THE MINUS PART, BY GAUSS SUMS

Prerequisites. Chapter 30: the modules $W_e = \mathbb{Q}_\ell/\mathbb{Z}_\ell(-e)$, the groups $\mathrm{Sha}_\ell(F,e)$, $\mathrm{Sha}_\ell(\mathbb{Q},e;\eta)$ and the lengths $h_{\ell,e}(F)$, critical characters, and Theorem 30.1.2. Chapter 29: the Stickelberger element and Problem 29.2.3. Chapter 32, Section 32.5: the coefficient ring $\mathcal{O}$ and the decomposition of Problem 32.5.3. Generalized Bernoulli numbers [Wa, Ch. 4], Gauss sums [Wa, Ch. 6], and Hilbert symbols [Se, Ch. III]. Throughout, ℓ is an odd prime, and for a finite extension $\mathcal{O}$ of $\mathbb{Z}_\ell$ the valuation $v_\mathcal{O}$ takes the value 1 on a uniformizer.

55.1. The two signs

Over $\mathbb{Q}$, odd twists are measured by Bernoulli numbers and even twists by the plus part of a class group (Section 30.2). The fields of the argument are the abelian CM fields

$$E = E(\psi,a,q,d) = A_\psi \cdot \mathbb{Q}(\zeta_{2^{a+2}})^+ \cdot \mathbb{Q}(\sqrt{-q}) \cdot \mathbb{Q}(\sqrt{-d}),$$

where A_ψ is the field cut out by a primitive Dirichlet character ψ, $a \geq 2$, and $q \equiv 3 \pmod 8$, $d \equiv 7 \pmod{16}$ are primes not dividing the conductor N_ψ [Zh, §5.3]. Which part of $\mathrm{Sha}_\ell(E,e)$ is measured by Bernoulli numbers? Let c be complex conjugation, which acts on $\mathrm{Sha}_\ell(E,e)$. The *plus part* $\mathrm{Sha}_\ell^+(E,e)$ is the subgroup on which c acts by $(-1)^e$, the *minus part* $\mathrm{Sha}_\ell^-(E,e)$ the subgroup on which it acts by $(-1)^{e+1}$, and $h_{\ell,e}^\pm(E)$ are their lengths.

Problem 55.1.1. Let R be a commutative ring with $2 \in R^\times$, M an R-module of finite length, and c an R-linear involution of M. Then $M = M^{c=1} \oplus M^{c=-1}$ and $\operatorname{len} M = \operatorname{len} M^{c=1} + \operatorname{len} M^{c=-1}$. Hence $h_{\ell,e}(E) = h_{\ell,e}^+(E) + h_{\ell,e}^-(E)$.

Problem 55.1.2. Let $\ell \nmid [E:\mathbb{Q}]$. In the decomposition of Problem 32.5.3, c acts on the summand of a character η of $\mathrm{Gal}(E/\mathbb{Q})$ by $\eta(-1)$. Hence $\mathrm{Sha}_\ell^-(E,e) \otimes \mathcal{O}$ is the sum of the summands of the η that are critical for e, that is, with $\eta(-1) = (-1)^{e+1}$.

Problem 55.1.3. 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.

Problem 55.1.4. $[E:\mathbb{Q}]$ divides 2^{a+2} times the order of ψ. Hence every odd prime dividing $[E:\mathbb{Q}]$ divides the order of ψ.

So on the minus part an L-value is available, and the primes $\ell \mid [E:\mathbb{Q}]$ form a fixed finite set.

55.2. The bound by Bernoulli numbers

The Lean formalization bounds each critical summand by one generalized Bernoulli number.

Date: November 26, 2026.

Theorem 55.2.1 (Bernoulli bound)**.** *Let $E \subseteq \mathbb{Q}(\zeta_N)$ be an abelian CM field, $\ell \nmid [E:\mathbb{Q}]$, $e \geq 1$, and $\eta\colon \mathrm{Gal}(E/\mathbb{Q}) \to \mathcal{O}^\times$ a character with $\eta(-1) = (-1)^{e+1}$. View η as a Dirichlet character modulo N, with primitive character η_0. Then*

$$\mathrm{len}_{\mathcal{O}} \mathrm{Sha}_\ell(\mathbb{Q}, e; \eta)_{\mathcal{O}} \leq v_{\mathcal{O}}\Big(N \prod_{p \leq e+2} p \cdot B_{e+1,\eta_0}\Big),$$

the product over primes p.

Status: proved in the Lean formalization from Poitou–Tate duality and an orthogonality law for unramified classes, by the method of Section 55.3; we have read the statements of its steps, not their proofs. The main conjecture of Mazur and Wiles [MW] is not used. Theorem 55.2.1 is a bound in one direction only; for $E = \mathbb{Q}(\zeta_\ell)$ and $\eta = 1$, Theorem 30.1.2 gives the exact value, and Problem 55.4.3 compares the two. The method is Rubin's, with Kolyvagin's Euler systems of Gauss sums [Ru91], [La, Appendix].

Problem 55.2.1. Let χ be a Dirichlet character of conductor $f \mid N$ and $k \geq 1$. Then $N \prod_{p \leq k+1} p \cdot B_{k,\chi}$ is an algebraic integer.

Problem 55.2.2. For $k \geq 2$ and $0 \leq s \leq 1$, $|B_k(s)| \leq 4\,k!/(2\pi)^k$. Hence, using $\prod_{p \leq n} p < 4^n$, $\big|N \prod_{p \leq k+1} p \cdot B_{k,\chi}\big| \leq 16N^{k+1}k!$ for every χ of conductor dividing N.

The size of one number controls every ℓ at once, as in Problem 30.2.4.

Problem 55.2.3. Let M_e be the product of the numbers $N \prod_{p \leq e+2} p \cdot B_{e+1,\eta_0}$ over the characters η of $\mathrm{Gal}(E/\mathbb{Q})$ critical for e. Then M_e is a nonzero rational integer, and

$$\sum_{\ell \nmid [E:\mathbb{Q}]} h^-_{\ell,e}(E) \log \ell \leq \log|M_e| \leq [E:\mathbb{Q}] \log\big(16N^{e+2}(e+1)!\big),$$

the sum over odd primes ℓ.

Problem 55.2.4. For $t \geq 2$ and $N \geq 1$, $\sum_{1 \leq e < t} \log\big(16N^{e+2}(e+1)!\big) \leq 3t^2 \log(tN)$.

At the finitely many odd ℓ dividing $[E:\mathbb{Q}]$ the idempotents of $\mathcal{O}[\mathrm{Gal}(E/\mathbb{Q})]$ are not integral, and the formalization uses annihilators instead.

Problem 55.2.5. Let A be 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.

Problem 55.2.6. If a finite $\mathbb{Z}_\ell$-module M is killed by ℓ^r, then $\mathrm{len}\, M \leq r \dim_{\mathbb{F}_\ell} M[\ell]$.

Lemma 55.2.2 (Stickelberger bound)**.** *There is an absolute constant C such that, for every abelian CM field $E \subseteq \mathbb{Q}(\zeta_N)$ satisfying a condition at ℓ that holds for the fields $E(\psi, a, q, d)$, and every $e \geq 1$, $h^-_{\ell,e}(E) \log \ell \leq C\ell[E:\mathbb{Q}]^2(e+1)\log^2(e\ell N)$.*

Status: proved in the Lean formalization from a Stickelberger element at modulus $N\ell$, Problem 55.2.5 for the exponent, and a separate bound for the ℓ-rank, combined by Problem 55.2.6, as described in [Zh, §5.4]. We have not transcribed the condition at ℓ or read the proof.

Problems 55.1.1–55.2.6, Theorem 55.2.1 and Lemma 55.2.2 prove the following, with N the conductor of E.

Theorem 55.2.3 (the minus part)**.** *There is an absolute constant C such that for every $E = E(\psi, a, q, d)$ and every $t \geq 2$,*

$$\sum_{\ell} \log \ell \sum_{1 \leq e < t} h^{-}_{\ell,e}(E) \leq 3[E:\mathbb{Q}]t^2 \log(tN) + C \sum_{\ell} \ell [E:\mathbb{Q}]^2 t^2 \log^2(t\ell N),$$

the first sum over odd primes ℓ, the second over the odd primes dividing the order of ψ.

Status: proved in the Lean formalization; it is part (II) of Theorem 52.4.2. It holds at every scale: no window is needed for the minus part.

55.3. Gauss sums and the Euler system

How does one bound a Selmer group from above by an L-value without the main conjecture? Kolyvagin's idea, in Rubin's version for class groups [Ru91]: Gauss sums at auxiliary primes $r \equiv 1 \pmod{\ell^m}$ give Kummer classes whose ramification is known; *derivative* classes built from them are unramified outside a few chosen primes; and a reciprocity law kills one generator of the dual Selmer group at a time. The formalization follows this route with Jacobi sums, auxiliary primes chosen by Chebotarev's theorem, and the twist by χ_ℓ^{-e}. The size of the Stickelberger value at the start is then compared with the Bernoulli number of Theorem 55.2.1. We state the checkable pieces.

For $F \geq 2$, b prime to F, and t prime to F, let $\tilde{t} \in [1, F)$ represent t, and put

$$\vartheta_F(b,t) = \lfloor b\tilde{t}/F \rfloor - \lfloor b(F-\tilde{t})/F \rfloor.$$

Let $\theta_F = \frac{1}{F}\sum_t \tilde{t}\,\sigma_t^{-1} \in \mathbb{Q}[G]$, $G = (\mathbb{Z}/F)^\times$, be the Stickelberger element of Chapter 29 at modulus F.

Problem 55.3.1. $\vartheta_F(b,t) = 2\lfloor b\tilde{t}/F \rfloor - b + 1$, and $\sum_t \vartheta_F(b,t)\sigma_t^{-1} = 2(b-\sigma_b)\theta_F - (b-1)\sum_t \sigma_t$. For $F = 5$, $b = 2$ the values at $\tilde{t} = 1, 2, 3, 4$ are $-1, -1, 1, 1$.

For a Dirichlet character χ modulo F (not necessarily primitive) put $B_{k,\chi}^{(F)} = F^{k-1}\sum_{a=1}^{F} \chi(a) B_k(a/F)$, and $d_k = 2k\prod_{p \leq k+1} p$.

Problem 55.3.2. Let $\ell^m \mid F$, $e \geq 1$, b prime to F, and χ a character modulo F with $\chi(-1) = (-1)^{e+1}$. Then

$$d_{e+1}\Big(b^e\chi(b)\sum_t \vartheta_F(b,t)\,\tilde{t}^{\,e}\chi(t) - 2\big(\chi(b)b^{e+1} - 1\big)\frac{B_{e+1,\chi}^{(F)}}{e+1}\Big) \equiv 0 \pmod{\ell^m}.$$

For $F = 5$, $e = 1$, $b = 2$ and χ trivial the expression in parentheses (before multiplication by $d_2 = 24$) is 10; for $F = 25$ it is 250.

So the Stickelberger value $\sum_t \vartheta_F(b,t)\tilde{t}^{\,e}\chi(t)$ is, modulo ℓ^m, a Bernoulli number times an explicit factor; the factor $\chi(b)b^{e+1} - 1$ is a unit for a suitable b unless $b \mapsto \chi(b)b^{e+1}$ is trivial modulo the maximal ideal. In that case the group vanishes.

Problem 55.3.3. Let $\eta = \omega^j$ with $j \equiv -e - 1 \pmod{\ell - 1}$, so that $W_e \otimes \eta^{-1}$ is congruent to $\mathbb{Z}/\ell(1)$. Then $\mathrm{Sha}_\ell(\mathbb{Q}, e; \eta) = 0$.

The derivative classes rest on an identity in the group ring of a cyclic group.

Problem 55.3.4. 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 last ingredient is a reciprocity law: for a global class, the local invariants sum to zero, so if all but one vanish, so does the last. Hilbert's law is the simplest instance.

Problem 55.3.5. 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 $(a,b)_r=1$.

Status of the assembly: in the Lean formalization, the reciprocity law used is deduced from Poitou–Tate duality and the orthogonality of unramified local classes; a system of derivative classes is constructed from Jacobi sums; the length of the η-summand is bounded by the valuation of a Stickelberger value at an auxiliary level $F=f\ell^m$; and Problem 55.3.2 identifies that value with the Bernoulli number of Theorem 55.2.1. We have read the statements of these steps but not the proofs of the bound by the Stickelberger value or of the reciprocity law. Zhang describes the same route [Zh, §5.4].

55.4. Examples

Problem 55.4.1. Let $\ell=37$, $E=\mathbb{Q}(\zeta_{37})$, $N=37$, $e=1$, and $\eta=\omega^j$ with j even. The bound of Theorem 55.2.1 is $1+v_{37}(B_{2,\omega^j})$. It equals 2 for $j=30$, 0 for $j=34$, and 1 for the other even j with $0\le j<36$.

For $j=30$ the 37-torsion of the summand is $\mathrm{Hom}(A^{(5)},\mathbb{F}_{37})$ by Problem 30.2.2, with $A^{(5)}\neq 0$ (Problem 29.2.8); for $j=34$ it vanishes by Problem 55.3.3, and the bound sees this.

Problem 55.4.2. Let $E=\mathbb{Q}(\zeta_\ell)$, $N=\ell$ and $\eta=1$. For odd e, Theorem 55.2.1 gives $h_{\ell,e}(\mathbb{Q})\le v_\ell(B_{e+1})+1+\delta$, with $\delta=1$ if $\ell\le e+2$ and $\delta=0$ otherwise. For $\ell=691$, $e=11$ the bound is 2, while $h_{691,11}(\mathbb{Q})=1$.

Problem 55.4.3. If e is odd and $(\ell-1)\nmid(e+1)$, the bound of Problem 55.4.2 exceeds the value given by Theorem 30.1.2 by exactly $1+\delta+v_\ell(e+1)$.

The loss is a bounded number of factors $\log\ell$ per twist, harmless against $\sqrt{b}$. On the plus part no L-value is available, and the next ingredient must replace the Bernoulli number by an integer built from automorphic forms.

In the Lean formalization. In [Lean] the two eigenspaces are `ShaPlus` and `ShaMinus`, with lengths `plusLen` and `minusLen`; Problem 55.1.1 is `length_eq_add_eigen` and `shaLen_eq_add`. Theorem 55.2.1 is `Odd.PsiBound`, proved by `ML.iv` through `ML.psiOf` and `ML.vChar`; the Bernoulli number with its factor is `alN`. The reciprocity law is `ML.Rec`, proved by `ML.recip` from `UnramifiedOrthogonality`; the derivative classes are `NuSys`, built by `kolInit`, `kolStep` and `nuSysEx` from Jacobi sums (`xJac`) and primes chosen by `chebQ`; the bound by the Stickelberger value is `ML.count`, the choice of level `ML.zEval`, Problem 55.3.2 is `ML.zCong` with ϑ_F the function `th`, and Problem 55.3.3 is the analogue over $\mathbb{Q}$ of `ML.exc`. Problem 55.2.3 is `PrimeBound`, Lemma 55.2.2 is `StickBound`, and Theorem 55.2.3 is `ThmBcFree`, from `thmBc_of`.

Hints

§55.1.

55.1.1: The projections $(1\pm c)/2$.

55.1.2: The action of $\gamma\in\mathrm{Gal}(E/\mathbb{Q})$ in Section 32.5, with $\gamma=c$.

55.1.3: $B_k(1-s) = (-1)^k B_k(s)$; 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 $L(k,\bar{\chi}) \neq 0$.

55.1.4: Degrees of the four fields in the compositum.

§55.2.

55.2.1: Expand $f^{k-1}B_k(a/f)$ in powers of a, and apply von Staudt–Clausen to the coefficients.

55.2.2: The Fourier series of $B_k(s)$, and $\zeta(k) \leq \zeta(2)$.

55.2.3: Theorem 55.2.1, Problems 55.1.2, 55.1.3, 55.2.1 and 55.2.2; the set of critical characters is stable under $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, and $\mathrm{len}_{\mathcal{O}}(M \otimes \mathcal{O}) = v_{\mathcal{O}}(\ell)\,\mathrm{len}_{\mathbb{Z}_\ell} M$.

55.2.4: Bound each of the three factors by a power of tN.

55.2.5: The Cayley–Hamilton theorem for multiplication by z.

55.2.6: Decompose M into cyclic modules.

§55.3.

55.3.1: $F \nmid b\tilde{t}$; then Problem 29.2.3 at modulus F.

55.3.2: Write $b\tilde{t} = r_t + F\lfloor b\tilde{t}/F \rfloor$, expand $\left(r_t + F\lfloor b\tilde{t}/F\rfloor\right)^{e+1}$ and sum over t; compare $\sum_a \chi(a)a^k$ with $FB_{k,\chi}^{(F)}$ through the expansion of $B_k(s)$; pair t with $F - t$.

55.3.3: Problem 30.2.2; which eigenspace of A appears?

55.3.4: Telescope, using $\sigma^M = 1$.

55.3.5: The formulas for $(a,b)_v$ and the product formula [Se, Ch. III, §2].

§55.4.

55.4.1: Compute $B_{2,\omega^j} = 37\sum_{a=1}^{36} \omega(a)^j B_2(a/37)$ in $\mathbb{Z}_{37}$ to a few digits; for $j = 0$ use $\eta_0 = 1$.

55.4.2: $\eta_0 = 1$, $B_{12} = -691/2730$, and Theorem 30.1.2.

55.4.3: $B_{e+1}/(e+1)$ is ℓ-integral when $(\ell-1) \nmid (e+1)$ [Wa, Cor. 5.14].

References

[La] S. Lang, *Cyclotomic Fields I and II*, combined 2nd ed., with an appendix by K. Rubin, Grad. Texts in Math. 121, Springer, 1990.

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

[MW] B. Mazur and A. Wiles, *Class fields of abelian extensions of* $\mathbf{Q}$, 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.

[Zh] R. Zhang, *A preliminary note on Alpöge's proposed proof of the generalized Riemann hypothesis*, 22 November 2026, `https://hexagonmath.org/pdf/2611.00809v1`.