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 $-n \leq r \leq m$, 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. $m+n \geq 1$. 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 $k \geq 2$ 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.