb{Q}}_\ell$-sheaf on X.*

(i) *If $\mathcal{F}$ has weights at most w, every eigenvalue of* Fr *on $H^i_c(X,\mathcal{F})$ has absolute value at most $q^{(w+i)/2}$.*

(ii) *If X is smooth and proper and $\mathcal{F}$ is lisse and pure of weight w, every eigenvalue of* Fr *on $H^i(X,\mathcal{F})$ has absolute value $q^{(w+i)/2}$.*

These are theorems of Deligne [Del74], [Del80, Théorème 3.3.1]; there (i) is stated for mixed sheaves, those with a filtration whose quotients are pure. By a result of Laumon and Deligne's dévissage, (i) follows from the case of a lisse sheaf on an open subset of $\mathbb{A}^1$ [Zh, Remark 1.3], and that case is written out by the sign-only method in [Zh]. The proof below instead treats every dimension directly. It is that of [Ald], and as recorded in Section S1.1, no human has checked that text. Zhang states that the argument adapts to this setting, but he does not write it out [Zh, Remark 1.3].

Problem S2.1.1. For $X = \mathbb{A}^d$ and $\mathcal{F} = \overline{\mathbb{Q}}_\ell$, $H^i_c(X,\overline{\mathbb{Q}}_\ell) = 0$ for $i \neq 2d$, and Fr acts on the line $H^{2d}_c(X,\overline{\mathbb{Q}}_\ell)$ by q^d. So (i) is attained for $w = 0$, $i = 2d$.

Let U be smooth and affine of pure dimension $d \geq 1$ over $\mathbb{F}_q$, and $\mathcal{F}$ lisse on U with $|\iota \operatorname{Tr}(\mathrm{Fr}_u \mid \mathcal{F}_{\bar{u}})| \leq C q^{nw/2}$ for all n and $u \in U(\mathbb{F}_{q^n})$. Let $\pi\colon U \to \mathbb{A}^d$ be finite (Noether normalization), B the number of generators of $\mathcal{O}(U)$ as an $\mathcal{O}(\mathbb{A}^d)$-module, and $z_1,\dots,z_s$ generators of the $\mathbb{F}_q$-algebra $\mathcal{O}(U)$. Let b be a nondegenerate bilinear form on $\mathbb{A}^d$, and for $k \geq 2$, $a = (a_{ij}) \in \mathbb{A}^{ks}$ and $c \in \mathbb{A}^1$ let $Y_{a,c} \subset U^k$ be the zero set of

$$\sum_{i=1}^{k-1} b\big(\pi(u_i),\pi(u_{i+1})\big) + \sum_{i=1}^{k}\sum_{j=1}^{s} a_{ij}\, z_j(u_i) + c.$$

This is the note's "vectorize to go up dimensions" [Alp, footnote 3]. Let $X := U^k$, $D := kd$, $\mathcal{F}_k := \mathcal{F}^{\boxtimes k}$, and, when (a,c) has coordinates in $\mathbb{F}_r$, $r = q^e$, define M_n,

Date: November 24, 2026.

N_n, R_n and K for $Y = Y_{a,c}$ as in §S1.3, with sums over the points with values in $\mathbb{F}_{r^n}$, and with H_c^{D-1} and H_c^{D+1} in the definition of K.

Problem S2.1.2. Let E be a finite field with r elements, ψ a nontrivial additive character of E, $b_1, \dots, b_{k-1}$ nondegenerate bilinear forms on E^d, and $t_1, \dots, t_k \colon E^d \to \mathbb{C}$ bounded by T. For $h \in E^\times$ and $c \in E$,

$$\Big| \sum_{x \in (E^d)^k} t_1(x_1) \cdots t_k(x_k)\, \psi\Big(h \sum_{i=1}^{k-1} b_i(x_i, x_{i+1}) + hc\Big) \Big| \le T^k r^{d(k+1)/2}.$$

This is [Ald, Lemma 3].

Problem S2.1.3. The map $u \mapsto \big(z(u_1), \dots, z(u_k), \sum_i b(\pi(u_i), \pi(u_{i+1}))\big)$ is a closed immersion $U^k \to \mathbb{A}^{ks+1}$, and the $Y_{a,c}$ are its hyperplane sections with last coefficient 1.

Problem S2.1.4. Over every finite extension of $\mathbb{F}_q$, each fibre of π has at most B rational points.

Problem S2.1.5. $H_c^j(X, \mathcal{F}_k) = 0$ for $j < D$, and $H_c^D(X, \mathcal{F}_k) = H_c^d(U, \mathcal{F})^{\otimes k}$.

By Problems S1.3.4 and S2.1.3 with $\mathcal{G} = \mathcal{F}_k^\vee$, there are $e \ge 1$ and (a, c) over $\mathbb{F}_r$, $r := q^e$, for which $Y := Y_{a,c}$ has property (WL) for $\mathcal{F}_k$.

Problem S2.1.6. For all $n \ge 1$, $(-1)^{D-1} R_n = \mathrm{Tr}\big(\mathrm{Fr}^{en} \mid H_c^d(U, \mathcal{F})^{\otimes k}\big) + \mathrm{Tr}\big(\mathrm{Fr}^{en} \mid K\big)$, where Fr^e is the geometric Frobenius over $\mathbb{F}_r$.

Problem S2.1.7. $|R_n| \le (BC)^k\, r^{n(k(w+d)/2+d/2+1)}$.

Problems S2.1.6, S2.1.7 and S1.3.8, the latter with its a equal to $(w+d)/2$ and $c_k = d/2 + 1$, prove:

Theorem S2.1.2 ([Ald, Theorem 9])**.** *Every eigenvalue of* Fr *on* $H_c^d(U, \mathcal{F})$ *has absolute value at most* $q^{(w+d)/2}$.

Below degree d there is nothing to prove, since $H_c^i(U, \mathcal{F}) = 0$ for $i < d$. The degrees above d are reached by induction on the dimension.

S2.2. Induction on the dimension

Problem S2.2.1. $H_c^1(\mathbb{G}_m, \overline{\mathbb{Q}}_\ell)$ is a line on which Fr acts by 1, and $H_c^2(\mathbb{G}_m, \overline{\mathbb{Q}}_\ell)$ a line on which it acts by q. So the inequality in (i) can be strict.

Problem S2.2.2. Theorem S2.1.1(i) holds when X has dimension 0.

Problem S2.2.3. A bound $|\alpha| \le q^{(w+i)/2}$ for the eigenvalues of Fr on $H_c^i(X, \mathcal{F})$ may be proved after replacing $\mathbb{F}_q$ by $\mathbb{F}_{q^e}$, with Fr^e and q^e in place of Fr and q; weights at most w are preserved.

Problem S2.2.4. Let $U \subset X$ be open with closed complement Z. Every eigenvalue of Fr on $H_c^i(X, \mathcal{F})$ is an eigenvalue on $H_c^i(U, \mathcal{F})$ or on $H_c^i(Z, \mathcal{F})$.

Problem S2.2.5. Every X of dimension d has a dense open subscheme U such that U_{red} is a finite disjoint union of smooth affine irreducible schemes and $\mathcal{F}$ is lisse on U.

Problem S2.2.6. If $\mathcal{F}$ is lisse of rank ρ on U with weights at most w, then $|\iota\, \mathrm{Tr}(\mathrm{Fr}_u \mid \mathcal{F}_{\bar{u}})| \le \rho\, q^{nw/2}$ for all n and $u \in U(\mathbb{F}_{q^n})$.

Problem S2.2.7. Let X be smooth and affine of pure dimension $d \geq 1$, $\mathcal{F}$ lisse, and $i > d$. Let $Y \subset X$ be a hyperplane section with property (WL) for $\mathcal{F}$, defined over $\mathbb{F}_q$ (after replacing $\mathbb{F}_q$ by a finite extension). If the eigenvalues of Fr on $H_c^{i-2}(Y, \mathcal{F})$ have absolute value at most $q^{(w+i-2)/2}$, then those on $H_c^i(X, \mathcal{F})$ have absolute value at most $q^{(w+i)/2}$.

Problems S2.2.2–S2.2.7 and Theorem S2.1.2, with Problem S1.3.4 applied to an embedding of X and to $\mathcal{F}^\vee$ to produce the hyperplane sections of Problem S2.2.7, prove Theorem S2.1.1(i) by induction on $\dim X$ [Ald, §8].

Problem S2.2.8. Theorem S2.1.1(i) implies Theorem S2.1.1(ii).

Hints

§S2.1.

S2.1.1: The Künneth formula, and $H_c^*(\mathbb{A}^1, \overline{\mathbb{Q}}_\ell) = \overline{\mathbb{Q}}_\ell(-1)$ in degree 2.

S2.1.2: As in Problem S1.1.6; each matrix $\big(\psi(h\, b_i(x,y))\big)_{x,y \in E^d}$ times its adjoint is r^d, as in Problem S1.1.2.

S2.1.3: As in Problem S1.3.5.

S2.1.4: A fibre is the spectrum of an algebra spanned by B elements.

S2.1.5: The Künneth formula and the vanishing of $H_c^j(U, \mathcal{F})$ for $j < d$.

S2.1.6: As in Problem S1.3.2, with Problems S1.3.1 and S2.1.5.

S2.1.7: As in Problems S1.3.6 and S1.3.7, with Problems S2.1.2 and S2.1.4 and $T = BC\, r^{nw/2}$.

§S2.2.

S2.2.1: The exact sequence of $\mathbb{G}_m \subset \mathbb{A}^1$ and the point 0.

S2.2.2: Frobenius permutes cyclically the geometric points over a closed point of degree m, and its m-th power acts on each stalk as the local Frobenius.

S2.2.3: Compare the eigenvalues of Fr and of Fr^e.

S2.2.4: The long exact sequence of $0 \to j_! j^* \mathcal{F} \to \mathcal{F} \to i_* i^* \mathcal{F} \to 0$.

S2.2.5: Cohomology does not see nilpotents. Remove the intersections of the irreducible components, then use constructibility and generic smoothness.

S2.2.6: A point $u \in U(\mathbb{F}_{q^n})$ lies over a closed point of degree $m \mid n$, and Fr_u is the (n/m)-th power of its local Frobenius.

S2.2.7: Problem S1.3.1.

S2.2.8: Apply (i) to $\mathcal{F}^\vee$, which is pure of weight $-w$, and use Poincaré duality.

References

[Ald] *A short proof of Deligne's bound for Frobenius eigenvalues, after Alpöge*, contributed by F. Alderliefste, deposit hexagon:2611.00789v1, 21 November 2026, `https://hexagonmath.org/2611.00789v1`.

[Alp] L. Alpöge, untitled note announcing a proof of the Riemann hypothesis, 20 November 2026, `https://alpo.ge/remark.pdf`.

[Del74] P. Deligne, *La conjecture de Weil. I*, Publ. Math. IHÉS **43** (1974), 273–307.

[Del80] P. Deligne, *La conjecture de Weil. II*, Publ. Math. IHÉS **52** (1980), 137–252.

[Mil] J. S. Milne, *Étale Cohomology*, Princeton, 1980.

[SGA4$\frac{1}{2}$] P. Deligne, *Cohomologie étale* (SGA $4\frac{1}{2}$), Lecture Notes in Math. **569**, Springer, 1977.

[Zh] D. Zhang, *On an elementary proof of Weil II*, arXiv:2611.30749, 23 November 2026 (listed as *Notes on an elementary proof of Weil II from Hexagon*), `https://arxiv.org/abs/2611.30749`.