RIBET'S CONVERSE THEOREM

YU-SHENG LEE

In this note we discuss the relation between Eisenstein congruences and Ribet's converse to the Herbrand-Ribet theorem. Following [Ski09], we treat the theorem as a specialized case of the Iwasawa main conjecture and emphasize the role of the congruence modules. Throughout, let p be an odd prime, $\chi\colon G_{\mathbf{Q}} \to \mathbf{Z}_p^\times$ be the p-th cyclotomic character, and

$$\omega = \overline{\chi}\colon G_{\mathbf{Q}} \to Gal(\mathbf{Q}(\mu_p)/\mathbf{Q}) \to \mathbb{F}_p^\times \cong \mu_{p-1}$$

be the Teichmuller character.

1. The Herbrand-Ribet theorem

Let $A = Cl(\mathbf{Q}(\mu_p)) \otimes \mathbf{Z}_p$ be the p-primary part of the field $\mathbf{Q}(\mu_p)$. The action of $Gal(\mathbf{Q}(\mu_p)/\mathbf{Q})$ on A gives a decomposition

$$A = \bigoplus_{n=0}^{p-2} A_n$$

where the Galois group acts on A_n by ω^n. Recall that p is said to be irregular if $A \neq 0$, and we are interested in the finer problem of whether $A_n \neq 0$.

When n is even, the Kummer-Vandiver conjectuere states that A_n should be trivial. Using the Stickelberger elements, Herbrand has shown that $A_0 = A_1 = 0$, and if $A_{p-k} \neq 0$ for some even $k < p-1$, then p divides the k-th Bernoulli number B_k defined by

$$\frac{t}{e^t - 1} = \sum_{n=0}^{\infty} B_n \frac{t^n}{n!}.$$

We refer to [Was82] for a detailed discussion of these facts. On the other hand, Ribet has shown that the converse of Herbrand's result is also true.

Theorem 1.1. [Rib76] Let $2 \leq k < p-1$ be an even number. If $p \mid B_k$, then $A_{p-k} \neq 0$.

Remark 1.2. By the von Staudt theorem we have $\mathrm{val}_p(B_{p-1}) = -1$. This is compatible with the fact that $A_1 = 0$.

We first reinterpret A_n as Selmer groups. Let $G = G_{\mathbf{Q}}, H = G_{\mathbf{Q}(\mu_p)}, \Delta = Gal(\mathbf{Q}(\mu_p)/\mathbf{Q}) = G/H$ and $W = \mathbb{F}(\omega^n)$, define

$$H^1_f(\mathbf{Q}, W) := \ker\left(H^1(\mathbf{Q}, W) \to \prod_{\ell} H^1(I_\ell, W)\right).$$

Since $p \nmid \#\Delta$, we can stare at the inflation-restriction exact sequence

$$\begin{array}{ccccccc}
H^1(\Delta, W) & \longrightarrow & H^1(G, W) & \xrightarrow{\sim} & H^1(H, W)^{\Delta} & \longrightarrow & H^2(\Delta, W) \\
\| & & \downarrow & & \downarrow & & \| \\
0 & & H^1(I_\ell, W) & \hookrightarrow & \prod_{v|\ell} H^1(I_v, W) & & 0
\end{array}$$

and the isomorphism $H^1(H, W)^{\Delta} \cong \mathrm{Hom}_{\Delta}(H, W)$, then realize that

$$H^1_f(\mathbf{Q}, W) \cong H^1_f(\mathbf{Q}(\mu_p), W)^{\Delta} = \{\phi \in \mathrm{Hom}_{\Delta}(H, W) \mid f(I_v) = 0 \text{ for all } v\} = \mathrm{Hom}(A_n, \mathbb{F}).$$

To show that $A_n \neq 0$, it suffices to show that $H^1_f(\mathbf{Q}, \mathbb{F}(\omega^n))$ is nontrivial, or equivalently, that there exists a non-split extension of Galois representations

$$0 \to \mathbb{F}(\omega^n) \to \overline{\rho} \to \mathbb{F} \to 0$$

that splits everywhere locally. We will find such an extension by studying the congruences between Galois representations of modular forms.

Consider the classical level 1 Eisenstein series E_k of weight k

$$E_k = \frac{\zeta(1-k)}{2} + \sum_{n=1}^{\infty} \sigma_{k-1}(n) q^n, \quad k \geq 4.$$

The constant terms $\frac{\zeta(1-k)}{2} = \frac{-B_k}{2k}$ have the following congruence relations.

(1) The values B_k/k lie in $\mathbf{Z}_p$ if and only if $(p-1) \nmid k$.
(2) If $k \equiv k' \not\equiv 0 \mod (p-1)$, then

$$\frac{B_k}{k} \equiv \frac{B_{k'}}{k'} \mod p.$$

It follows that if $k < p-1$ is even and $p \mid B_k$, the Eisenstein series $E_{k+m(p-1)}$ have p-integral Fourier coefficients and the constant term is divisible by p. We may thus assume $k > 4$ and E_k is such an Eisenstein series. Then there exists $k = 4a + 6b$ such that

$$F := E_k - \frac{\zeta(1-k)}{2}(240E_4)^a(-504E_6)^b$$

is a nonzero level 1 cusp form of weight k. The Fourier coefficients of F are congruent to those of the Eisenstein series

$$a_\ell(F) \equiv a_\ell(E_k) = 1 + \ell^{k-1} \mod p.$$

Example 1.3. Consider $B_{12} = -691/2730$, then $E_{12} - (240E_4)^3$ is a nonzero multiple of the Ramanujan Δ function.

Let $S = S_k(1, \mathbf{Z}_p)$ be the space of cusp forms and $\mathbb{T} = \mathbb{T}_k(1, \mathbf{Z}_p) \subset \mathrm{End}_{\mathbf{Z}_p}(S)$ be the $\mathbf{Z}_p$-subalgebra generated by the Hecke operators. We have the following facts.

(1) The Hecke algebra $\mathbb{T}$ is reduced and finite flat over $\mathbf{Z}_p$.

(2) There exists a perfect bilinear pairing

$$\mathbb{T} \times S \to \mathbf{Z}_p, \quad (T, f) \mapsto a_1(Tf)$$

which identifies $S \cong \mathrm{Hom}(\mathbb{T}, \mathbf{Z}_p)$. A cusp form f is a Hecke eigenform if and only if it corresponds to a homomorphism of $\mathbf{Z}_p$-algebras.

(3) The $\mathbf{Q}_p$-algebra $\mathbb{T} \otimes \mathbf{Q}_p$ is semi-simple and has a decomposition $\mathbb{T} \otimes \mathbf{Q}_p = \prod_\lambda K_\lambda$ into finite extensions over $\mathbf{Q}_p$ There is a correspondence between the fields (or the minimal primes of $\mathbb{T}$) and the conjugacy classes of Hecke eigenforms.

Since E_k is a Hecke eigenform, the $\mathbf{Z}_p$-module homomorphism associated to F

$$\eta \colon \mathbb{T} \to \mathbb{F}_p, \quad T_\ell \mapsto a_\ell(F) \equiv 1 + \ell^{k-1} \mod p$$

becomes a ring homomorphism after modulo by p.

Lemma 1.4 (Deligne-Serre lifting)**.** There exists an eigenform $f \in S_k(1, \mathcal{O})$, where $\mathcal{O}$ is the ring of integer of a finite extension over $\mathbf{Q}_p$ with a uniformizer ϖ, such that

$$a_\ell(f) \equiv 1 + \ell^{k-1} \mod (\varpi).$$

Proof. We apply the going-down to the maximal ideal $\mathfrak{m} := \ker(\eta)$ in $\mathbb{T}$. Since $\mathfrak{m} \cap \mathbf{Z}_p = (p)$, there exists a minimal prime ideal $\mathfrak{p} \subset \mathbb{T}$ such that $\mathfrak{p} \cap \mathbf{Z}_p = (0)$. The quotient $\mathbb{T}/\mathfrak{p}$ is isomorphic to a ring $\mathcal{O}$ as in the statement. Let f be the eigenform corresponding to the ring homomorphism $\mathbb{T} \to \mathbb{T}/\mathfrak{p} \cong \mathcal{O}$. The congruence property follows from that (ϖ) pullbacks to $\mathfrak{m}$. □

The irreducible Galois representation associated to f

$$\rho_f \colon G_{\mathbf{Q}} \to \mathrm{GL}_2(K), \quad K = \operatorname{Frac} \mathcal{O}$$

is unramified away from p and satisfies $\mathrm{tr}\rho_f(\mathrm{Frob}_\ell) = a_\ell(f)$ for all $\ell \neq p$. It follows from

$$\mathrm{tr}\rho_f(\mathrm{Frob}_\ell) = a_\ell(f) \equiv 1 + \ell^{k-1} = 1 + \chi^{k-1}(\mathrm{Frob}_\ell) \mod (\varpi) \tag{1}$$

and the Chebotarev's density that $\mathrm{tr}\rho_f(\sigma) \equiv 1 + \chi^{k-1}(\sigma) \mod (\varpi)$ for all $\sigma \in G_{\mathbf{Q}}$. Therefore, the semi-simplified reduction $\overline{\rho}^{ss}$ is isomorphic to $\omega^{k-1} \oplus 1$. To find a lattice whose reduction gives the desired non-split extension (up to a twist), we need to employ Urban's lattice construction.

Proposition 1.5 ([Urb01])**.** Let $\rho \colon G_{\mathbf{Q}} \to \mathrm{GL}_2(K)$ be an irreducible Galois representation such that

$$\mathrm{tr}\rho \equiv \chi_1 + \chi_2 \mod \mathfrak{a} = (\varpi)^n.$$

for characters $\chi_i \colon G_{\mathbf{Q}} \to \mathcal{O}^\times$ that are distinct modulo (ϖ). Then there exists a stable lattice $\mathcal{L} \subset K^2$ whose reduction is a non-split extension between χ_1 and χ_2 modulo $\mathfrak{a}$.

Proof. Observe that $\det \rho(\sigma) = \mathrm{tr}\rho(\sigma^2) - \mathrm{tr}\rho(\sigma)^2/2$ and therefore

$$\det(X\mathbf{I} - \rho(\sigma)) \equiv (X - \chi_1(\sigma))(X - \chi_2(\sigma)) \mod \mathfrak{a}.$$

Since χ_i are distinct modulo (ϖ), we can pick $\sigma_0 \in G_{\mathbf{Q}}$ whose characteristic polynomial has distinct roots modulo (ϖ). By the Hensel lemma, the the roots lift to distinct eigenvalues in $\mathcal{O}$. We pick a basis $\{v_1, v_2\}$ of eigenvectors and write

$$\rho(\sigma_0) = \begin{pmatrix} \alpha_1 & \\ & \alpha_2 \end{pmatrix}, \quad \alpha_i \in \mathcal{O}, \quad \alpha_i \equiv \chi_i(\sigma_0) \mod \mathfrak{a}.$$

Since $\mathrm{tr}\rho(\sigma\sigma_0^n) \equiv \chi_1(\sigma\sigma_0^n) + \chi_2(\sigma\sigma_0^n) \mod \mathfrak{a}$, the relation

$$a_\sigma\alpha_1^n + d_\sigma\alpha_2^n \equiv \chi_1(\sigma)\alpha_1^n + \chi_2(\sigma)\alpha_2^n \mod \mathfrak{a}, \quad \rho(\sigma) = \begin{pmatrix} a_\sigma & b_\sigma \\ c_\sigma & d_\sigma \end{pmatrix}$$

holds for all n and $\sigma \in G_{\mathbf{Q}}$. And since $\{(1,1),(\alpha_1,\alpha_2)\}$ generate $\mathcal{O}^2$, we actually have

$$a_\sigma \equiv \chi_1(\sigma), \quad d_\sigma \equiv \chi_2(\sigma) \mod \mathfrak{a}$$

for all $\sigma \in G_{\mathbf{Q}}$ and thus

(1) $a_\sigma, d_\sigma \in \mathcal{O}$ for all $\sigma \in G_{\mathbf{Q}}$,
(2) $b_\sigma c_\tau = a_{\sigma\tau} - a_\sigma a_\tau \in \mathcal{O}$ for all $\sigma, \tau \in G_{\mathbf{Q}}$ and $b_\sigma c_\tau \equiv 0 \mod \mathfrak{a}$.

Let $C = \{c_\sigma \mid \sigma \in \mathcal{O}[G_{\mathbf{Q}}]\}$ be the $\mathcal{O}$-submodule in K generated by all $c_\sigma \in G_{\mathbf{Q}}$. Then C is nonzero because ρ is irreducible and it is actually a fractional ideal since the Galois group is compact. We put $\mathcal{L}_1 = \mathcal{O}v_1, \mathcal{L}_2 = Cv_2$ and $\mathcal{L} = \mathcal{L}_1 \oplus \mathcal{L}_2$, which is the stable lattice generated by v_1 over $\mathcal{O}[G_{\mathbf{Q}}]$. By above, the reduction of $\mathcal{L}$ modulo $\mathfrak{a}$ is an extension

$$0 \to \mathcal{O}/\mathfrak{a}(\chi_2) \cong \overline{\mathcal{L}}_2 \to \overline{\mathcal{L}} \to \overline{\mathcal{L}}_1 \cong \mathcal{O}/\mathfrak{a}(\chi_1) \to 0 \tag{2}$$

as $C/\mathfrak{a}C \cong \mathcal{O}/\mathfrak{a}$. We claim that $\overline{\mathcal{L}}$ has no quotient on which $G_{\mathbf{Q}}$ acts by χ_2. Otherwise

$$(\rho(\sigma_0) - \chi_2(\sigma_0))v_1 \equiv (\alpha_1 - \alpha_2)v_1 \mod \mathfrak{a},$$

and therefore v_1 lies in the kernel, which contradicts that v_1 generates $\mathcal{L}$. In particular, the extension gives a nontrivial class in $\mathrm{Ext}^1_{G_{\mathbf{Q}}}(\overline{\chi}_1, \overline{\chi}_2) = H^1(\mathbf{Q}, \mathcal{O}/\mathfrak{a}(\chi_2\chi_1^{-1}))$. □

Remark 1.6. The proposition was proved for the more general setting when $\mathcal{O}$ is local Henselian and $\overline{\rho}^{ss}$ is the sum of mutually non-isomorphic irreducible representations. We refer to [BC09, chapter 1] for a formulation of these results in terms of pseudo-representations and generalized matrix algebras.

Apply the construction to $\mathfrak{a} = (\varpi)$ and $(\chi_1, \chi_2) = (1, \chi^{k-1})$, we can obtain a nontrivial class in $H^1(\mathbf{Q}, \mathbb{F}(\omega^{k-1}))$ or $H^1(\mathbf{Q}, \mathbb{F}(\omega^{1-k}))$. In either case, the restriction to I_ℓ for $\ell \neq p$ is trivial since ρ_f is unramified away from p and the image of $\mathcal{L}_1$ in $\overline{\mathcal{L}}$ is a section of the extension in (2). To finish the proof, we need to use the fact that $a_p(f) \equiv 1 + p^{k-1} \equiv 1$ is a unit and thus f is ordinary.

Theorem 1.7. We say an eigenform f is p-ordinary if $a_p(f)$ is a p-unit. When this is the case,

$$\rho_f|_{I_p} \sim \begin{pmatrix} \chi^{k-1} & * \\ & 1 \end{pmatrix}.$$

Now, if the reduction of the lattice $\mathcal{L}$ is a non-split extension $0 \to \mathbb{F} \to \overline{\mathcal{L}} \to \mathbb{F}(\omega^{k-1}) \to 0$ and $\mathcal{F} \subset K^2$ is the subspace where I_p acts by χ^{k-1}, the reduction of $\mathcal{L} \cap F$ is a section of the extension when restricted to I_p. Therefore we have show that

$$0 \neq [\overline{\mathcal{L}}] \in H^1_f(\mathbf{Q}, \mathbb{F}(\omega^{1-k})) \cong \mathrm{Hom}(A_{p-k}, \mathbb{F}).$$

This completes the proof of Ribet's converse theorem.

2. Congruence modules

What happens when $\zeta(1-k)/2$ is divisible by higher powers of p? It is natural to expect that we will be able to construct non-split extensions in larger coefficients. Indeed, if the congruence relation (1) holds for $\mathfrak{a} = (\varpi^n)$, the same arguments will give a nontrivial class in

$$H^1_f(\mathbf{Q}, \mathcal{O}/\mathfrak{a}(\chi^{1-k})) := \ker\left(H^1(\mathbf{Q}, \mathcal{O}/\mathfrak{a}(\chi^{1-k})) \to \prod_\ell H^1(I_\ell, \mathcal{O}/\mathfrak{a}(\chi^{1-k}))\right).$$

However, the Deligne-Serre lifting lemma only works for prime ideals, and we have no control of the sizes of congruences for each minimal prime below $\mathfrak{m} = \ker(\eta)$. We therefore need to consider all these primes, or equivalently all the Hecke eigenforms congruent to E_k, at the same time.

Suppose $p^r \parallel \zeta(1-k)/2$. The ring homomorphism

$$\mathbb{T} \to \mathbf{Z}_p/(p^r), \quad T_\ell \mapsto 1 + \ell^{k-1} \mod (p^r)$$

factors through the ideal $I := (T_\ell - 1 - \ell^{k-1}) \subset \mathbb{T}$. Let J be the kernel of the surjective homomorphism $\mathbf{Z}_p \to \mathbb{T}/I$, the following commutative diagram shows that $J \subset (p^r)$.

$$\begin{tikzcd}
 & \mathbb{T}/I \arrow[r, "\eta"] \arrow[d] & \mathbb{T}/\mathfrak{m} \arrow[d, "\wr"] \\
\mathbf{Z}_p/J \arrow[ur, "\sim"] \arrow[r] & \mathbf{Z}_p/(p^r) \arrow[r] & \mathbb{F}_p
\end{tikzcd}$$

Let $\mathbb{T}_\mathfrak{m}$ be the localization, then the components of $K := \mathbb{T}_\mathfrak{m} \otimes \mathbf{Q}_p = \prod_\lambda K_\lambda$ corresponds to conjugacy classes of eigenforms that are congruent to E_k. If ρ_λ is the p-adic Galois representation associated to each eigenform, we write

$$\rho_\mathfrak{m} = \prod \rho_\lambda \colon G_\mathbf{Q} \to \mathrm{GL}_2(K) = \prod \mathrm{GL}_2(K_\lambda),$$

which is irreducible at each component and $\mathrm{tr}\rho_\mathfrak{m}(\mathrm{Frob}_\ell) = T_\ell \in \mathbb{T}_\mathfrak{m} \subset K$ if $\ell \neq p$. Since by tautology

$$\mathrm{tr}\rho_\mathfrak{m}(\mathrm{Frob}_\ell) = T_\ell \equiv \ell^{k-1} + 1 = \chi^{k-1}(\mathrm{Frob}_\ell) + 1 \mod I,$$

we have $\mathrm{tr}\rho_\mathfrak{m}(\sigma) \equiv \chi^{k-1}(\sigma) + 1 \mod I$ for $\sigma \in G_\mathbf{Q}$. Apply the same argument as in the proof of the lattice construction, we can find a basis $\{v_1, v_2\}$ of eigenvectors for some $\rho_\mathfrak{m}(\sigma_0)$ such that

$$\rho_\mathfrak{m}(\sigma) = \begin{pmatrix} a_\sigma & b_\sigma \\ c_\sigma & d_\sigma \end{pmatrix} \quad \text{satisfies}$$

(1) $a_\sigma \in \mathbb{T}_\mathfrak{m}$ for all $\sigma \in G_\mathbf{Q}$ and $a_\sigma \equiv \chi^{k-1}(\sigma) \mod I$,
(2) $d_\sigma \in \mathbb{T}_\mathfrak{m}$ for all $\sigma \in G_\mathbf{Q}$ and $d_\sigma \equiv 1 \mod I$,
(3) $b_\sigma c_\tau \in \mathbb{T}_\mathfrak{m}$ for all $\sigma, \tau \in G_\mathbf{Q}$ and $b_\sigma c_\tau \equiv 0 \mod I$.

Let $C = \{c_\sigma \mid \sigma \in \mathbb{T}_\mathfrak{m}[G_\mathbf{Q}]\}$ be the $\mathbb{T}_\mathfrak{m}$-submodule in K generated by all $c_\sigma \in G_\mathbf{Q}$. Since each ρ_λ is an irreducible Galois representation, the projection of C to each K_λ is a nonzero fractional ideal. In particular, C is a finite faithful $\mathbb{T}_\mathfrak{m}$-module.

Put $\mathcal{L}_1 = \mathbb{T}_\mathfrak{m} v_1, \mathcal{L}_2 = C v_2$ and $\mathcal{L} = \mathcal{L}_1 \oplus \mathcal{L}_2$. Again, $\mathcal{L}$ is the stable lattice generated by v_1 over $\mathbb{T}_\mathfrak{m}[G_\mathbf{Q}]$ and the reduction modulo I is an extension

$$0 \to C/IC \cong \overline{\mathcal{L}}_2 \to \overline{\mathcal{L}} \to \overline{\mathcal{L}}_1 \cong \mathbb{T}_\mathfrak{m}/I(\chi^{k-1}) \to 0$$

having no quotient on which $G_\mathbf{Q}$ acts trivially. Since $\mathbb{T}_\mathfrak{m}/I = \mathbf{Z}_p/J$, for any $\phi \in \mathrm{Hom}(C/IC, \mathbf{Q}_p/\mathbf{Z}_p)$ the non-split extension

$$0 \to \overline{\mathcal{L}}_2/\ker(\phi) \to \overline{\mathcal{L}}/\ker(\phi) \to \overline{\mathcal{L}}_1 \to 0$$

gives a nontrivial class in $H^1_f(\mathbf{Q}, \overline{\mathcal{L}}_2/\ker(\phi)(\chi^{1-k})) \hookrightarrow H^1_f(\mathbf{Q}, \mathbf{Q}_p/\mathbf{Z}_p(\chi^{1-k}))$. Thus the map

$$\mathrm{Hom}(C/IC, \mathbf{Q}_p/\mathbf{Z}_p) \hookrightarrow H^1_f(\mathbf{Q}, \mathbf{Q}_p/\mathbf{Z}_p(\chi^{1-k}))$$

is injective and dually we have a surjective homomorphism $H^1_f(\mathbf{Q}, \mathbf{Q}_p/\mathbf{Z}_p(\chi^{1-k}))^\vee \twoheadrightarrow C/IC$ between finitely-generated Z_p-modules.

Definition 2.1. Let M be an R-module of finite presentation

$$R^a \xrightarrow{h} R^b \to M \to 0.$$

We define the (0-th) Fitting ideal $\mathrm{Fitt}_R(M)$ to be the R-ideal generated by the determinants of all (b,b)-minors in h if $a \geq b$, and $\mathrm{Fitt}_R(M) = R$ if $a < b$. The definition is independent of the choice of the presentation.

We also recall the following facts from [MW84, Appendix].

(1) $\mathrm{Fitt}(M) \subset \mathrm{Fitt}(M')$ if $M \twoheadrightarrow M$.
(2) $\mathrm{Fitt}(M) \subset \mathrm{Ann}(M)$, therefore the Fitting ideal of a faithful R-module is trivial.
(3) $\mathrm{Fitt}_{R/I}(M/IM) = \mathrm{Fitt}_R(M) \mod I$.

We can deduce from which that $\mathrm{Fitt}_{\mathbf{Z}_p} H^1_f(\mathbf{Q}, \mathbf{Q}_p/\mathbf{Z}_p(\chi^{1-k})^\vee \subset \mathrm{Fitt}_{\mathbf{Z}_p}(C/IC)$ and

$$\mathrm{Fitt}_{\mathbf{Z}_p}(C/IC) \mod J = \mathrm{Fitt}_{\mathbf{Z}_p/J}(C/IC) = \mathrm{Fitt}_{\mathbb{T}_\mathfrak{m}/I}(C/IC) = \mathrm{Fitt}_{\mathbb{T}_\mathfrak{m}}(C) \mod I.$$

But $\mathrm{Fitt}_{\mathbb{T}_\mathfrak{m}}(C) = 0$ since C is a faithful $\mathbb{T}_\mathfrak{m}$-module, thus

$$\mathrm{Fitt}_{\mathbf{Z}_p}(C/IC) \subset J \subset (p^r) = (\zeta(1-k)).$$

And as $\#C/IC = \#\mathbf{Z}_p/\mathrm{Fitt}_{\mathbf{Z}_p}(C/IC) \geq \#\mathbf{Z}_p/(\zeta(1-k)$, we obtain the following proposition that partially answers the question we posed in the beginning of the section.

Proposition 2.2. Let $k \geq 4$ be an even number and $(p-1) \nmid k$, we have

$$\#H^1_f(\mathbf{Q}, \mathbf{Q}_p/\mathbf{Z}_p(\chi^{1-k})) \geq \#\mathbf{Z}_p/(\zeta(1-k)).$$

At last, we recall the definition of congruence modules and reinterpret the above chain of inclusions. Let $M' = M'_k(1, \mathbf{Z}_p)$ be the space of modular forms with $a_n(f) \in \mathbf{Z}_p$ for all $n \geq 1$ and $\mathbb{T}'$ be the Hecke algebra acting on M'. Note that we do not require the constant term to be p-integral. Since $S \subset M'$, the Hecke algebra $\mathbb{T}$ is a quotient of $\mathbb{T}'$. In fact, we have

$$\mathbb{T}' \otimes \mathbf{Q}_p \cong \mathbf{Q}_p \times (\mathbb{T} \otimes \mathbf{Q}_p)$$

where the $\mathbf{Q}_p$-component is given by the Eisenstein series E_k. Let $e \in \mathbb{T}' \otimes \mathbf{Q}_p$ be the idempotent corresponding to $(\mathbb{T} \otimes \mathbf{Q}_p)$, then $e\mathbb{T}' = \mathbb{T}$.

Definition 2.3. Following [TU22], we define the congruence modules

$$C_0(\mathbb{T}') = e\mathbb{T}'/e\mathbb{T}' \cap \mathbb{T}', \quad C_0(M') = eM'/eM' \cap M'.$$

Since $e\mathbb{T}' \cap \mathbb{T}'$ is the kernel of the homomorphism to the Eisenstein component

$$\mathbb{T}' \to \mathbf{Q}_p, \quad T_\ell \mapsto 1 + \ell^{k-1},$$

its image in $e\mathbb{T}' = \mathbb{T}$ is precisely $I = (T_\ell - 1 - \ell^{k-1})$ and we have recovered $C_0(\mathbb{T}') \cong \mathbb{T}/I$. On the other hand, we have $eM' \cap M' = S$ and $C_0(M')$ measures the congruences between cusp forms and the Eisenstein series E_k.

Lemma 2.4. The congruence module $C_0(M')$ has an element of order p^n if and only if there exists $G \in M'$ such that $F := E_k - p^n G \in S$.

Proof. Since $C_0(M') \cong M'/(\mathbf{Z}_p E_k \oplus S)$, if $G \in M'$ projects to an element of order p^n in $C_0(M')$, then $p^n G = aE_k + F$ for some $a \in \mathbf{Z}_p^\times$ and $F \in S \setminus pS$. The converse is then also clear. □

In particular, recall that we have constructed $F = E_k - \frac{\zeta(1-k)}{2}(240E_4)^a(-504E_6)^b \in S$. By the lemma there exists a submodule isomorphic to $\mathbf{Z}_p/(\zeta(1-k))$ in $C_0(M')$. We now observe that

$$\mathrm{Ann}_{\mathbf{Z}_p} C_0(M') \subset (\zeta(1-k)), \quad \text{since } \mathbf{Z}_p/(\zeta(1-k)) \hookrightarrow C_0(M'),$$
$$J = \mathrm{Ann}_{\mathbf{Z}_p} C_0(\mathbb{T}') \subset \mathrm{Ann}_{\mathbf{Z}_p} C_0(M'), \quad \text{since } C_0(\mathbb{T}') \otimes M' \twoheadrightarrow C_0(M'),$$

and we have already proved $\mathrm{Fitt}_{\mathbf{Z}_p} H^1_f(\mathbf{Q}, \mathbf{Q}_p/\mathbf{Z}_p(\chi^{1-k}))^\vee \subset J$. In conclusion, we have

$$(\zeta(1-k)) \supset \mathrm{Ann}_{\mathbf{Z}_p} C_0(M') \supset \mathrm{Ann}_{\mathbf{Z}_p} C_0(\mathbb{T}') \supset \mathrm{Fitt}_{\mathbf{Z}_p} H^1_f(\mathbf{Q}, \mathbf{Q}_p/\mathbf{Z}_p(\chi^{1-k}))^\vee.$$

This will turn out to be a recurring theme.

References

[BC09] Joël Bellaïche and Gaëtan Chenevier. *Families of Galois representations and Selmer groups*. Number 324 in Astérisque. Société mathématique de France, 2009. 4

[MW84] B. Mazur and A. Wiles. Class fields of abelian extensions of Q. *Inventiones mathematicae*, 76:179–330, 1984. 6

[Rib76] Kenneth A. Ribet. A Modular Construction of Unramified p-Extensions of $\mathbf{Q}(\mu_p)$. *Inventiones mathematicae*, 34:151–162, 1976. 1

[Ski09] Christopher M. Skinner. Galois representations, Iwasawa Theory, and Special Values of L-functions. *CMI Summer School on Galois representations*, 2009. 1

[TU22] Jacques Tilouine and Eric Urban. Integral period relations and congruences. *Algebra & Number Theory*, 2022. 7

[Urb01] Eric Urban. Selmer groups and the Eisenstein-Klingen ideal. *Duke Mathematical Journal*, 106(3):485 – 525, 2001. 3

[Was82] Lawrence C. Washington. *Introduction to cyclotomic fields*. Springer-Verlag, New York, 1982. 1