THE PLUS PART, BY CONGRUENCES

Prerequisites. Chapter 55, Section 55.1: the fields $E = E(\psi, a, q, d)$, the plus part $\mathrm{Sha}_\ell^+(E, e)$ and its length $h_{\ell,e}^+(E)$. Chapter 30: W_e, $\mathrm{Sha}_\ell(\mathbb{Q}, e; \eta)$ and Problem 30.2.7. Chapter 32, Section 32.5: the coefficient ring $\mathcal{O}$, with ramification index $e_\mathcal{O}$ over $\mathbb{Z}_\ell$. Chapter 33: the length bound of Theorem 33.4.1 and its factor two (Section 33.5). Chapter 54: layers. Galois representations attached to modular forms, Bloch–Kato Selmer groups [BK], and Bertrand's postulate [AZ, Ch. 2]. Throughout, ℓ is an odd prime, $N = \mathrm{lcm}(2^{a+2}, N_\psi)qd$ is the modulus of E, and v_ℓ is normalized by $v_\ell(\ell) = 1$.

56.1. Characters and cases

On the plus part no L-value is available (Problem 55.1.3). How can one bound it at all, uniformly in ℓ and e? The answer in the formalization is a case analysis over (ℓ, e, η), with a different arithmetic argument in each case, and in the main case an integer built from automorphic forms in place of a Bernoulli number. First the reduction to characters. For a character η modulo N with values in $\mathcal{O}$, let $\mathrm{Sha}_\ell^{(N)}(\mathbb{Q}, e; \eta)$ be the group of classes in $\mathrm{Sha}_\ell(\mathbb{Q}, e; \eta)_\mathcal{O}$ that vanish also on the decomposition groups at the primes dividing N. The character η is *plus for* e if $\eta(-1) = (-1)^e$.

Lemma 56.1.1 (reduction to characters)**.** *If $\ell \nmid [E : \mathbb{Q}]$ and $e \geq 1$, then $e_\mathcal{O}\, h_{\ell,e}^+(E) \leq \sum_\eta \mathrm{len}_\mathcal{O} \mathrm{Sha}_\ell^{(N)}(\mathbb{Q}, e; \eta)$, the sum over the characters η of $\mathrm{Gal}(E/\mathbb{Q})$ that are plus for e.*

Status: proved in the Lean formalization; we have read the statement, not the proof. Without the extra local conditions it would follow from Problems 32.5.3 and 55.1.2.

Problem 56.1.1. $\mathrm{Sha}_\ell^{(N)}(\mathbb{Q}, e; \eta) \subseteq \mathrm{Sha}_\ell(\mathbb{Q}, e; \eta)_\mathcal{O}$. Hence, if $\ell \geq 5$, $e \geq 2$ is even and $(\ell - 1) \mid 2e$, the summand of the trivial character vanishes.

Let o be the order of ψ. Let p_K be the least prime $p \equiv 3 \pmod 4$ with $p \geq 7$ and $p \nmid N_\psi$, let h_* be the class number of $\mathbb{Q}(\sqrt{-p_K})$, and let p_1 be the least prime $p \equiv 1$ modulo the odd part of o with $p \nmid 2N_\psi p_K$. The set of *bad primes* of ψ is

$$\mathcal{B}_\psi = \{3\} \cup \{\text{odd primes dividing } o\, N_\psi\, p_K\, h_*\, p_1\}.$$

It depends only on ψ. The role of p_K and h_* is presumably to supply the imaginary quadratic field of Section 56.2; we have not checked this, nor traced the role of p_1.

Problem 56.1.2. For $\psi = 1$, $\mathcal{B}_\psi = \{3, 7\}$. For the quadratic character of conductor 5, $\mathcal{B}_\psi = \{3, 5, 7\}$. For a character of order 3 and conductor 7, $p_K = 11$, $h_* = 1$, $p_1 = 13$ and $\mathcal{B}_\psi = \{3, 7, 11, 13\}$.

Problem 56.1.3. Let $\ell \notin \mathcal{B}_\psi$ and let η be a character of $\mathrm{Gal}(E/\mathbb{Q})$. Then $\ell \nmid [E : \mathbb{Q}]$, $\ell \nmid o(\eta)$, and the component of η at ℓ (its restriction to $(\mathbb{Z}/\ell^{v_\ell(N)})^\times$) has order at most 2.

Date: November 26, 2026.

Let $\chi_P(\eta)$ be the character obtained from η by removing its part of ℓ-power order and then its component at ℓ. For $0 < e < t$ and η plus for e, the formalization distinguishes:

I $\ell \notin \mathcal{B}_\psi$ and $(\ell-1) \nmid 2e$;
Z $\ell \notin \mathcal{B}_\psi$, $(\ell-1) \mid 2e$ and $\eta = 1$;
II $e \geq 2$, the order of $\chi_P(\eta)$ is even, and $\ell \in \mathcal{B}_\psi$ or $(\ell-1) \mid 2e$;
III $\ell \notin \mathcal{B}_\psi$, $(\ell-1) \mid 2e$, $\eta \neq 1$ and the order of η is odd;
IV $\ell \in \mathcal{B}_\psi$, $e \geq 2$ and the order of $\chi_P(\eta)$ is odd;
V $\ell \in \mathcal{B}_\psi$ and $e = 1$.

Problem 56.1.4. Suppose $2t+1 < q$ and $2t+1 < d$. Then every triple (ℓ, e, η) as above lies in at least one of the cases I–V and Z. In Cases II and III with $\ell \notin \mathcal{B}_\psi$, $\ell \leq 2e+1 < 2t+1$.

Case Z vanishes by Problem 56.1.1. Cases II and III have ℓ small, Case I has ℓ arbitrary, and Cases II, IV and V with $\ell \in \mathcal{B}_\psi$ involve finitely many ℓ.

56.2. The congruence integer

In Case I the Bernoulli number of the minus part is replaced by an integer. Let K be an imaginary quadratic field, w a prime of K above a prime $p \geq 7$ with $p \nmid N\Delta_K$, $Q = |\mathcal{O}_K/w|$, $\ell \neq p$, $\sigma \in G_K$ an arithmetic Frobenius at w, and $\Psi = \eta\chi_\ell^e$, a character of $G_\mathbb{Q}$ that we also restrict to G_K. Since $\Psi \oplus 1 \oplus \Psi^{-1}$ is self-dual, σ and σ^{-1} have the same trace on it. For a root of unity z put

$$t_z = Q^{-e}z + 1 + Q^e z^{-1}.$$

Problem 56.2.1. The trace of σ^{-1} on $\Psi \oplus 1 \oplus \Psi^{-1}$ is t_z with $z = \eta(\sigma)^{-1}$, and $Q^e t_z$ is an algebraic integer.

The representations that may be congruent to this Eisenstein point are three-dimensional representations ρ of G_K of two kinds, called *admissible* below: those attached to automorphic representations of a unitary group in three variables with weights $(e, 0, -e)$ and bounded level, and those of the form $1 \oplus W$ with W attached to a newform of weight $2e+1$. We have not transcribed the precise conditions.

Lemma 56.2.1 (one character)**.** *Let K, ℓ, e, N and η satisfy: $e \geq 1$, N even, $\ell \nmid o(\eta)$, the component of η at ℓ has order at most 2, η is plus for e, $\ell \nmid \Delta_K h_K$, $(\Delta_K, N) = 1$, $(\ell-1) \nmid 2e$, and a further condition relating K and η. Let $\sigma \in G_K$ and $t = \Psi(\sigma) + 1 + \Psi(\sigma)^{-1}$, and suppose $\operatorname{tr}\rho(\sigma) \neq t$ for every admissible ρ. Then $\mathrm{Sha}_\ell^{(N)}(\mathbb{Q}, e; \eta)$ is finite, and there is a finite set X of pairwise non-isomorphic admissible ρ with*

$$\operatorname{len}_\mathcal{O} \mathrm{Sha}_\ell^{(N)}(\mathbb{Q}, e; \eta) \leq 2e_\mathcal{O} \sum_{\rho \in X} v_\ell\big(\operatorname{tr}\rho(\sigma) - t\big).$$

Lemma 56.2.2 (the integer)**.** *For each K there are c and A with the following property. Let $e, N \geq 1$, p, w, Q be as above, and (z_o) a finite family of roots of unity, stable under $\mathrm{Aut}(\mathbb{C})$. There is a nonzero integer M with $\log|M| \leq c \cdot \#(z_o) \cdot (N(e+1))^A \log p$ such that, for every odd $\ell \neq p$ and all finite sets X_o of pairwise non-isomorphic admissible ρ, one has $\operatorname{tr}\rho(\sigma^{-1}) \neq t_{z_o}$ and $v_\ell(M) \geq \sum_o \sum_{\rho \in X_o} v_\ell\big(\operatorname{tr}\rho(\sigma^{-1}) - t_{z_o}\big)$.*

Status: both lemmas are proved in the Lean formalization; we have read their statements, not their proofs. The first is a bound for a Selmer group by trace differences at congruent points, of the kind modelled in Theorem 33.4.1, with the factor two of Section 33.5; its proof uses deformation rings, automorphy lifting and the input of Section 56.3. The second counts automorphic forms on a unitary group in three variables. Zhang describes both [Zh, §5.4].

Here is why such an integer exists, in a model.

Problem 56.2.2. If the eigenvalues of $\rho(\sigma^{-1})$ have absolute value 1 under an isomorphism $\overline{\mathbb{Q}}_\ell \simeq \mathbb{C}$, then $\operatorname{tr}\rho(\sigma^{-1}) \neq t_z$.

Problem 56.2.3. Let $a_1, \dots, a_D$ be algebraic numbers, permuted by $\mathrm{Aut}(\mathbb{C})$, with $Q^e a_s$ integral and $|a_s| \leq 3$ in every complex embedding, and let (z_o) be as in Lemma 56.2.2. Then $M = \prod_o \prod_s Q^e(a_s - t_{z_o})$ is a nonzero integer, $\log|M| \leq D \cdot \#(z_o) \cdot (2e \log Q + 1)$, and $v_\ell(M) = \sum_{o,s} v_\ell(a_s - t_{z_o})$ for $\ell \neq p$.

Problem 56.2.4. Fix an isomorphism $\overline{\mathbb{Q}}_\ell \simeq \mathbb{C}$, and assume the hypotheses of Lemma 56.2.1, other than the trace condition, for every η in an orbit of characters under $\mathrm{Aut}(\mathbb{C})$. Then Lemmas 56.2.1 and 56.2.2, applied to the family (z_η) indexed by the η in this orbit, with $z_\eta = \eta(\sigma)^{-1}$, give $\sum_\eta \operatorname{len}_{\mathcal{O}} \operatorname{Sha}_\ell^{(N)}(\mathbb{Q}, e; \eta) \leq 2e_{\mathcal{O}} v_\ell(M)$ for $\ell \neq p$.

Problem 56.2.5. Let $p \neq p'$, M_p, $M_{p'}$ nonzero integers, and suppose that $L_\ell \leq 2v_\ell(M_p)$ for odd $\ell \neq p$ and $L_\ell \leq 2v_\ell(M_{p'})$ for odd $\ell \neq p'$. Then $\sum_\ell L_\ell \log \ell \leq 2\log|M_p| + 2\log|M_{p'}|$, the sum over odd ℓ.

Problem 56.2.6. The two least primes $p < p'$ with $p \geq 7$ and $p, p' \nmid 30N\Delta_K$ satisfy $\log p' \leq C(1 + \log(N|\Delta_K|))$, with C absolute.

56.3. Kato's vanishing

At the points $1 \oplus W$ the deformation argument must not see Selmer classes of W itself. Let θ be the quadratic character of K.

Problem 56.3.1. Let V be a two-dimensional representation with $\det V = \theta$. Then $\mathrm{Hom}(1, V) \oplus \mathrm{Hom}(V, 1) \cong V \oplus (V \otimes \theta)$.

Problem 56.3.2. If $\operatorname{tr} W \equiv \theta\Psi + \Psi^{-1}$ modulo the maximal ideal, then on G_K the trace of $1 \oplus W$ is congruent to $t = \Psi + 1 + \Psi^{-1}$: the point $1 \oplus W$ is congruent to the Eisenstein point.

Lemma 56.3.1 (Kato)**.** *Let W be a two-dimensional ℓ-adic representation of $G_{\mathbb{Q}}$ that is a Tate twist of the representation of a newform of weight $2e + 1$, with $\det W = \theta$, satisfying further conditions we do not transcribe. Then the Bloch–Kato Selmer groups $H^1_f(\mathbb{Q}, W)$ and $H^1_f(\mathbb{Q}, W \otimes \theta)$ vanish.*

Status: Kato proved the finiteness of the Selmer groups of modular forms at the critical twists other than the central one [Ka, Thm. 14.2], which gives this vanishing at the relevant twists [Zh, §5.4]. In the Lean formalization Lemma 56.3.1 is an input of the proof of Lemma 56.2.1; we have not read how it is established there.

Problem 56.3.1 says that the two components of an adjoint class at $1 \oplus W$ are classes for W and $W \otimes \theta$, so Lemma 56.3.1 removes them.

56.4. The plus part

Problem 56.4.1. Suppose each pair (ℓ, η) in Cases II and III with $\ell \notin \mathcal{B}_\psi$ contributes $\operatorname{len}_{\mathcal{O}} \operatorname{Sha}_\ell^{(N)}(\mathbb{Q}, e; \eta) \log \ell \le (\ell N e)^C$, with $C \ge 1$; here $e_{\mathcal{O}} = 1$, since $\ell \nmid [E : \mathbb{Q}]$ by Problem 56.1.3. Then the sum of these contributions over ℓ, η and $1 \le e < t$ is at most $(Nt)^{5C+4}$.

Problem 56.4.2. Suppose $2t+1 < q$ and $2t+1 < d$. Assume Lemma 56.1.1, with $\mathcal{O}$ depending on ℓ, the bound of Problem 56.4.1, and for each $e < t$ the bound

$$\sum_\ell \log \ell \sum_\eta e_{\mathcal{O}}^{-1} \operatorname{len}_{\mathcal{O}} \operatorname{Sha}_\ell^{(N)}(\mathbb{Q}, e; \eta) \le (Nt)^C,$$

the sum over the ℓ in Case I. Then

$$\sum_{\ell \notin \mathcal{B}_\psi} \log \ell \sum_{1 \le e < t} h^+_{\ell,e}(E) \le 2(Nt)^{5C+4}.$$

In the formalization the bound for Case I comes from Problems 56.2.4–56.2.6; the bound $(\ell N e)^C$ in Cases II and III from a statement about automorphic forms on the group GSp_4 of symplectic similitudes in four variables, whose content we have not traced; and Case V from a lifting argument for unitary groups that uses the nonvanishing of a Bernoulli number modulo ℓ; Zhang describes unitary groups over $\mathbb{Q}(i)$ here [Zh, §5.4]. At $\ell \in \mathcal{B}_\psi$, Case IV and part of Case V are reduced to the fixed layers of Chapter 54. The hypothesis used there is a bound B on layers: for every $\ell \in \mathcal{B}_\psi$ and the layer L of degree $\ell^{j(\ell)}$ over $\mathbb{Q}(\zeta_{\ell N_\psi})$,

$$\sum_{1 \le e < t} h_{\ell,e}(L) \le B.$$

The result is the following.

Theorem 56.4.1 (the plus part)**.** *Let ψ be primitive and j a function on primes. There are C and primes r_1, r_2 such that the following holds. Let $E = E(\psi, a, q, d)$ with $q, d > \max(r_1, r_2, 2t+1, N_\psi, o, p_K, h_*, p_1)$, $t \ge 2$, and suppose the bound B on layers holds. Then*

$$\sum_\ell \log \ell \sum_{1 \le e < t} h^+_{\ell,e}(E) \le (Nt)^C + CB,$$

the sum over odd primes ℓ.

Status: proved in the Lean formalization. For $\ell \notin \mathcal{B}_\psi$ it is Problem 56.4.2 with the case bounds above. We have not read the treatment of $\ell \in \mathcal{B}_\psi$, which uses a version of Lemma 56.1.1 with a loss term when $\ell \mid [E : \mathbb{Q}]$. With $B = \exp(x^{4\varepsilon/5})$ on the windows of the next chapter, Theorem 56.4.1 is the bound for P_+ in part (I) of Theorem 52.4.2.

Problem 56.4.3. If e is even and $\ell \nmid [E : \mathbb{Q}]$, then $h_{\ell,e}(\mathbb{Q}) \le h^+_{\ell,e}(E)$.

What remains. The theorem is a uniform weakening of Vandiver's conjecture for the fields E. For $\psi = 1$, $a = 2$, and q, d the least admissible primes above $\max(r_1, r_2, 2t+1, 7)$, which are of size polynomial in t by the prime number theorem in arithmetic progressions, Problems 56.4.2 and 56.4.3 bound $\sum_{\ell \ne 3,7} \log \ell \sum_{e<t,\ e \text{ even}} h_{\ell,e}(\mathbb{Q})$ by a polynomial in t: the kind of bound asked for at the end of Chapter 30. Its proof is the part of the argument that we have been

able to follow least: Lemmas 56.1.1, 56.2.1, 56.2.2 and 56.3.1, and the cases with GSp_4, are proved in the formalization by long arguments that we have not read.

In the Lean formalization. In [Lean] Lemma 56.1.1 is `HV.redPrime`; the group $\mathrm{Sha}_\ell^{(N)}(\mathbb{Q}, e; \eta)$ has length `Vlen`. The set $\mathcal{B}_\psi$ is `Bchi`, with `pK`, `hStar`, `pOne`; the cases are `Host.CaseI`, ..., `Host.CaseV` and `CaseZ`, with $\chi_P(\eta)$ the character `chiP`. Lemma 56.2.1 is `OneCharU_s`, with hypotheses `GD` and admissible representations `Adm3U_s` or `Adm2A`; Lemma 56.2.2 is `NumberU3U_s`, with t_z the function `eis3`; Problem 56.2.4 is `propGK_of_numberU3U_of_oneCharU`, and Problem 56.2.5 is the passage from `PropGK` to `CorGK`. Lemma 56.3.1 is `KatoTwoW`. The case bounds are `CountI`, `CountII`, `CountIII`, `CountIV`, `CountV`, `CountZ`, the second and third from `SymplecticFourImageDense`; the bound on layers is `LayerLe`, and Theorem 56.4.1 is `PointHV`, from `sumIn` and `sumOut`.

Hints

§56.1.

56.1.1: More local conditions give a smaller group; then Problem 30.2.7.
56.1.2: $h(\mathbb{Q}(\sqrt{-7})) = h(\mathbb{Q}(\sqrt{-11})) = 1$.
56.1.3: Problem 55.1.4; the characters of $\mathrm{Gal}(E/\mathbb{Q})$ are generated by ψ, characters of 2-power conductor, and the Legendre symbols modulo q and d.
56.1.4: If $(\ell - 1) \mid 2e$, compare ℓ with q and d.

§56.2.

56.2.1: $\chi_\ell(\sigma) = Q$.
56.2.2: $|t_z| \geq Q^e - 1 - Q^{-e}$ and $Q \geq 7$.
56.2.3: $|Q^e(a_s - t_z)| \leq Q^{2e} + 4Q^e + 1 \leq 2Q^{2e}$; the product is fixed by $\mathrm{Aut}(\mathbb{C})$; Problem 56.2.2.
56.2.4: Take X_o to be the set X of Lemma 56.2.1 for the character of index o, with σ replaced by σ^{-1}.
56.2.5: Every ℓ differs from p or from p'.
56.2.6: Bertrand's postulate gives a prime in each interval $(2^k, 2^{k+1}]$, and an integer $m \geq 1$ has at most $\log_2 m$ prime factors.

§56.3.

56.3.1: For a two-dimensional V, $V^\vee \cong V \otimes \det V^{-1}$.
56.3.2: θ is trivial on G_K.

§56.4.

56.4.1: At most $3t$ primes ℓ, t twists and N characters; $3t \leq t^3$.
56.4.2: Problems 56.1.3, 56.1.4 and 56.1.1; sum the Case I bound over $e < t$.
56.4.3: The summand of the trivial character in Problem 32.5.3, and Problem 55.1.2.

References

[AZ] M. Aigner and G. M. Ziegler, *Proofs from THE BOOK*, 6th ed., Springer, 2018.
[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.
[Ka] K. Kato, *p-adic Hodge theory and values of zeta functions of modular forms*, Astérisque **295** (2004), 117–290.

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

[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`.