DIVISIBILITY AT INERT PRIMES, IN GENERAL

Prerequisites. Chapters 14, 16 and 17 on inert CM reduction and invariant derivatives; Chapter 18 on formal pairings; Chapters 19 and 25 on the integral Hecke image and the composite of lifts. The simplest incarnations below recall Chapter 4 (the prime sum), Chapter 5 (the tops), Chapters 6 and 8 (the slope method and the chain), Chapter 13 (theta intertwiners), Chapter 15 (one CM determinant) and Chapter 24 (Hecke operators and theta lifts). We use the convention $v_p(p) = 1$, $(z)_+ = \max(z, 0)$. This chapter states results of [Adr, §§8–12] in the form used later and checks them on examples; it does not reproduce their definitions in full, and the reader needs [Adr, §§8–12] open.

Which powers of p gained by differentiating a theta kernel survive the chain of lifts, and what is the index of the source on which they survive?

37.1. The scalar in the kernel law

In the manuscript $K = \mathbb{Q}(\sqrt{-d})$, where the auxiliary prime $d \equiv 7 \bmod 16$; the CM period lattice Λ has discriminant one. Fix $p \geq 5$ inert in K and the good integral model of [Adr, §8.2]. Write $W = W(\overline{\mathbb{F}}_p)$, with Frobenius σ.

Theorem 37.1.1 (Lubin–Tate coordinate)**.** *Over W the curve's formal $\mathcal{O}_{K,p}$-module admits an integral coordinate with unit linear term and logarithm* $\lg(X) = \sum_{k\geq 0} X^{p^{2k}}/p^k$ [LT]*,* [Adr, Prop. 8.11].

Status: classical. Simplest incarnation: Problem 14.3.7 gives an integral change of parameter for the Gaussian curve, with uniformizer $-p$.

Theorem 37.1.2 (Kernel law)**.** *Let M be a positive definite hermitian $\mathcal{O}_K$-lattice, $L_M = M \otimes_{\mathcal{O}_K} \Lambda$, and $NL_M \subset L \subset N^{-1}L_M$ with $p \nmid N$. Let G be a theta function on L for the induced polarization, with sign semicharacter and algebraic Taylor coefficients. In an orthonormal frame of M_p, the Taylor series corrected by the product of the one-variable exponential factors of* [Adr, Thm. 8.19] *has bounded coefficients. Suppose M_p is an orthogonal sum of hyperbolic planes and a lattice with orthonormal basis. Write x_e, y_e for the Lubin–Tate coordinates of the two isotropic vectors in each plane. The restriction to these planes in the period normalization of* [Adr, Thm. 8.21] *has the form*

$$\Theta(x, y) = c \exp\left(-\sum_e \beta(x_e, y_e) \right) U(x, y), \qquad c \in \mathbb{C}_p^\times, \quad U \in \mathcal{O}_{\mathbb{C}_p}[[x, y]].$$

Here β is the coboundary of the one-variable theta correction in [Adr, Eq. (8.6)].

Status: proved in [Adr]. The theorem says nothing about the scalar c. For the kernels of the Lean formalization [Lean], built from one theta function of the CM curve normalized to take the value 1 at the origin, it holds with $c = 1$ (Theorem 38.3.2 of Chapter 38). Simplest incarnation: Theorem 17.2.1 gives an integral restriction $\widehat{P}(X)$ to one isotropic line for $K = \mathbb{Q}(i)$, $p \equiv 3 \bmod 8$. Theorem 16.4.1 gives

Date: November 25, 2026.

$v_p(D^n f(0)) \geq \sum_{i>0,\ i\ \mathrm{odd}} \lfloor n/p^i \rfloor$ for an integral series f and its invariant derivation D.

Problem 37.1.1. In one hyperbolic plane $\beta(x,0) = 0$. Show that $c^{-1}\Theta(x,0)$ is integral. In the Gaussian model with its integral line series $\widehat{P}$, show that $v_p(D^{p^3}\widehat{P}(0)) \geq p^2+1$ for $p \equiv 3 \bmod 8$.

37.2. What a minor can absorb

Index the planes by $0 \leq r < \nu,\ 0 \leq a < r_0,\ 0 \leq b < r_1$. The *positions* $s \in \mathbb{Z}/(2\nu)$ number the places of the CM type above p in one Frobenius orbit, so that Frobenius followed by complex conjugation moves the place at s to the place at $s+1$ [Adr, §11.1]; Section 39.1 of Chapter 39 gives the details. After the trace-dual change of coordinates, the variable matrices $X_s = (X_{s,a,b})$ are indexed by the positions. For $\varpi_p^{p^2-1} = p$, put

$$\mathsf{S}_{s,a,b} = \sum_{k\geq 0} (-1)^k X_{s-2k,a,b}^{p^{2k}}, \qquad h_\upsilon = \sum_{s,a,b} \upsilon_s \mathsf{S}_{s,a,b}^p \mathsf{S}_{s+1,a,b}.$$

For $h(0) = 0$, let $\mathcal{C}(h)$ consist of the series $\sum_{i\geq 0} p^{-i} h^i g_i$ with integral g_i. Each denominator p^i therefore comes with i factors of h.

Theorem 37.2.1 (Trace-dual coordinates)**.** *In Theorem 37.1.2, use trace-dual bases ω_r, ω_r^* of the unramified degree-ν extension of $\mathbb{Q}_{p^2}$ over $\mathbb{Q}_{p^2}$, integral on both sides. In the two logarithmic variables substitute respectively $\sum_{s\ \mathrm{even}} \sigma^s(\omega_r^*) X_{s,a,b}$ and $\sum_{s\ \mathrm{odd}} \sigma^s(\omega_r) X_{s,a,b}$; call the resulting series $\Theta^\flat$. Then $c^{-1}\Theta^\flat(\varpi_p X) \in \mathcal{C}(h_\upsilon)$ for some integral υ_s. Indeed, write A, B for those two linear forms, and ϕ for the compositional inverse of $\varpi_p^{-1}\lg(\varpi_p X)$. For $\sigma^2 z = z$ in W, the congruence of* [Adr, Thm. 9.4] *is*

$$\sum_{r,a,b} \big(z\phi(A)\phi(B)^p - \sigma(z)\phi(B)\phi(A)^p \big) \equiv h_\upsilon \pmod{p},$$

where $\upsilon_s = z$ for odd s and $-\sigma(z)$ for even s. Applying this to the kernel pairing gives the class assertion [Adr, Prop. 9.5, Cor. 8.22].

Status: proved in [Adr]. Simplest incarnation: Theorem 18.3.1 puts the rescaled one-pair exponential times an integral series in $\mathcal{C}(\sigma(c_0)x^p y - c_0 x y^p)$, where c_0 is its pairing parameter.

Problem 37.2.1. Work modulo p. In $\mathsf{S}_{s,a,b}^p \mathsf{S}_{s+1,a,b}$, take the k-th term from the first factor after Frobenius and the linear term from the second. Its exponents are p^{2k+1} and 1; its positions differ by $2k+1$ modulo 2ν.

A *shape* consists of a set $\mathcal{T}$ of positions, called *tops*, and at each position a list of columns of heights $h_c \leq r_0$, with a list I_c of h_c column indices for each [Adr, §9]. Use the first h_c rows of a common frame $Y_s X_s$ and the columns I_c to form a determinant; P_I is their product over columns and positions. Pair by $\langle P_I, F\rangle = P_I(\partial)F(0)$, a polynomial in the frame entries.

Problem 37.2.2. For a square minor of $X + tuv^{\mathsf{T}}$, the coefficient of t^d vanishes for $d \geq 2$. Deduce that a product of w framed minors has degree at most w along any rank-one direction, whatever their heights.

Problem 37.2.2 explains why each remaining column costs one. At a top s, count its columns of height one as α_s; set $\alpha_s = 0$ at the other positions. The *remaining* columns at s are the others: all columns if s is not a top, and the columns of height at least two if it is. Write cap_s for their number and λ_s for their number of boxes, the sum of their heights; thus λ_s does not count the columns of height one at a top. Put $\mathrm{len}_p(0) = 0$, and let $\mathrm{len}_p(n)$ count base-p digits for $n > 0$. For a top s, let $E(s)$ consist of the least nonnegative residues of $s' - s$ for tops s' of opposite parity. For positive odd i put $A_{s,i} = (\alpha_s/p^i - \mathrm{cap}_{s+i})_+$. The bounds of [Adr, Thm. 9.6] use

$$\Delta = \sum_s \big(r_1 \,\mathrm{len}_p(\alpha_s) + r_0 r_1 \,\mathrm{len}_p(\lambda_s)\big) + \sum_{s\in\mathcal{T}} \mathrm{len}_p(\alpha_s)^2,$$

$$g^A = \sum_{s\in\mathcal{T}} \sum_{i\notin E(s)} A_{s,i} - \Delta,$$

$$g^B = \frac{p}{p^2-1} \sum_{s\in\mathcal{T}_{\mathrm{ev}}} \alpha_s + \sum_{s\in\mathcal{T}_{\mathrm{odd}}} \sum_i A_{s,i} - \Delta.$$

Theorem 37.2.2 (Valuations of entries)**.** *If $F(\varpi_p X) \in \mathcal{C}(h_\upsilon)$ with integral υ_s, every frame coefficient z of $\langle P_I, F\rangle$ satisfies*

$$v_p(z) \ge g^A, \qquad v_p(z) \ge g^B - \sum_{s\in\mathcal{T}_{\mathrm{ev}}} \alpha_s, \qquad v_p(p^{N_J} z) \ge g^B$$

for every set J of column indices. Here N_J counts height-one top columns labelled outside J at even tops or inside J at odd tops, and adds, for each remaining column at an odd position, the number of its distinct labels in J [Adr, Thm. 9.6].

Status: proved in [Adr]. Simplest incarnation: Theorem 17.3.1 gives the directional bound $\sum_i (\lfloor a/p^i \rfloor - w)_+$ on the Gaussian plane; Theorem 18.4.1 gives an entry bound both before and after multiplication by p^w for one formal pair.

Problem 37.2.3. Use the Gaussian plane for comparison and take $p = 11$, $\nu = r_0 = r_1 = 1$, one even top with $a = 2 \cdot 11^3$ columns and one column at the other position. The directional bound of Theorem 17.3.1 is 242. Show that the two contributing levels in $g^A + \Delta$ give the same 242, while the first inequality of Theorem 37.2.2 gives 221, since λ_s at the top is zero.

37.3. What survives composition

A chain datum [Adr, Def. 10.1] gives integral lattices of equivariant functions Int_j on lattice classes; its steps sum local kernel maps over classes with reciprocal stabilizer weights. Let d_j bound the denominator valuation of those weights at level j.

Theorem 37.3.1 (Integral frames and stabilizers)**.** *For every commutative ring the canonical bideterminants of a fixed shape span a free module with standard-tableau basis, stable under integral row changes and compatible with base change (Green; De Concini–Eisenbud–Procesi). A finite subgroup of $\mathrm{GL}_n(\mathbb{Z})$ has order dividing Minkowski's $M(n)$, where $v_p M(n) = \sum_{h\ge 0} \lfloor n/(p^h(p-1)) \rfloor$ at odd p* [Adr, Thms. 11.2 and 11.13].

Status: classical. Simplest incarnation: the monomials $x^{k-j}y^j$ give the integral polynomial lattice in Theorem 19.5.1; the reciprocal stabilizer orders occur already in the theta sum of Chapter 24, after Theorem 24.2.1.

Problem 37.3.1. For $[E:\mathbb{Q}] = 2f$ and ranks $N_j \le N_m$, the common denominator $D_\Gamma = M(2fN_m)$ satisfies $v_p(D_\Gamma) \le 2fN_m p/(p-1)^2$. For $p = 5,\ 2fN_m = 20$ its valuation is 6.

Write $\mathcal{V}$ for the finite set of Frobenius orbits. At orbit v and step j, g^0, g^1 are the two entry bounds and Pr is the price of commuting the normalized Hecke operator y_v through the composite. More precisely, the nontrivial Hecke terms have bound g^1, the trivial term has bound $\max(g^0, g^1 - \alpha)$; the commutation polynomial has integral coefficients and constant coefficient of valuation at least α. The price bounds the valuation of the scalar in this commutation [Adr, Defs. 10.4 and 10.5, Thm. 10.7].

Theorem 37.3.2 (Gain on the source)**.** *For a chain datum with the Hecke commutation data and orbit bounds of* [Adr, Thm. 10.7]*, choose a set $B \subseteq \mathcal{V}$ of orbits, the* served *orbits, and numbers $S_v \ge \sum_{j=1}^{m} (g^1 - \mathrm{Pr} - g^0)_+(v,j)$ on B. The composite maps the span of*

$$\left(\prod_{v \in B'} y_v\right)^m p^{\sum_{v \in B \setminus B'} S_v} \mathrm{Int}_0 \quad (B' \subseteq B)$$

into $p^{g^{\mathrm{tot}}}\mathrm{Int}_m$, where p^z on a lattice denotes the valuation filtration at z, and

$$g^{\mathrm{tot}} = \sum_{j=1}^{m} \left(\sum_{v \in B} \max(g^0, g^1 - \mathrm{Pr})(v,j) + \sum_{v \notin B} g^0(v,j) \right) - \sum_{j=0}^{m-1} d_j.$$

Status: proved in [Adr]. In the formalization the gain on the Hecke image is Theorem 42.2.1 of Chapter 42, proved from an input on the lifts that their construction supplies. Simplest incarnation: Theorem 25.4.1 gives the sum of the stepwise maxima $\max(\gamma_j(0), A + \delta_j)$ on $y^m\mathrm{Int}_0$ for one orbit.

Problem 37.3.2. Serve one orbit for two steps. Take $d_j = g^0 = 0$, $g^1 = (3,2)$, $\mathrm{Pr} = (1,3)$. Show that the composite maps both $y^2\mathrm{Int}_0$ and $p^2\mathrm{Int}_0$ into $p^2\mathrm{Int}_2$, with the whole improvement coming from the first step.

Theorem 37.3.3 (True lifts)**.** *Let $p \ge 5$ be inert in K and unramified in the CM field E of the lift data of* [Adr, Defs. 11.5, 11.7 and 11.10]*. Suppose that*

(a) *every step kernel satisfies Theorem 37.1.2 with $c = 1$: in the hyperbolic coordinates there, it is $\exp(-\sum_e \beta(x_e, y_e))\, U$ with U integral;*
(b) *the scalar normalizing each step changes only by p-adic units when the lattice at one orbit changes;*
(c) *at the odd positions the frames are the duals of the frames at the even positions, and entry estimates pass to inclusions of lattices there as at the even positions, with determinant factors of the opposite sign.*

Then the true lifts form a chain datum on the integral frame lattices with $d_j = v_p(D_\Gamma)$, commuting normalized Hecke operators, and orbit bounds $(g^A, g^B, \alpha_{\mathrm{ev}})$, where α_{ev} counts the height-one columns at even tops. Theorem 37.3.2 applies with the prices of [Adr, Prop. 11.32, Thm. 11.45].

Status: derived in [Adr, Thm. 11.45] from three hypotheses on the lifts, which are (a)–(c) in the form given there: (N3), [Adr, Hyp. 11.42], for (a); (N1), [Adr, Hyp. 11.22], for (b); and (N2), [Adr, Hyp. 11.38], for (c). Of these, (N1) is proved in [Adr, Prop. 11.27] for the step normalization of [Adr, Def. 11.23], and (N2) and (N3)

are assumed there. The Lean formalization [Lean] proves the final theorem through statements of the form (a)–(c), which Chapters 38 and 39 develop. Its kernels are built from one theta function of the CM curve, normalized to take the value 1 at the origin, and for them (a) is Theorem 38.3.2. Its scalars are p-adic units, which gives (b) (Section 39.4). Its frames at the odd positions are the duals of those at the even positions, and Section 39.3 carries out for them the bookkeeping of (c) that [Adr, Rem. 11.39] leaves to be written. We have not checked that the chain datum of the formalization is the one of [Adr, Thm. 11.45]. Simplest incarnation: Theorem 24.2.1 expresses a sum over neighbours as a Hecke translate plus a scalar multiple of the original theta series; Chapter 13 composes the two theta intertwiners in Theorem 13.4.1.

Theorem 37.1.2 alone does not give (a), since it allows an unknown scalar for each pair of lattice tuples.

Problem 37.3.3. Multiplying a kernel with corrected constant term 1 by p^{-1} preserves boundedness in Theorem 37.1.2 and prevents any expression with both c and U integral. Deduce that applying the boundedness theorem separately to every tuple does not give (a) of Theorem 37.3.3.

37.4. The price of passing to the Hecke image

From here on x is the scale, $0 < \varepsilon < 1/52$, $y = x^{\varepsilon}$, $b = e^{y}$, $a = xb$, k is the rank and n the number of columns, as in [Adr, §5]. Put $X' = \exp(x^{\varepsilon/3})$, $b' = a/X'$, $X'' = xnX'$ and $p_* = k^2 x^{26}$ [Adr, §12.1].

For a representation V of highest weight data λ at a single orbit and $c_* \geq 4(D+1)$, $\mathrm{LP}(r, \lambda; t, D, \kappa, c_*)$ asks for the following at every target lattice. Choose incoming r-edges and integral source vectors in their prescribed depth-t lattices. Each vector vanishes to order c_* in the edge lattice of every other edge out of its source (order measured in the local uniformizer). Integral combinations of their pairings with tests in the depth-t target lattice must give $p^D I_n$ on $n \geq (1-\kappa)\dim V$ independent tests [Adr, Def. 12.6]. Thus κ measures a fraction of the dimension.

Theorem 37.4.1 (Hecke nondegeneracy)**.** *Let p be a prime of* class I*, meaning that odd Frobenius powers from a top land in the top half of the places* [Adr, §12.1]*, whose Frobenius orbits on the columns have length $n_p \geq x^{\varepsilon/4}$. Let t_0 be such an orbit that is* good*, that is, satisfies the spacing conditions of* [Adr, Def. 5.19] *on the tops along it, and let $N(t_0)$ be the number of tops on it. Assume the size conditions of* [Adr, §12.6] *and the three engines of* [Adr, Hyp. 12.12]*: (A) sufficient rank of the reduced segment symbols, (B) detection by the twisted Fock pairing at the stated depth, (C) the mean bound for bad segment shares. Then for large x the following holds at every target lattice, with r, t, D and the share $\kappa = \kappa(a,b)$ of* [Adr, Thm. 12.11]*, where (a,b) are the weights.*

(i) *If $13 \leq p < p_*$, then $\mathrm{LP}(r, \lambda; \lceil t \rceil, D, \kappa, 8(D+1))$ holds with $\kappa \leq N(t_0)x^{-12}$ for all weights in the windows.*

(ii) *If $p_* \leq p < X'$ and no power p^i lies in the band $|p^i - X'| \leq x^{-2}X'$, let κ be the least share for which $\mathrm{LP}(1, \lambda; \lceil t \rceil, D, \kappa, 8(D+1))$ holds. Its mean over the weights in the windows is at most $N(t_0)x^{-12}$.*

Status: derived in [Adr, Thm. 12.11, Cor. 12.13] from the engines [Adr, Hyp. 12.12], assumed there. The proof in [Adr, Thm. 12.11] is an outline; it also calls on a Pieri splitting and a passage from segment shares to κ. The formalization proves the final

theorem; the three engines are not separate statements in it. Chapter 40 states its condition at one edge, which plays the role of LP, and the theorems that establish it for small primes and for primes of class I (Theorems 40.5.1 and 40.5.2), whose proofs are large and are not developed there; we have not matched the engines to its lemmas. Simplest incarnation: at one tree vertex, Theorem 19.5.1 diagonalizes the image on degree-k polynomials. For residue size $Q > k$ the exponent of $x^{k-j}y^j$ is

$$\varepsilon_j = \min\left(k-j,\ \min_{0\le i\le j}\left(i + v_p\binom{k-i}{j-i}\right)\right).$$

Problem 37.4.1. For $p = k = 5$, $Q = 25$, the six exponents are $0, 1, 1, 1, 1, 0$. Deduce that the image has rank two after reduction in the target modulo 5, but its integral colength over the unramified valuation ring is only four. For every $Q > k$ this colength is at most $\sum_{j=0}^{k} v_p\binom{k}{j}$.

For each candidate prime, first sum $\mathrm{Sig}(p) = m\sum_{v\ \mathrm{good}} \kappa_v$ over all its good orbits. The candidates are the class I primes $p < X'$ with $n_p \ge x^{\varepsilon/4}$, subject to the power-band exclusion of Theorem 37.4.1(ii) for $p \ge p_*$. Here κ_v is the share of Theorem 37.4.1 at the orbit v, and t_v, D_p are its exponents. Serve the good orbits only when $\mathrm{Sig}(p) \le x^{-\varepsilon}$; otherwise the served set $\mathcal{V}_p$ is empty. Noncandidates have empty served set as well.

Write $P(M)$ for the sum of the Hecke images with scalar alternatives in Theorem 37.3.2, and $M^{\mathrm{ram}} = M \cap V^{\mathrm{ram}}$ for the saturated lattice in the chosen ramified subspace. For $\mathcal{V}_p \neq \varnothing$, put

$$\tau(p) = e_p + m\sum_{v\in\mathcal{V}_p}(\lceil t_v\rceil + D_p + 1), \quad \mathrm{io}(p) = 2\mathrm{Sig}(p)\max_{v\in\mathcal{V}_p} S_v.$$

Here e_p is the exponent comparing the two integral structures. For an empty served set put $\tau(p) = \mathrm{io}(p) = 0$; a rejected candidate retains its original $\mathrm{Sig}(p)$.

Theorem 37.4.2 (Colength)**.** *At $w \mid p$ for a served class I prime $p \le X''$, $p \neq T_u$, take the lattices and Hecke operators at w given by the chain datum at level zero* [Adr, §12.3, (F1)–(F5)]*, and assume* LP *at every served orbit with parameters $\lceil t_v\rceil, D_p, \kappa_v, 8(D_p+1)$, and $\mathrm{Sig}(p) \le 1/2$. Then $NP_w = P(M) \cap p^{\lceil\tau(p)\rceil}M \cap V^{\mathrm{ram}}$ lies in $p^{\lceil\tau(p)\rceil}M^{\mathrm{ram}}$, and*

$$\mathrm{length}_{\mathcal{O}_w}(M^{\mathrm{ram}}/NP_w) \le v_w(p)\,\mathrm{rk}(M)\big(\tau(p) + \mathrm{io}(p)\big)$$

with v_w the uniformizer valuation [Adr, Thm. 12.18]*. For an empty served set take $NP_w = M^{\mathrm{ram}}$.*

Status: proved in [Adr]. The formalization proves the colength bound in the form of Theorem 41.4.1 of Chapter 41, from the condition at one edge. Simplest incarnation: Theorem 19.5.1 charges the sum of the exponents on a single vertex. Theorem 6.5.1 charges the logarithmic index of a source sublattice divided by its rank.

Problem 37.4.2. Use the inclusion and length bound as a numerical model on a lattice of rank eight, with full ramified part, $v_w(p) = 2$, $m = 2$, one served orbit and $S_v = 3$. For $\kappa_v = 1/8$ and integral τ, show that the length lies between 16τ and $16\tau + 24$. With $\kappa_v = 0$, deduce that $NP_w = p^{\tau}M^{\mathrm{ram}}$.

37.5. The prime sum and the slope

Let T be the set of N_T tops (Section 5.3), m the chain length, a_t the top weights, w_j the bottom weights. In the notation of Section 4.2,

$$S = \sum_{t\in T}\sum_{j=1}^{m} P_{t,w_j}(a_t), \qquad P_{t,w}(a) = \sum_{r} \Lambda_d(r)\big(a/r - w(\mathrm{cell}_t(r))\big)_+.$$

In particular an admitted unramified inert prime contributes $2\log p$ times the sum of these positive parts at its odd powers. Let $\mathrm{gain}_j^{\mathcal{D}}(p)$ be the sum of the local maxima of Theorem 37.3.2 at p, with the baseline truncated at zero and the zero-gain and dropped primes treated as in [Adr, Def. 12.3 and §12.1]. The global gain and the remaining index correction are

$$\Gamma = \sum_{p\in\mathcal{P}} 2\log p \left(\sum_{j=1}^{m} \mathrm{gain}_j^{\mathcal{D}}(p) - \tau(p)\right), \qquad I = \mathrm{IO} = \sum_{p\in\mathcal{P}} \mathrm{io}(p)\log p.$$

Here $\mathcal{P}$ is the set of admitted inert primes of [Adr, §12.1]. The uniform scaling τ has already been deducted in Γ. As in Chapter 58, Γ is the total gain; it is not the Galois group of Chapter 4. The two theorems below use the following *global inputs*, which [Adr, §12.6, (L1)–(L8)] takes from the constructions of the lifts and of the auxiliary prime: at each served place, the local lattices, Hecke operators and orbit bounds of Theorem 37.4.2; the base lattice M_u and its saturated ramified part; the auxiliary prime $T_u \geq X'$, the nodes and their weights; a sublattice at T_u of colength at most λ_T times the rank, with λ_T as in Theorem 37.5.2; and finite supports for the local terms, with residue characteristics whose logarithms sum to at most X''.

Theorem 37.5.1 (Prime sum (A1))**.** *Assume the global inputs, the size conditions of* [Adr, §12.6]*, and weights in the prescribed windows with* lhsW $\leq x^{-9}$*. Here* lhsW *sums* $(21_{\mathrm{Sig}(p)>x^{-\varepsilon}} + 4\mathrm{Sig}(p))\log p/p$ *over candidate primes. Then*

$$S - \Gamma \leq (2\log 4 + 1)N_T mb, \qquad 0 \leq I \leq N_T mb$$

[Adr, Thm. 12.27]*. The count of tops on orbits that are not good comes from* [Adr, Prop. 5.20]*; choosing weights with small* lhsW *uses the engines.*

Status: derived in [Adr, Thm. 12.27] from the engines [Adr, Hyp. 12.12] and from the global inputs, which rest there on (N2) and (N3) through Theorem 37.3.3; these hypotheses are assumed there. The formalization proves the final theorem by a different arrangement at this step (Chapter 42). Its counterpart of this theorem is Theorem 42.4.1, an inequality between explicit numbers at each prime: the gains, prices and colengths of Theorem 37.3.2 and Theorem 37.4.2 against the prime sum. It is proved with the chain of lifts replaced by the zero chain, for which the divisibility clause holds trivially (Problem 42.2.4). The divisibility of the lifts is Theorem 42.2.1, proved on a separate branch, where (a)–(c) of Theorem 37.3.3 enter (Chapters 38 and 39); the two branches meet only in the source lattice N_u (Section 42.3). The engines are not separate statements in the formalization. Simplest incarnation: Theorem 17.3.1 supplies the positive parts for one inert prime; Theorem 15.1.2 sums $\log p/p$ over $p \equiv 3 \bmod 4$ with main term $\frac{1}{2}\log X$.

Problem 37.5.1. The node offset costs b'/x per top and step at served primes $p < X' = xb/b'$. From $\sum_{p\leq X}\log p \leq X\log 4$, show that its total cost is at most

$2\log 4\, N_T mb$. If the other losses together cost at most $N_T mb$, this gives the first inequality of Theorem 37.5.1.

Problem 37.5.2. Put $a = xb$. At a served prime, $S_v \le 2mN_T a/p$ by the local gain estimate in the proof of [Adr, Thm. 12.27]. Show that $I \le amN_T \,\mathrm{lhsW} \le N_T mb\, x^{-8}$. Thus the mean-share input controls the excess colength even after summing over primes.

Problem 37.5.3. Of $2n$ places, $N_2 = \delta n$ carry weight b. Average their total weight over all places, then sum over tops and steps to obtain $N_T mb\delta/2$. For a prime p with $\chi_d(p) = -1$, show that $1 - \chi_d(p)^i$ gives weight two for odd i and zero for even i, independently of N_2. Thus changing N_2 changes only the first of these two counts.

For each chain index u, M_u is the original hermitian lattice and N_u is the rescaled source obtained using NP_w and the auxiliary lattice at T_u [Adr, Def. 12.20]. Write $\mu, \mu_{\max}$ for mean and maximal slopes. In the chain record L is the common real shift and $E_u = \sum_j E_{u,j}$ the sum of the step corrections.

Theorem 37.5.2 (Slope (A2))**.** *Under the global inputs and the size conditions, with* $\mathrm{Sig}(p) \le 1/2$ *at every served prime,*

$$\mu(M_u) + \Gamma + L - E_u - e_{2,u} \le \mu(N_u),$$
$$\mu_{\max}(N_u) \le \mu_{\max}(M_u) + \Gamma + L - E_u.$$

Here $e_{2,u} = 4I + 4\lambda_T \log T_u + R_X + 1$, $4\lambda_T = C_T N_T m(a/k + b')$, *and* $R_X \le 6X'' + 2\log T_u$, *with* k *the base rank* [Adr, Thm. 12.21].

Status: derived in [Adr, Thm. 12.21] from the same hypotheses as Theorem 37.5.1, assumed there; for its selected local lattices [Adr, §18.7] derives the colength bound at the auxiliary prime [Adr, §12.6, (L7)] with $C_T = 36$. The formalization proves the final theorem; there the slope bound comes from the source lattice N_u of Section 42.3, on which the divisibility of the lifts makes the pairing integral, and the colength it costs (Problem 42.3.1). Simplest incarnation: Theorem 8.4.2 bounds the sum of finite gains by the difference of the two end slopes plus the archimedean step heights.

Problem 37.5.4. If $\log T_u \le Cmy$, then the a/k part of $4\lambda_T \log T_u$ is at most $CC_T\, yN_T a\, m^2/k$. Under $N_T m(a/k + b') \ge 1$, show that

$$e_{2,u} \le \mathrm{Lo}_u = C_* I + C_* N_T m(a/k + b') \log T_u + C_* X'' + 1$$

for $C_* \ge \max(6, C_T + 2)$.

Problem 37.5.5. Take $e_L = 0$ and enlarge C_* to at least $2\log 4 + 1$. Theorem 37.5.1 then gives both inequalities of (K1). Show that Theorem 37.5.2 and Problem 37.5.4 give (K2), whose upper bound allows an extra $C_* mB_0 \ge 0$. Conversely, replacing Lo_u in its lower bound by a common $e_2 \ge \mathrm{Lo}_u$ gives the lower bound (A2) used in assembly [Adr, Lem. 18.13, Prop. 18.14].

Deliverable. Theorems 37.5.1 and 37.5.2 supply (K1) and (K2) of [Adr, Def. 18.9] with $I = \mathrm{IO}$ and $e_L = 0$. In [Adr] they are derived from (N1)–(N3) and the engines of [Adr, Hyp. 12.12], of which (N2), (N3) and the engines are assumed there. The formalization proves the final theorem. At this step it proves the inequality of Theorem 37.5.1 between explicit numbers, with the zero chain in place of the lifts,

and the divisibility of the lifts on a separate branch, through the kernel law, the unit scalars and the dual frames of Theorem 37.3.3 (Chapters 38, 39 and 42); the Hecke image is treated in Chapters 40 and 41, and the engines are not separate statements in it; see Section 58.7 of Chapter 58. Alongside (N2), (N3) and the three engines, [Adr, §18.7] singles out the comparisons between levels and the test systems, the Weyl lattice model in [Adr, Cor. 12.65], the polynomial bound for c_G in [Adr, Prop. 12.67], and the identifications needed to transfer to another construction its derivation of (L7) for the selected local lattices at the auxiliary prime.

Hints

§37.2.

37.2.2: Use multilinearity in the columns.

37.2.3: Count digits at the two positions separately.

§37.3.

37.3.1: Sum a geometric series.

§37.4.

37.4.1: Separate $i = 0$ from $i \geq 1$.

37.4.2: Use additivity through $p^{\tau} M^{\mathrm{ram}}$.

References

[Adr] J. Adriazola, *The Alpöge proof of the Riemann hypothesis*, manuscript, revised 25 November 2026, commit `9eefc08`.

[Lean] The Lean community, *riemann-hypothesis*, a Lean formalization of Alpöge's argument, `https://github.com/leanprover-community/riemann-hypothesis`.

[LT] J. Lubin and J. Tate, Formal complex multiplication in local fields, Ann. of Math. (2) **81** (1965), 380–387.