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 $X_{\mathrm{odd}} = \big(\prod_{0<e<t} Y_e\big)^{y^{20}} h_E$: one integer $X_{\mathrm{odd}} \le 2^{4(N+t+3)^{27}} h_E$ bounds $\mathrm{len}_{\mathcal{O}} \mathrm{Sha}_\ell^{\mathrm{odd}}(E, \mathcal{O}; e, n)$ by $v_{\mathcal{O}}(X_{\mathrm{odd}})$ 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_{odd} that it chooses for the data of Chapter 33; the denominator error at ℓ includes the term $t\, v_\ell(X_{\mathrm{odd}})$ (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 $v_\ell(X_{\mathrm{odd}})$ with weights $\log \ell$ it uses the size of X_{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.