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, \( \chi: G_{\mathbb{Q}} \to \mathbb{Z}_p \times \mathbb{Z}_p \) be the \( p \)-th cyclotomic character, and
\[
\omega = \overline{\chi}: G_{\mathbb{Q}} \to \text{Gal}(\mathbb{Q}(\mu_p)/\mathbb{Q}) \to \mathbb{F}_p \cong \mu_{p-1}
\]
be the Teichmuller character.

1. The Herbrand-Ribet theorem

Let \( A = Cl(\mathbb{Q}(\mu_p)) \otimes \mathbb{Z}_p \) be the \( p \)-primary part of the field \( \mathbb{Q}(\mu_p) \). The action of \( \text{Gal}(\mathbb{Q}(\mu_p)/\mathbb{Q}) \)
on \( A \) gives a decomposition
\[
A = \bigoplus_{n=0}^{p-2} A_n
\]
where the Galois group acts on \( A_n \) by \( \omega^n \). 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 conjecture 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 \( \text{val}_p(B_{p-1}) = -1 \). This is compatible with the
fact that \( A_1 = 0 \).

We first reinterpret \( A_n \) as Selmer groups. Let \( G = G_{\mathbb{Q}}, H = G_{\mathbb{Q}(\mu_p)}, \Delta = \text{Gal}(\mathbb{Q}(\mu_p)/\mathbb{Q}) = G/H \)
and \( W = \mathbb{F}(\omega^n) \), define
\[
H^1_f(\mathbb{Q}, W) := \ker \left( H^1(\mathbb{Q}, W) \to \prod_{\ell} H^1(I_{\ell}, W) \right).
\]
Since \( p \nmid \# \Delta \), we can stare at the inflation-restriction exact sequence

\[
\begin{array}{ccccccccc}
H^1(\Delta, W) & \longrightarrow & H^1(G, W) & \sim & H^1(H, W)^\Delta & \longrightarrow & H^2(\Delta, W) \\
\downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & H^1(I_\ell, W) & \longrightarrow & \prod_v H^1(I_v, W) & \longrightarrow & 0
\end{array}
\]

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

\[
\begin{align*}
H^1_{f}(Q, W) & \sim H^1_{f}(Q(\mu_p), W) \\
& = \{ \phi \in \text{Hom}_\Delta(H, W) \mid f(I_v) = 0 \text{ for all } v \} = \text{Hom}(A_n, \mathbb{F}).
\end{align*}
\]

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

\[
0 \to \mathbb{F}(\omega^n) \to \mathbb{F} \to 0
\]

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 \( \mathbb{Z}_p \) 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 \( \Delta \) function.

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

1. The Hecke algebra \( \mathbb{T} \) is reduced and finite flat over \( \mathbb{Z}_p \).
(2) There exists a perfect bilinear pairing
\[ \mathbb{T} \times S \to \mathbb{Z}_p, \quad (T, f) \mapsto a_1(Tf) \]
which identifies \( S \cong \text{Hom}(\mathbb{T}, \mathbb{Z}_p) \). A cusp form \( f \) is a Hecke eigenform if and only if it corresponds to a homomorphism of \( \mathbb{Z}_p \)-algebras.

(3) The \( \mathbb{Q}_p \)-algebra \( \mathbb{T} \otimes \mathbb{Q}_p \) is semi-simple and has a decomposition \( \mathbb{T} \otimes \mathbb{Q}_p = \prod \lambda K_{\lambda} \) into finite extensions over \( \mathbb{Q}_p \). 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 \( \mathbb{Z}_p \)-module homomorphism associated to \( F \)
\[ \eta: \mathbb{T} \to \mathbb{F}_p, \quad T_\ell \mapsto a_\ell(F) \equiv 1 + \ell^{k-1} \mod p \]
becomes a ring homomorphism after modulo by \( p \).

**Lemma 1.4** (Deligne-Serre lifting). There exists an eigenform \( f \in S_k(\mathcal{O}) \), where \( \mathcal{O} \) is the ring of integer of a finite extension over \( \mathbb{Q}_p \) with a uniformizer \( \varpi \), such that
\[ a_\ell(f) \equiv 1 + \ell^{k-1} \mod (\varpi). \]

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

The irreducible Galois representation associated to \( f \)
\[ \rho_f: G_{\mathbb{Q}} \to \text{GL}_2(K), \quad K = \text{Frac} \mathcal{O} \]
is unramified away from \( p \) and satisfies \( \text{tr}(\rho_f(Frob_\ell)) = a_\ell(f) \) for all \( \ell \neq p \). It follows from
\[ \text{tr}(\rho_f(Frob_\ell)) = a_\ell(f) \equiv 1 + \ell^{k-1} = 1 + \chi^{k-1}(\text{Frob}_\ell) \mod (\varpi), \]
and the Chebotarev’s density that \( \text{tr}(\rho_f(\sigma)) \equiv 1 + \chi^{k-1}(\sigma) \mod (\varpi) \) for all \( \sigma \in G_{\mathbb{Q}} \). Therefore, the semi-simplified reduction \( \rho^{ss} \) is isomorphic to \( \omega^{k-1} \boxplus 1 \). 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 \( \rho: G_{\mathbb{Q}} \to \text{GL}_2(K) \) be an irreducible Galois representation such that
\[ \text{tr}\rho \equiv \chi_1 + \chi_2 \mod \frak{a} = (\varpi)^n. \]
for characters \( \chi_i: G_{\mathbb{Q}} \to \mathcal{O}^\times \) that are distinct modulo \( (\varpi) \). Then there exists a stable lattice \( \mathcal{L} \subset K^2 \) whose reduction is a non-split extension between \( \chi_1 \) and \( \chi_2 \) modulo \( \frak{a} \).

**Proof.** Observe that \( \det(\rho(\sigma)) = \text{tr}(\rho(\sigma^2)) - \text{tr}(\rho(\sigma))^2/2 \) and therefore
\[ \det(XI - \rho(\sigma)) \equiv (X - \chi_1(\sigma))(X - \chi_2(\sigma)) \mod \frak{a}. \]
Since \( \chi_i \) are distinct modulo \( (\varpi) \), we can pick \( \sigma_0 \in G_{\mathbb{Q}} \) whose characteristic polynomial has distinct roots modulo \( (\varpi) \). 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
\[ \rho(\sigma_0) = \begin{pmatrix} \alpha_1 \\ \alpha_2 \end{pmatrix}, \quad \alpha_i \in \mathcal{O}, \quad \alpha_i \equiv \chi_i(\sigma_0) \mod \frak{a}. \]
Since $\text{tr} \rho(\sigma \sigma_0^n) \equiv \chi_1(\sigma \sigma_0^n) + \chi_2(\sigma \sigma_0^n) \mod a$, the relation
\[ a_\sigma \alpha_1^n + d_\sigma \alpha_2^n \equiv \chi_1(\sigma) \alpha_1^n + \chi_2(\sigma) \alpha_2^n \mod a, \quad \rho(\sigma) = \begin{pmatrix} a_\sigma & b_\sigma \\ c_\sigma & d_\sigma \end{pmatrix} \]
holds for all $n$ and $\sigma \in G_{Q}$. And since $\{ (1,1), (\alpha_1, \alpha_2) \}$ generate $O^2$, we actually have
\[ a_\sigma \equiv \chi_1(\sigma), \quad d_\sigma \equiv \chi_2(\sigma) \mod a \]
for all $\sigma \in G_{Q}$ and thus

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

Let $C = \{ c_\sigma \mid \sigma \in O[G_{Q}] \}$ be the $O$-submodule in $K$ generated by all $c_\sigma \in G_{Q}$. Then $C$ is nonzero because $\rho$ is irreducible and it is actually a fractional ideal since the Galois group is compact. We put $L_1 = \mathcal{O}v_1, L_2 = C \cdot v_2$ and $L = L_1 \oplus L_2$, which is the stable lattice generated by $v_1$ over $O[G_{Q}]$. By above, the reduction of $L$ modulo $a$ is an extension
\[ 0 \to \mathcal{O}/a(\chi_2) \cong \mathcal{L}_2 \to \mathcal{L} \to \mathcal{L}_1 \cong \mathcal{O}/a(\chi_1) \to 0 \]
as $C/aC \cong O/a$. We claim that $\mathcal{L}$ has no quotient on which $G_{Q}$ acts by $\chi_2$. Otherwise
\[ (\rho(\sigma_0) - \chi_2(\sigma_0))v_1 \equiv (\alpha_1 - \alpha_2)v_1 \mod a, \]
and therefore $v_1$ lies in the kernel, which contradicts that $v_1$ generates $L$. In particular, the extension gives a nontrivial class in $\text{Ext}^1_{G_{Q}}(\mathcal{X}_1, \mathcal{X}_2) = H^1(Q, O/\mathcal{O}(\chi_2^{-1}))$. \hfill $\square$

Remark 1.6. The proposition was proved for the more general setting when $O$ is local Henselian and $\overline{p}^{ss}$ 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 $a = (\pi)$ and $(\chi_1, \chi_2) = (1, \chi^{k-1})$, we can obtain a nontrivial class in $H^1(Q, \mathbb{F}(\omega^{k-1}))$ or $H^1(Q, \mathbb{F}(\omega^{1-k}))$. In either case, the restriction to $I_f$ for $\ell \neq p$ is trivial since $\rho_f$ is unramified away from $p$ and the image of $L_1$ in $\mathcal{L}$ 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,
\[ \rho_f|_{I_p} \sim \begin{pmatrix} \chi^{k-1} & \ast \\ 1 \end{pmatrix}. \]

Now, if the reduction of the lattice $L$ is a non-split extension $0 \to F \to \mathcal{L} \to \mathbb{F}(\omega^{k-1}) \to 0$ and $F \subset K^2$ is the subspace where $I_p$ acts by $\chi^{k-1}$, the reduction of $L \cap F$ is a section of the extension when restricted to $I_p$. Therefore we have show that
\[ 0 \neq [\mathcal{L}] \in H^1(Q, \mathbb{F}(\omega^{1-k})) \cong \text{Hom}(A_{p-k}, \mathbb{F}). \]
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 $a = (\varpi^n)$, the same arguments will give a nontrivial class in

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

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 $m = \ker(\eta)$. We therefore need to consider all these primes, or equivalently all the Hecke eigenforms congruent to $E_k$, at the same time.

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

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

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

$$\begin{array}{ccc}
\mathbb{T}/I & \xrightarrow{\eta} & \mathbb{T}/m \\
\downarrow & & \downarrow \\
\mathbb{Z}_p/J & \xrightarrow{\iota} & \mathbb{F}_p
\end{array}$$

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

$$\rho_m = \prod \rho_\lambda: G_\mathbb{Q} \to \text{GL}_2(K) = \prod \text{GL}_2(K_\lambda),$$

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

$$\text{tr}\rho_m(\text{Frob}_\ell) = T_\ell \equiv \ell^{k-1} + 1 = \chi^{k-1}(\text{Frob}_\ell) + 1 \mod I,$$

we have $\text{tr}\rho_m(\sigma) \equiv \chi^{k-1}(\sigma) + 1 \mod I$ for $\sigma \in G_\mathbb{Q}$. 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 $\rho_m(\sigma_0)$ such that

$$\rho_m(\sigma) = \begin{pmatrix} a_\sigma & b_\sigma \\ c_\sigma & d_\sigma \end{pmatrix}$$

satisfies

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

Let $C = \{c_\sigma \mid \sigma \in \mathbb{T}_m[G_\mathbb{Q}]\}$ be the $\mathbb{T}_m$-submodule in $K$ generated by all $c_\sigma \in G_\mathbb{Q}$. Since each $\rho_\lambda$ is an irreducible Galois representation, the projection of $C$ to each $K_\lambda$ is a nonzero fractional ideal. In particular, $C$ is a finite faithful $\mathbb{T}_m$-module.
Put \( \mathcal{L}_1 = T_m v_1, \mathcal{L}_2 = C v_2 \) and \( \mathcal{L} = \mathcal{L}_1 \oplus \mathcal{L}_2. \) Again, \( \mathcal{L} \) is the stable lattice generated by \( v_1 \) over \( T_m[G_Q] \) and the reduction modulo \( I \) is an extension

\[
0 \to C/IC \cong \mathcal{L}_2 \to \mathcal{L} \to \mathcal{L}_1 \cong T_m/I(\chi^{k-1}) \to 0
\]

having no quotient on which \( G_Q \) acts trivially. Since \( T_m/I = \mathbb{Z}_p/J, \) for any \( \phi \in \text{Hom}(C/IC, \mathbb{Q}_p/\mathbb{Z}_p) \) the non-split extension

\[
0 \to \mathcal{L}_2/\ker(\phi) \to \mathcal{L}/\ker(\phi) \to \mathcal{L}_1 \to 0
\]
gives a nontrivial class in \( H^1_j(Q, \mathcal{L}_2/\ker(\phi)(\chi^{1-k})) \to H^1_j(Q, \mathbb{Q}_p/\mathbb{Z}_p(\chi^{1-k})). \) Thus the map

\[
\text{Hom}(C/IC, \mathbb{Q}_p/\mathbb{Z}_p) \to H^1_j(Q, \mathbb{Q}_p/\mathbb{Z}_p(\chi^{1-k}))
\]

is injective and dually we have a surjective homomorphism \( H^1_j(Q, \mathbb{Q}_p/\mathbb{Z}_p(\chi^{1-k}))^\vee \to C/IC \) between finitely-generated \( \mathbb{Z}_p \)-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 \( \text{Fitt}_R(M) \) to be the \( R \)-ideal generated by the determinants of all \( (b, b) \)-minors in \( h \) if \( a \geq b \), and \( \text{Fitt}_R(M) = R \) if \( a < b \). The definition is independent of the choice of the presentation.

We also recall the following facts from \([\text{MW84}, \text{Appendix}]\).

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

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

\[
\text{Fitt}_{\mathbb{Z}_p}(C/IC) \mod J = \text{Fitt}_{\mathbb{Z}_p/J}(C/IC) = \text{Fitt}_{\mathbb{T}_m}(C/IC) \mod I.
\]

But \( \text{Fitt}_{\mathbb{T}_m}(C) = 0 \) since \( C \) is a faithful \( \mathbb{T}_m \)-module, thus

\[
\text{Fitt}_{\mathbb{Z}_p}(C/IC) \subset J \subset (p') = (\zeta(1-k)).
\]

And as \( \#C/IC = \#\mathbb{Z}_p/\text{Fitt}_{\mathbb{Z}_p}(C/IC) \geq \#\mathbb{Z}_p/(\zeta(1-k)) \), 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

\[
\#H^1_j(Q, \mathbb{Q}_p/\mathbb{Z}_p(\chi^{1-k})) \geq \#\mathbb{Z}_p/(\zeta(1-k)).
\]

At last, we recall the definition of congruence modules and reinterpret the above chain of inclusions. Let \( M' = M'_n(1, \mathbb{Z}_p) \) be the space of modular forms with \( a_n(f) \in \mathbb{Z}_p \) 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

\[
\mathbb{T}' \otimes \mathbb{Q}_p \cong \mathbb{Q}_p \times (\mathbb{T} \otimes \mathbb{Q}_p)
\]

where the \( \mathbb{Q}_p \)-component is given by the Eisenstein series \( E_k \). Let \( e \in \mathbb{T}' \otimes \mathbb{Q}_p \) be the idempotent corresponding to \( (\mathbb{T} \otimes \mathbb{Q}_p) \), 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
\[ \mathbb{T}' \to \mathbb{Q}_p, \quad T_t \mapsto 1 + \ell^{-k-1}, \]
its image in \( e\mathbb{T}' \) is precisely \( I = (T_t - 1 - \ell^{-k-1}) \) 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 \( C_0(M') \cong M' / (\mathbb{Z}_p E_k \oplus S) \), 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 \( a \in \mathbb{Z}_p^\times \) and \( F \in S \setminus pS \). The converse is then also clear. \( \square \)

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 \( \mathbb{Z}_p / (\zeta(1-k)) \) in \( C_0(M') \). We now observe that
\[ \text{Ann}_{\mathbb{Z}_p} C_0(M') \subset (\zeta(1-k)), \quad \text{since } \mathbb{Z}_p / (\zeta(1-k)) \hookrightarrow C_0(M'), \]
\[ J = \text{Ann}_{\mathbb{Z}_p} C_0(\mathbb{T}') \subset \text{Ann}_{\mathbb{Z}_p} C_0(M'), \quad \text{since } C_0(\mathbb{T}') \otimes M' \twoheadrightarrow C_0(M'), \]
and we have already proved \( \text{Fitt}_{\mathbb{Z}_p} H_j^1(\mathbb{Q}, \mathbb{Q}_p / \mathbb{Z}_p(\chi^{1-k}))^\vee \subset J \). In conclusion, we have
\[ (\zeta(1-k)) \supset \text{Ann}_{\mathbb{Z}_p} C_0(M') \supset \text{Ann}_{\mathbb{Z}_p} C_0(\mathbb{T}') \supset \text{Fitt}_{\mathbb{Z}_p} H_j^1(\mathbb{Q}, \mathbb{Q}_p / \mathbb{Z}_p(\chi^{1-k}))^\vee. \]
This will turn out to be a recurring theme.

References


