MODULARITY OF RESIDUAL GALOIS EXTENSIONS AND THE EISENSTEIN IDEAL

TOBIAS BERGER AND KRZYSZTOF KLOSIN

ABSTRACT. For a totally real field F, a finite extension $\mathbf{F}$ of $\mathbf{F}_p$ and a Galois character $\chi : G_F \to \mathbf{F}^\times$ unramified away from a finite set of places $\Sigma \supset \{\mathfrak{p} \mid p\}$ consider the Bloch-Kato Selmer group $H := H^1_\Sigma(F, \chi^{-1})$. In [BK15] it was proved that the number d of isomorphism classes of (non-semisimple, reducible) residual representations $\overline{\rho}$ giving rise to lines in H which are modular by some ρ_f (also unramified outside Σ) satisfies $d \geq n := \dim_{\mathbf{F}} H$. This was proved under the assumption that the order of a congruence module is greater than or equal to that of a divisible Selmer group. We show here that if in addition the relevant local Eisenstein ideal J is non-principal, then $d > n$. When $F = \mathbf{Q}$ we prove the desired bounds on the congruence module and the Selmer group. We also formulate a congruence condition implying the non-principality of J that can be checked in practice, allowing us to furnish an example where $d > n$.

1. INTRODUCTION

Let p be an odd prime and let Σ be a finite set of primes of $\mathbf{Q}$ containing p where each prime $\ell \in \Sigma$, $\ell \neq p$ satisfies $\ell \not\equiv 1 \pmod{p}$. Write G_Σ for the absolute Galois group of the maximal Galois extension of $\mathbf{Q}$ unramified outside of Σ. Let E be a finite extension of $\mathbf{Q}_p$ with integer ring $\mathcal{O}$, uniformizer ϖ and $\mathcal{O}/\varpi\mathcal{O} = \mathbf{F}$. Let $\chi : G_\Sigma \to \mathbf{F}^\times$ be a character. Consider a non-split extension of G_Σ-modules

$$0 \to \mathbf{F} \to \overline{\rho} \to \mathbf{F}(\chi) \to 0.$$

In this paper we are interested in the modularity of $\overline{\rho}$ in the following sense: Fix a positive integer N divisible only by the primes in $\Sigma - \{p\}$. We will say that $\overline{\rho}$ is modular (of level N) if there exists a newform f (of level N) giving rise to a (irreducible) Galois representation $\rho_f : G_\Sigma \to \mathrm{GL}_2(E)$ and a G_Σ-stable $\mathcal{O}$-lattice in the space of ρ_f such that with respect to this lattice the mod ϖ reduction $\overline{\rho}_f$ of ρ_f is isomorphic to $\overline{\rho}$ (as representations).

This is a very strong notion of modularity for two reasons:

(1) we require that $\overline{\rho}_f \cong \overline{\rho}$ rather than simply $\operatorname{tr} \overline{\rho}_f = \operatorname{tr} \overline{\rho}$ and
(2) we do not allow ρ_f to be ramified at primes outside of Σ.

The requirement (2) stands in contrast with the work of Hamblen and Ramakrishna [HR08] who prove modularity of such $\overline{\rho}$ by ρ_f in the sense of (1), but allow for additional ramification of ρ_f. More specifically, they show the existence of a

The first author's research was supported by the EPSRC Grant EP/R006563/1. The second author was supported by the Young Investigator Grant #H98230-16-1-0129 from the National Security Agency, a Collaboration for Mathematicians Grant #578231 from the Simons Foundation and by a PSC-CUNY award jointly funded by the Professional Staff Congress and the City University of New York.

characteristic zero lift $\rho : G_{\Sigma'} \to \mathrm{GL}_2(\mathcal{O})$ of $\overline{\rho}$ for some set $\Sigma' \supset \Sigma$ and then use the modularity theorem of Skinner and Wiles [SW99] to conclude modularity of $\overline{\rho}$.

To the best of our knowledge the question of modularity of $\overline{\rho}$ in our strong sense has never been studied despite being rather natural. (In the semi-simple reducible case such an analysis was carried out by Billerey and Menares in [BM18] using a different method.) While we are not able to prove that all $\overline{\rho}$ as above are modular in this sense, this is perhaps not to be expected. In particular not all such extensions will in general be modular if we fix the level N as there are only finitely many forms of fixed level (we also fix the weight by imposing a condition on the determinant). So, in particular enlarging $\mathbf{F}$ (which increases the number of isomorphism classes of $\overline{\rho}$) will produce non-modular extensions. This prompts an intriguing question: given N how many of the extensions $\overline{\rho}$ are modular of level N? In this article we give a lower bound on this number when $\overline{\rho}$ is in the image of the Fontaine-Laffaille functor as we now explain. While we limit most of our discussion here for simplicity to the case of $\mathbf{Q}$, we prove some of our results for a general totally real field F (see below).

Any isomorphism class $\overline{\rho}$ in the category of representations gives rise to a line in the residual Bloch-Kato Selmer group $H^1_\Sigma(\mathbf{Q}, \chi^{-1})$ (where we do not impose any conditions on primes in Σ other than p). We showed in [BK15] that under some assumptions the group $H^1_\Sigma(\mathbf{Q}, \chi^{-1})$ has a basis consisting of modular extensions, i.e., that at least $n := \dim H^1_\Sigma(\mathbf{Q}, \chi^{-1})$ such isomorphism classes of $\overline{\rho}$ are modular.

Improving this bound (which is the main goal of this paper) is a tougher problem and we show it is related to the structure of the Eisenstein ideal J of the (local) cuspidal Hecke algebra $\mathbf{T}$. We obtain the most satisfactory answer for $F = \mathbf{Q}$. In this case we show that if J is not principal and the Selmer group $H^1_\Sigma(\mathbf{Q}, \chi)$ ("for extensions in the opposite order" of characters to the one in $\overline{\rho}$) is one-dimensional, then the number of modular isomorphism classes of the representations $\overline{\rho}$ is strictly larger than n (under some restrictions on Σ and χ) - cf. Corollary 5.8.

One of the immediate consequences of our results is that if J is not principal then $\dim H^1_\Sigma(\mathbf{Q}, \chi^{-1}) > 1$ (since in a one-dimensional Selmer group there is only one line!). We note that Wake and Wang-Erickson [WWE18] give a cohomological lower bound on the number of generators of the Eisenstein ideal for modular forms of weight 2 and trivial nebentypus. A side effect of our result (but one that applies to the case of $k > 2$ or $k = 2$ and non-trivial nebentypus, so not the case studied in [WWE18]) is that it provides a condition in the converse direction, i.e., J not principal implies $\dim H^1_\Sigma > 1$.

In the process of proving Corollary 5.8 (i.e., when $F = \mathbf{Q}$) we establish a lower bound on the congruence module $\mathbf{T}/J$ by a certain Bernoulli number with correction factors. Previous results of this kind include Theorem 5.1 in [SW97], which applies in the case of $k = 2$ and non-trivial nebentypus and an analogous result of Mazur [Maz77], Proposition II.9.7 (for $k = 2$, prime level and trivial nebentypus). We also establish a corresponding upper bound on the relevant Bloch-Kato Selmer group which together with the $\mathbf{T}/J$-bound are key for the existence of a modular basis of $H^1_\Sigma(\mathbf{Q}, \chi^{-1})$. We also prove bounds on other Selmer groups that allow one to check when $\dim_{\mathbf{F}} H^1_\Sigma(\mathbf{Q}, \chi) = 1$ and $\dim_{\mathbf{F}}(\mathbf{Q}, \chi^{-1}) > 1$ (the case when our theorem is interesting).

For a general F we obtain a similar result. However the existence of corresponding bounds on $\mathbf{T}/J$ and the Selmer group, while expected to hold, is not yet known.

Let us discuss the organization of the paper. In section 2 we establish basic notation and facts regarding Selmer groups and Fontaine-Laffaille representations. In section 3 we study the relevant Hecke algebra $\mathbf{T}$ along with its quotients $\mathbf{T}_\tau$ corresponding to newforms whose Galois representations reduce to different isomorphism classes of (reducible) residual representations τ. We also define the Eisenstein ideal J and prove a preliminary result guaranteeing the existence of more than n modular Galois extensions (Proposition 3.9). In section 4 we introduce and study the ideals of reducibility of the Galois representations $\rho_\tau : G_\Sigma \to \mathrm{GL}_2(\mathbf{T}_\tau)$ (whose existence we prove) showing their principality under the assumption that $\dim_{\mathbf{F}} H^1_\Sigma(\mathbf{Q}, \chi) = 1$. This allows us to strengthen Proposition 3.9 to Theorem 4.8. In section 5 we strengthen Theorem 4.8 further in the case $F = \mathbf{Q}$ by proving an equality between the orders of $\mathbf{T}/J$ and the relevant divisible Selmer group. In section 6 we establish bounds on certain Selmer groups allowing us (among other things) to verify the condition $\dim_{\mathbf{F}} H^1_\Sigma(\mathbf{Q}, \chi) = 1$ for an example which we discuss in section 7.

We would like to thank David Spencer for informing us about [BM18] and [Spe18]. We are also grateful to Neil Dummigan and Carl Wang-Erickson for helpful comments.

2. Setup

Let F be a totally real field and $p > 2$ a prime with $p \nmid \#\,\mathrm{Cl}_F$ and p unramified in $F/\mathbf{Q}$. Let Σ be a finite set of finite places of F containing all the places lying over p. Assume that if $\mathfrak{q} \in \Sigma$, then $N\mathfrak{q} \not\equiv 1 \pmod{p}$. Let G_Σ denote the Galois group $\mathrm{Gal}(F_\Sigma/F)$, where F_Σ is the maximal extension of F unramified outside Σ. For every prime $\mathfrak{q}$ of F we fix compatible embeddings $\overline{F} \hookrightarrow \overline{F}_\mathfrak{q} \hookrightarrow \mathbf{C}$ and write $D_\mathfrak{q}$ and $I_\mathfrak{q}$ for the corresponding decomposition and inertia subgroups of G_F (and also their images in G_Σ by a slight abuse of notation). Let E be a (sufficiently large) finite extension of $\mathbf{Q}_p$ with ring of integers $\mathcal{O}$ and residue field $\mathbf{F}$. We fix a choice of a uniformizer ϖ. We will write ϵ for the p-adic cyclotomic character, $\bar{\epsilon}$ for its mod p reduction, and ω for the Teichmüller lift of ϵ. For a local ring A we write $\mathfrak{m}_A$ for its maximal ideal.

2.1. Fontaine-Laffaille representations.

Let n be any positive integer. Suppose

$$r : G_\Sigma \to \mathrm{GL}_n(\mathbf{F})$$

is a continuous homomorphism.

We recall from [CHT08] p. 35 the definition of a *Fontaine-Laffaille* representation: Let $\mathfrak{p} \mid p$ and A be a local complete Noetherian $\mathbf{Z}_p$-algebra with residue field $\mathbf{F}$. A representation $\rho : D_\mathfrak{p} \to \mathrm{GL}_n(A)$ is Fontaine-Laffaille if for each Artinian quotient A' of A, $\rho \otimes A'$ lies in the essential image of the Fontaine-Laffaille functor $\mathbf{G}$ (for its definition see e.g. [BK13] Section 5.2.1). We also call a continuous finite-dimensional G_Σ-representation V over $\mathbf{Q}_p$ Fontaine-Laffaille if, for all primes $\mathfrak{p} \mid p$, it is crystalline and $\mathrm{Fil}^0 D = D$ and $\mathrm{Fil}^{p-1} D = (0)$ for the filtered vector space $D = (B_{\mathrm{crys}} \otimes_{\mathbf{Q}_p} V)^{D_\mathfrak{p}}$ defined by Fontaine (for details see again [BK13] Section 5.2.1).

For $j \in \{1,2\}$ let $\tau_j : G_\Sigma \to \mathrm{GL}_{n_j}(\mathbf{F})$ be an absolutely irreducible continuous representation. Assume that $\tau_1 \not\cong \tau_2$. Consider the set of isomorphism classes of n-dimensional residual Fontaine-Laffaille representations of the form:

$$\tau = \begin{bmatrix} \tau_1 & * \\ & \tau_2 \end{bmatrix} : G_\Sigma \to \mathrm{GL}_n(\mathbf{F}), \tag{2.1}$$

which are non-semi-simple ($n = n_1 + n_2$).

2.2. **Selmer groups.** For a p-adic G_Σ-module M (finitely generated or cofinitely generated over $\mathcal{O}$ - for precise definitions cf. [BK13], section 5) we define the Selmer group $H^1_\Sigma(F, M)$ to be the subgroup of $H^1_{\mathrm{cont}}(F_\Sigma, M)$ consisting of cohomology classes which are crystalline in the sense of Bloch-Kato at all primes $\mathfrak{p}$ of F dividing p, i.e.

$$H^1_\Sigma(F, M) = \ker(H^1(G_\Sigma, M) \to \prod_{\mathfrak{p}|p} (H^1(F_\mathfrak{p}, M)/H^1_f(F_\mathfrak{p}, M)).$$

For G_Σ-modules M occurring as $\mathcal{O}$-lattices T in E-vector spaces V or as divisible modules V/T the crystalline conditions $H^1_f(F_\mathfrak{p}, M)$ are as defined by Bloch-Kato in [BK90] (cf. also section 1 in [Rub00]). For G_K-modules M of finite cardinality we use Fontaine-Laffaille theory to define the local condition: If K denotes an unramified extension of $\mathbf{Q}_p$ then if M is in the essential image of the Fontaine-Laffaille functor $\mathbf{G}$ we define $H^1_f(K, M)$ as the image of $\mathrm{Ext}^1_{\mathcal{MF}_\mathcal{O}}(1_{\mathrm{FD}}, D)$ in $H^1(K, M) \cong \mathrm{Ext}^1_{\mathcal{O}[G_K]}(1, M)$, where $\mathcal{MF}_\mathcal{O}$ is the category of filtered Dieudonné modules, $\mathbf{G}(D) = M$ and 1_{FD} is the unit filtered Dieudonné module defined in Lemma 4.4 of [BK90]. Note that we place no restrictions at the primes in Σ that do not lie over p. For more details cf. [loc.cit.].

3. The rings $\mathbf{T}_\tau$

Proposition 3.1. *Suppose $\rho : G_\Sigma \to \mathrm{GL}_n(E)$ is irreducible and satisfies*

$$\overline{\rho}^{\mathrm{ss}} \cong \tau_1 \oplus \tau_2, \tag{3.1}$$

where $\overline{\rho}^{\mathrm{ss}}$ denotes the semi-simplification of any residual representation of ρ. Then there exists a lattice inside E^n so that with respect to that lattice the mod ϖ reduction $\overline{\rho}$ of ρ has the form

$$\overline{\rho} = \begin{bmatrix} \tau_1 & * \\ 0 & \tau_2 \end{bmatrix}$$

and is non-semi-simple.

Proof. This argument goes back to Ribet and in this form is a special case of [Urb01], Theorem 1.1, where the ring $\mathcal{B}$ in [loc.cit.] is the discrete valuation ring $\mathcal{O}$. □

For τ as in (2.1) let $\Phi_{\tau,E}$ be the set of isomorphism classes of Fontaine-Laffaille at $\mathfrak{p} \mid p$ Galois representations $\rho : G_\Sigma \to \mathrm{GL}_n(E)$ such that there exists a G_Σ-stable lattice L in the space of ρ so that the mod ϖ-reduction of ρ_L equals τ. The following is a higher-dimensional analogue of Lemma 2.13(ii) from [SW99]:

Proposition 3.2 ([BK15], Proposition 3.2)**.** *One has $\Phi_{\tau,E} \cap \Phi_{\tau',E} = \emptyset$ if $\tau \not\cong \tau'$.*

For the rest of this section set $n = 2$, $\tau_1 = 1$ and $\tau_2 = \chi = \psi\bar{\epsilon}^{k-1}$, where ψ is unramified at p and k is an integer such that $2 \leq k \leq p-1$. Write $\tilde{\psi}$ for the Teichmüller lift of ψ and set $\tilde{\chi} = \tilde{\psi}\epsilon^{k-1}$.

Let $\mathfrak{N}$ be an ideal of $\mathcal{O}_F$ divisible only by primes in Σ which do not lie over p. We consider the space $\mathcal{S}_k(\mathfrak{N}, \tilde{\psi})$ of cuspidal Hilbert modular forms (over the field F) of parallel weight $k \geq 2$, level $\Gamma_0(\mathfrak{N})$ and character $\tilde{\psi}$. Let $\mathbf{T}'$ be the $\mathcal{O}$-subalgebra of $\mathrm{End}_{\mathbf{C}}\, \mathcal{S}_k(\mathfrak{N}, \tilde{\psi})$ generated by the Hecke operators $T_{\mathfrak{q}}$ for all $\mathfrak{q} \notin \Sigma$. Set J' to be the ideal of $\mathbf{T}'$ generated by the set $\{T_{\mathfrak{q}} - (1 + \tilde{\psi}(\mathfrak{q})(N\mathfrak{q})^{k-1}) \mid \mathfrak{q} \notin \Sigma\}$. Let $\mathfrak{m}$ be a maximal ideal of $\mathbf{T}'$ containing J' and set $\mathbf{T}$ to be the completion of $\mathbf{T}'$ at the ideal $\mathfrak{m}$.

Definition 3.3. We will call $J := J'\mathbf{T}$ the (local) *Eisenstein ideal* (associated to $\tilde{\psi}$).

We refer to the surjective $\mathcal{O}$-algebra homomorphisms $\lambda : \mathbf{T} \twoheadrightarrow \mathcal{O}$ as *Hecke eigensystems*. For each such λ we denote by $\tilde{\tau}_\lambda : G_\Sigma \to \mathrm{GL}_2(E)$ the corresponding (irreducible) Galois representation. Using Proposition 3.1 we see that there exists a lattice in E^2 with respect to which $\tilde{\tau}_\lambda$ is valued in $\mathrm{GL}_2(\mathcal{O})$ such that its mod ϖ reduction $\bar{\tilde{\tau}}_\lambda$ is non-semisimple. Proposition 3.2 guarantees that the isomorphism class of $\bar{\tilde{\tau}}_\lambda$ is independent of the choice of such a lattice. In view of this we will simply write τ_λ for the *non-semi-simple residual* Galois representation attached to λ (well-defined up to isomorphism). We write $\mathbf{T}_\tau$ for the image of the canonical map

$$\mathbf{T} \to \prod_{\lambda : \tau_\lambda \cong \tau} \mathcal{O},$$

i.e., the quotient of $\mathbf{T}$ corresponding to all Hecke eigensystems whose associated residual non-semisimple Galois representations are isomorphic to τ. If no τ_λ is isomorphic to τ we set $\mathbf{T}_\tau = 0$. We will denote by J_τ the image of J in $\mathbf{T}_\tau$.

Remark 3.4. It is clear that $\mathbf{T}$ and $\mathbf{T}_\tau$ are finitely generated $\mathcal{O}$-modules. Furthermore, $\#\mathbf{T}/J < \infty$ as otherwise, as we show below, there would exist a surjective $\mathcal{O}$-algebra map $\mathbf{T} \to \mathcal{O}$ factoring through $\mathbf{T}/J$. The existence of such a map would violate the Ramanujan bounds. For the sake of contradiction suppose $\#\mathbf{T}/J = \infty$. Then $\mathbf{T}/J = \mathcal{O}^s \times T$ as an $\mathcal{O}$-module with T finite and $s > 0$. Hence $\mathbf{T}/J$ is not of finite length as an $\mathcal{O}$-module, and it is easy to see that it is also not of finite length as a module over itself. Since $\mathbf{T}$ is Noetherian, it follows that there is a prime ideal $\mathfrak{p}$ of $\mathbf{T}/J$ which is not maximal (cf. Theorem 2.14 in [Eis95]), hence $\mathbf{T}/(J + \mathfrak{p})$ is an infinite domain (as all finite domains are fields). This implies that the structure map $\mathcal{O} \to \mathbf{T}/(J + \mathfrak{p})$ is injective (as $\mathbf{T}$ is a finitely generated $\mathcal{O}$-module), and so the domain $\mathbf{T}/(J + \mathfrak{p})$ is finite over $\mathcal{O}$, thus we may assume it equals $\mathcal{O}$ as $\mathcal{O}$ is assumed to be sufficiently large. Hence the canonical map $\mathbf{T}/J \twoheadrightarrow \mathbf{T}/(J + \mathfrak{p}) = \mathcal{O}$ gives us the $\mathcal{O}$-algebra surjection.

Note that isomorphism classes of Fontaine-Laffaille residual representations $\tau : G_\Sigma \to \mathrm{GL}_2(\mathbf{F})$ such that $\tau = \begin{bmatrix} 1 & * \\ & \chi \end{bmatrix}$ are in one-to-one correspondence with lines in $H^1_\Sigma(F, \chi^{-1})$. Since $2 \leq k < p$ the representations $\tilde{\tau}_\lambda$ (and τ_λ) are Fontaine-Laffaille at primes lying over p.

Definition 3.5. We will say that (an isomorphism class of) $\tau = \begin{bmatrix} 1 & * \\ & \chi \end{bmatrix} : G_\Sigma \to \mathrm{GL}_2(\mathbf{F})$ is *modular* if there exists $\lambda : \mathbf{T} \to \mathcal{O}$ such that $\tau_\lambda \cong \tau$ (in other words, if $\mathbf{T}_\tau \neq 0$).

Remark 3.6. Note that the requirement in Definition 3.5 is stronger than the usual definition of modularity which simply asks that $\operatorname{tr} \tau = \operatorname{tr} \tilde{\tau}_\lambda$ for $\tilde{\tau}_\lambda : G_\Sigma \to \mathrm{GL}_2(E)$.

Theorem 3.7 (Corollary 4.8 in [BK15])**.** *Suppose that $\#H^1_\Sigma(F, \tilde{\chi}^{-1} \otimes E/\mathcal{O}) \leq \#\mathbf{T}/J$. Then there exists a basis $\mathcal{B}$ of $H^1_\Sigma(F, \chi^{-1})$ such that each $\tau \in \mathcal{B}$ is modular.*

Proof. Let us only explain why Assumption 2.4 in [BK15] used in Corollary 4.8 therein is satisfied. For this it is enough to show that there are no non-trivial infinitesimal deformations of 1, respectively χ. This can be proved exactly as [BK13] Proposition 9.5 since $p \nmid \#\operatorname{Cl}_F$. □

Remark 3.8. The assumption that $\#H^1_\Sigma(F, \tilde{\chi}^{-1} \otimes E/\mathcal{O}) \leq \#\mathbf{T}/J$ is used in the proof of Corollary 4.8 in [BK15]. The left-hand side of the inequality encodes certain crystalline G_Σ-extensions of torsion $\mathcal{O}$-modules while the right-hand side encodes corresponding modular extensions (arising from Eisenstein congruences). Hence it can be viewed as in some sense ensuring an abundance of reducible modular deformations of appropriate type. Roughly speaking, the Selmer group on the left hand side should be bounded by a certain L-value by virtue of the relevant case of the Bloch-Kato Conjecture. Then the inequality in the assumption reflects the belief that Eisenstein congruences should be controlled by the same L-value. In section 5 we will prove that these inequalities are often satisfied when $F = \mathbf{Q}$.

Let $\mathfrak{T}$ denote the set of isomorphism classes of residual Galois representations of the form (2.1). Let $\mathfrak{T}_{\mathrm{mod}}$ be the subset of $\mathfrak{T}$ consisting of isomorphism classes which are modular. Note that by Proposition 3.1 each element of $\mathfrak{T}_{\mathrm{mod}}$ can be identified with a line in $H^1_\Sigma(\mathbf{Q}, \chi^{-1})$ and Theorem 3.7 gives a sufficient condition for the existence of at least $\dim_{\mathbf{F}} H^1_\Sigma(F, \chi^{-1})$-many such lines. These lines span the Selmer group, but a natural question to ask is if one could strengthen the conditions of Theorem 3.7 to guarantee the existence of even more modular lines. This is achieved by the following proposition which is the first main result of this paper.

Proposition 3.9. *Suppose that $\#H^1_\Sigma(F, \tilde{\chi}^{-1} \otimes E/\mathcal{O}) \leq \#\mathbf{T}/J$. If J_τ is principal for every $\tau \in \mathfrak{T}_{\mathrm{mod}}$ but J is not principal, then the set $\mathfrak{T}_{\mathrm{mod}}$ of modular isomorphism classes has cardinality strictly greater than $\dim_{\mathbf{F}} H^1_\Sigma(F, \chi^{-1})$.*

Proof. Let us first note that by Remark 3.4 we have that $\mathbf{T}$ is finitely generated as an $\mathcal{O}$-module and $\#\mathbf{T}/J < \infty$, hence the results of [BK15] and [BKK14] apply. By Proposition 5.1 in [BK15] we have that

$$\#\mathbf{T}/J \geq \# \prod_{\tau \in \mathfrak{T}_{\mathrm{mod}}} \mathbf{T}_\tau/J_\tau.$$

By Theorem 3.7 we know that there exists a modular basis $\mathcal{B}$ of $H^1_\Sigma(F, \chi^{-1})$, so in particular $\#\mathfrak{T}_{\mathrm{mod}} \geq \dim_{\mathbf{F}} H^1_\Sigma(F, \chi^{-1})$. Suppose that in fact equality holds. Since any modular extension gives rise to an element of $\mathfrak{T}_{\mathrm{mod}}$, we see that any other modular basis of $H^1_\Sigma(F, \chi^{-1})$ must be obtained from $\mathcal{B}$ by scaling its elements, i.e., $\mathcal{B}$ is 'projectively unique' in the terminology of [BK15]. Then by Proposition 5.4 in [BK15] we get that $\#\mathbf{T}/J = \#\prod_{\tau \in \mathfrak{T}_{\mathrm{mod}}} \mathbf{T}_\tau/J_\tau$. This however implies that J is

principal by Corollary 2.7 of [BKK14] - note that principality of J_τ is necessary for the application of the corollary (cf. p. 73 of [BKK14]). □

For future use we note that the opposite inequality $\#H^1_\Sigma(F, \tilde{\chi}^{-1} \otimes E/\mathcal{O}) \geq \#\mathbf{T}/J$ always holds:

Proposition 3.10. *One has*

$$\#H^1_\Sigma(F, \tilde{\chi}^{-1} \otimes E/\mathcal{O}) \geq \#\mathbf{T}/J.$$

Proof. This is proved by applying Urban's lattice construction, as explained in the proof of [BK15] Lemma 4.4 (we do not need the assumptions 2.5 and 4.2 there as we just want an inequality of orders). □

In the next section we show that if one assumes one-dimensionality of the "opposite" Selmer group $H^1_\Sigma(F, \chi)$ then principality of each J_τ follows.

4. Ideal of reducibility and its principality

Let G be a group and A be a complete Noetherian local $\mathcal{O}$-algebra (with residue field $\mathbf{F}$) which is reduced. Set $R = A[G]$. Let $\tau_1, \tau_2 : G \to \mathrm{GL}_{n_i}(\mathbf{F})$ be two absolutely irreducible representations with $\tau_1 \ncong \tau_2$. Set $n := n_1 + n_2$ and assume that $n!$ is invertible in A. Let T be a (residually multiplicity free) pseudo-representation $T : R \to A$ of dimension n. Following [BC09] we define the *ideal of reducibility of* T to be the smallest ideal I of A such that $T = T_1 + T_2 \bmod I$, where T_1, T_2 are pseudo-representations with the property that $T_i = \operatorname{tr} \tau_i \bmod \mathfrak{m}_A$. Let $\rho : R \to M_n(A)$ be an A-algebra homomorphism. Suppose that the mod $\mathfrak{m}_A$ reduction $\overline{\rho} : R \to M_n(\mathbf{F})$ of ρ has the form

$$\overline{\rho} = \begin{bmatrix} \tau_1 & * \\ & \tau_2 \end{bmatrix}$$

and is non-semi-simple. We define the ideal of reducibility of ρ to be the ideal of reducibility of the pseudo-representation $\operatorname{tr} \rho$.

Write $\mathcal{F} := \mathrm{Frac}(A)$, the total ring of fractions of A, which is a finite product of fields $\prod_{i=1}^s A_i$ (cf. e.g., [BC09], section 1.7). Fix $S_{ij} \subset \mathrm{Ext}^1_{\mathbf{F}[G]}(\tau_i, \tau_j)$ one-dimensional subspaces for $(i,j) \in \{(1,2),(2,1)\}$. Assume that the pseudo-representation $\operatorname{tr} \rho_i : R \to A_i$ is absolutely irreducible for every $i = 1, 2, \ldots, s$. Moreover, assume that $\overline{\rho} : R \to M_n(\mathbf{F})$ which factors through $\mathbf{F}[G] \to M_n(\mathbf{F})$ gives rise to a non-trivial element in S_{21}.

Proposition 4.1 ([BC09], Proposition 1.7.4)**.** *One has*

$$\dim_{\mathbf{F}} \mathrm{Ext}^1_{(R/\ker\rho)/\mathfrak{m}_A(R/\ker\rho)}(\tau_2, \tau_1) = 1.$$

Proof. Let us only note that Proposition 1.7.4 in [BC09] concerns $\ker T$ instead of $\ker \rho$. However, it follows from Proposition 1.6.4 of [BC09] along with our assumption on absolute irreducibility of $\operatorname{tr} \rho_i$ that $\ker \rho = \ker T$. □

The goal of this section is to give a sufficient condition guaranteeing that I is principal. Before we begin let us briefly explain the method. If the dimension of $\mathrm{Ext}^1_{(R/\ker\rho)/\mathfrak{m}_A(R/\ker\rho)}(\tau_1, \tau_2)$ ("opposite direction") is also one, I would be principal by Proposition 1.7.5 of [BC09]. To prove this we use Urban's construction to obtain an A-module $\mathcal{T} \oplus A$ together with a G-action which modulo $\mathfrak{m}_A$ gives a non-split extension in the "opposite direction". If $\mathcal{T} = A$, then this extension is a reduction of a representation of G into $\mathrm{GL}_2(A)$ and Proposition 1.7.4 in [BC09]

gives us the desired one-dimensionality. In the proof of Theorem 4.2 we formulate a condition that allows us to conclude that $\mathcal{T}/\mathfrak{m}_A\mathcal{T} = \mathbf{F}$ and essentially deduce from this that $\mathcal{T} = A$ by Nakayama's Lemma.

From now on assume that A is finite over $\mathcal{O}$. We will later apply this for $A = \mathbf{T}_\tau$ for which this assumption is satisfied (cf. Remark 3.4). Then by Theorem 1.1 in [Urb01] there exists an A-lattice $\mathcal{L}$ in $\mathcal{F}^n$ and an A-lattice $\mathcal{T}$ in $\mathcal{F}$ such that

$$0 \to \tau_2 \otimes_A \mathcal{T}/\mathfrak{m}_A\mathcal{T} \to \mathcal{L} \otimes_A \mathbf{F} \to \tau_1 \otimes_A \mathbf{F} \to 0. \tag{4.1}$$

As in [Urb01] (see also [Klo09], p. 159-160) we get a cocycle $c \in H^1(G, \mathrm{Hom}(\tau_1, \tau_2) \otimes \mathcal{T}/\mathfrak{m}_A\mathcal{T})$ and a map

$$\iota : \mathrm{Hom}(\mathcal{T}/\mathfrak{m}_A\mathcal{T}, \mathbf{F}) \to \mathrm{Ext}^1_{\mathbf{F}[G]}(\tau_1, \tau_2) = H^1(G, \mathrm{Hom}(\tau_1, \tau_2)), \quad f \mapsto (1 \otimes f)(c),$$

which is injective by Lemma 4.5 in [BK15].

Theorem 4.2. *If the image of ι lies in S_{12}, then I is principal.*

Proof. We have $\mathcal{T}/\mathfrak{m}_A\mathcal{T} = \mathbf{F}^s$ for some $s \in \mathbf{Z}_+$. Since $S_{12} = \mathbf{F}$, the injectivity of ι implies that $s = 1$. Hence (4.1) itself is an element of S_{12}. Moreover by a complete version of Nakayama's Lemma, $\mathcal{T}$ is generated by 1 element, say $x \in \mathcal{T}$, as an A-module. We claim that this implies that $\mathcal{T} = A$. Indeed, consider the A-module map $\phi : A \twoheadrightarrow \mathcal{T}$ given by $r \mapsto rx$. We will show that this map is injective. Suppose a is in the kernel. Then a annihilates $\mathcal{T}$. However, by definition of $\mathcal{T}$ and the fact that A is reduced and hence embeds into its ring of fractions $\mathcal{F}$ we can consider x and a as elements of $\mathcal{F} = \prod_i A_i$, i.e., write them as $a = (a_1, a_2, \ldots, a_s)$ and $x = (x_1, x_2, \ldots, x_s)$. We want to show that $a = 0$.

Let $\mathcal{J}$ be the set of i such that $a_i \neq 0$. First note that if $j \in \mathcal{J}$, then $xA \otimes_A A_j = 0$. Indeed, if $j \in \mathcal{J}$, then since $ax = 0$, we must have $x_j = 0$, so $x\alpha \otimes 1 = x\alpha a \otimes 1/a_j = 0$ for all $\alpha \in A$. Secondly note that if $j \notin \mathcal{J}$, then $xA \otimes_A A_j$ is of dimension ≤ 1 as an A_j-vector space. Indeed, let $\sum_k x\alpha_k \otimes \beta_k \in xA \otimes_A A_j$ and write π_j for the map $A \to A_j$. Then

$$\sum_k x\alpha_k \otimes \beta_k = \sum_k x \otimes \pi_j(\alpha_k)\beta_k = x \otimes \left(\sum_k \pi_j(\alpha_k)\beta_k\right) = (x \otimes 1) \cdot \left(\sum_k \pi_j(\alpha_k)\beta_k\right),$$

hence indeed $xA \otimes_A A_j$ is spanned over A_j by $x \otimes 1$.

Thus we get

$$\mathcal{T} \otimes_A \mathcal{F} = xA \otimes_A \prod_i A_i = \prod_i xA \otimes_A A_i = \prod_{i \notin \mathcal{J}} xA \otimes_A A_i$$

and each piece of the product is either 0 or A_j. Since $\mathcal{T}$ is a lattice we must have $\mathcal{T} \otimes_A \mathcal{F} = \mathcal{F} = \prod_i A_i$, and this forces $\mathcal{J} = \emptyset$.

Hence $\mathcal{L} \cong A^n$, so (4.1) is the reduction of a representation $R \to M_n(A)$. Thus by [BC09], Proposition 1.7.4, we get that

$$\dim_{\mathbf{F}} \mathrm{Ext}^1_{(R/\ker\rho)/\mathfrak{m}_A(R/\ker\rho)}(\tau_1, \tau_2) = 1$$

and thus by [loc.cit.], Proposition 1.7.5 the ideal I is principal. □

Lemma 4.3. *Let $\tau \in \mathfrak{T}_{\mathrm{mod}}$. There exists a representation $\rho_\tau : G_\Sigma \to \mathrm{GL}_2(\mathbf{T}_\tau)$ that reduces to τ modulo $\mathfrak{m}_{\mathbf{T}_\tau}$.*

Proof. Consider the representation

$$\rho'_\tau : G_\Sigma \to \prod_{\lambda:\tau_\lambda\cong\tau} \mathrm{GL}_2(\mathcal{O}) \subset \mathrm{GL}_2(\mathrm{Frac}(\mathbf{T}_\tau))$$

given by the representations $\tilde{\tau}_\lambda$. We now proceed as in the proof of Theorem 6.2 in [BK15] replacing $R^{\mathrm{tr},0}_\tau$ there with $\mathbf{T}_\tau$. We only give a brief outline here as the argument is essentially identical. Using Theorem 4.1 in [BK15] we deduce the existence of a Galois invariant lattice $\mathcal{L}$ in the representation space $\mathrm{Frac}(\mathbf{T}_\tau)^2$ of ρ'_τ and a $\mathbf{T}_\tau$-lattice $\mathcal{T}_\tau \subset \mathrm{Frac}(\mathbf{T}_\tau)$ which fits into the exact sequence

$$0 \to \mathcal{T}_\tau/I_\tau\mathcal{T}_\tau \to \mathcal{L}\otimes_{\mathbf{T}_\tau}\mathbf{T}_\tau/I_\tau \to \tilde{\chi}\otimes_{\mathcal{O}}\mathbf{T}_\tau/I_\tau \to 0, \tag{4.2}$$

where I_τ is the ideal of reducibility of the pseudo-representation $\mathrm{tr}\,\tau$.

As in the proof of Theorem 6.2 in [BK15] one notes that $\mathcal{L}\cong\mathcal{T}_\tau\oplus\mathbf{T}_\tau$ as $\mathbf{T}_\tau$-modules and then shows that $\mathcal{T}_\tau/I_\tau\mathcal{T}_\tau\otimes_{\mathbf{T}_\tau}\mathbf{F}\cong\mathbf{F}$, so we get $\mathcal{T}_\tau=\mathbf{T}_\tau$ as in the proof of Theorem 4.2 above. Thus (4.2) gives rise to a representation ρ_τ as in the statement of the Lemma. □

Remark 4.4. We note that Lemma 4.3 does not imply that there is a representation of G_Σ into $\mathrm{GL}_2(\mathbf{T})$. In the residually irreducible case this is in fact the case (cf. Lemma 3.27 in [DDT97]). Also if one assumes that τ is unique (i.e., that there is only one isomorphism class of non-semisimple residual representations with semi-simplification $1\oplus\chi$) this is also true and follows from the fact that in this case the universal deformation ring is generated by traces (cf. Corollary 3.2 in [SW97] and Proposition 7.13 in [BK13]). However, in general (when several different τs exist), this need no longer be the case. Lemma 4.3 can be viewed as providing a substitute for the existence of a representation into $\mathrm{GL}_2(\mathbf{T})$ when one fixes a particular residual representation τ. However, while $\mathbf{T}_\tau$ is a quotient of $\mathbf{T}$, in general there is no natural map $\mathbf{T}_\tau\to\mathbf{T}$.

Using Lemma 4.3 we can write I_τ for the ideal of reducibility of ρ_τ. Let us now apply Theorem 4.2 to our situation with $A=\mathbf{T}_\tau$. Note that the cuspidality of $\mathbf{T}_\tau$ ensures that the assumption of absolute irreducibility of the generic components of ρ_τ is satisfied.

Lemma 4.5. *One has $J_\tau = I_\tau$.*

Proof. This can be proved like Lemma 2.9 in [BK15]. □

Proposition 4.6. *If $\dim_{\mathbf{F}} H^1_\Sigma(F,\chi)=1$ then I_τ is a principal ideal.*

Proof. Because τ is an actual representation, Proposition 4.1 gives us that

$$\dim_{\mathbf{F}} \mathrm{Ext}^1_{(\mathbf{T}_\tau[G_\Sigma]/\ker\rho_\tau)/\mathfrak{m}_\tau(\mathbf{T}_\tau[G_\Sigma]/\ker\rho_\tau)}(\chi,1)=1.$$

We set $A=\mathbf{T}_\tau$, $G=G_\Sigma$ and $S_{21}=H^1_\Sigma(\mathbf{Q},\chi)$. The claim follows from Theorem 4.2 and Lemma 4.7 below. □

Lemma 4.7. *The image of $\iota : \mathrm{Hom}(\mathcal{T}/\mathfrak{m}_{\mathbf{T}}\mathcal{T},\mathbf{F}) \to H^1(G_\Sigma,\chi)$ is contained in $H^1_\Sigma(F,\chi)$.*

Proof. This follows from Lemma 4.5 in [BK15], except that we do not need the assumptions 2.5 and 4.2 there, as we do not claim surjectivity of ι here. □

Combined with Proposition 3.9 we obtain the following result.

Theorem 4.8. *Suppose that* $\#H^1_\Sigma(F, \tilde{\chi}^{-1} \otimes E/\mathcal{O}) \leq \#\mathbf{T}/J$. *If* $\dim_{\mathbf{F}} H^1_\Sigma(F, \chi) = 1$ *and the Eisenstein ideal* J *is not principal, then* $\#\mathfrak{T}_{\mathrm{mod}} > \dim_{\mathbf{F}} H^1_\Sigma(F, \chi^{-1})$.

We end this section by stating a cohomological criterion guaranteeing the principality of the Eisenstein ideal.

Corollary 4.9. *Suppose that* $\#H^1_\Sigma(F, \tilde{\chi}^{-1} \otimes E/\mathcal{O}) \leq \#\mathbf{T}/J$. *Suppose furthermore that* $\dim_{\mathbf{F}} H^1_\Sigma(F, \chi) = \dim_{\mathbf{F}} H^1_\Sigma(F, \chi^{-1}) = 1$. *Then* J *is principal.*

Proof. In this case there is only one line in $H^1_\Sigma(F, \chi^{-1})$ which is modular by Theorem 3.7, i.e., we must have $\#\mathfrak{T}_{\mathrm{mod}} = 1$. The claim now follows directly from Theorem 4.8. □

5. $F = \mathbf{Q}$

In this section we take $F = \mathbf{Q}$. As in section 3 we set $\tau_1 = 1$ and $\tau_2 = \chi$ where χ is a character ramified at p. By class field theory we can write $\chi = \omega^{k-1}\psi$ for some k with $2 \leq k \leq p-1$ and a character ψ unramified at p. We write $\tilde{\psi}$ for the Teichmüller lift of ψ and $\tilde{\chi} = \tilde{\psi}\epsilon^{k-1}$. The assumption that $N\mathfrak{q} \not\equiv 1 \pmod{p}$ for all $\mathfrak{q} \in \Sigma$ is unnecessary for any of the results in this section.

5.1. **Proving** $\#H^1_\Sigma(\mathbf{Q}, \tilde{\chi}^{-1} \otimes E/\mathcal{O}) \leq \#\mathbf{T}/J$**.** For the convenience of the reader let us recall our setup. We denote by $\mathbf{T}'$ the Hecke algebra acting on the space of cusp forms $S_k(\Gamma_0(\mathfrak{N}))$ (as before $\mathfrak{N} \in \mathbf{Z}_+$ is only divisible by primes in $\Sigma - \{p\}$), i.e., the $\mathcal{O}$-subalgebra of $\mathrm{End}_{\mathbf{C}}(S_k(\Gamma_0(\mathfrak{N})))$ generated by T_ℓ for all $\ell \nmid \mathfrak{N}p$. Set J' to be the ideal of $\mathbf{T}'$ generated by the operators $T_\ell - (1 + \tilde{\psi}(\ell)\ell^{k-1})$ for all $\ell \notin \Sigma$. Let $\mathfrak{m}$ be the maximal ideal of $\mathbf{T}'$ containing J' and write $\mathbf{T}$ for the completion of $\mathbf{T}'$ at $\mathfrak{m}$. Set J to be the image of J' in $\mathbf{T}$.

Put

$$\eta(\tilde{\psi}, k) := B_k(\tilde{\psi}) \cdot \prod_{\ell \in \Sigma - \{p\}} (1 - \tilde{\psi}(\ell)\ell^k),$$

where $B_k(\tilde{\psi})$ is the kth Bernoulli number of $\tilde{\psi}$. Here we treat $\tilde{\psi}$ as a Dirichlet character of $\mathbf{Z}/\mathfrak{M}\mathbf{Z}$ rather than of $\mathbf{Z}/\mathfrak{N}\mathbf{Z}$, where $\mathfrak{M}$ is the largest factor of $\mathfrak{N}$ only divisible by primes dividing the conductor of $\tilde{\psi}$ (in other words we do not set $\tilde{\psi}(\ell) = 0$ if $\ell \nmid \mathrm{cond}(\tilde{\psi})$).

Remark 5.1. It is expected that $\#\mathbf{T}/J \geq \#\mathcal{O}/\eta(\tilde{\psi}, k)$ as long as $k > 2$ or $k = 2$ but $\psi \neq 1$. The case $k = 2$ and $\psi = 1$ is slightly different. For $\Sigma = \{p, \ell\}$ with ℓ a prime different from p Mazur [Maz77] Proposition II.9.7 proved

$$\mathrm{val}_p(\#\mathbf{T}/J) = [\mathcal{O} : \mathbf{Z}_p] \, \mathrm{val}_p(\mathrm{num}\left(\frac{\ell - 1}{12}\right)).$$

This corresponds to $\eta(1 \pmod{\ell}, k)$ where we - different to our convention above - take $\tilde{\psi} = 1$ as a Dirichlet character modulo ℓ, i.e. put $\tilde{\psi}(\ell) = 0$. In the proof of Proposition 5.2 below the case $k = 2$, $\psi = 1$ is excluded due to the different form of the constant term of the Eisenstein series. See also [Oht14] and [Yoo16] who treat a related Hecke algebra when $k = 2$, $\psi = 1$ and the level is composite.

We now prove that $\#\mathbf{T}/J \geq \#\mathcal{O}/\eta(\tilde{\psi}, k)$ under some conditions.

Proposition 5.2. *Let* $k \geq 2$. *If* $k = 2$ *assume that* $\psi \neq 1$. *Let* $N = \mathrm{cond}(\tilde{\psi})$, $\Sigma = \{p, \ell, q \mid N\}$ *for some prime* $\ell \nmid Np$. *Then there exists* $m > 0$ *such that* $\#\mathbf{T}/J \geq \#\mathcal{O}/\eta(\tilde{\psi}, k)$ *for* $\mathfrak{N} = N\ell^m$.

Remark 5.3. We note that our proof in fact shows that $\#\tilde{\mathbf{T}}/\tilde{J} \geq \#\mathcal{O}/\eta(\tilde{\psi}, k)$, where $\tilde{\mathbf{T}}$ is the Hecke algebra including T_p, and $\tilde{J}$ has the additional generator $T_p - (1 + \tilde{\psi}(p)p^{k-1})$. Note that $\mathbf{T}/J \twoheadrightarrow \tilde{\mathbf{T}}/\tilde{J}$. We do not use the congruence module $\tilde{\mathbf{T}}/\tilde{J}$ in this paper, but for other applications it might be of interest that the corresponding cusp forms congruent to the Eisenstein series are ordinary at p. Let us also note that for Proposition 5.2 we allow for the primes dividing $\mathfrak{N}$ to be congruent to 1 mod p.

Proof of Proposition 5.2. We partially adapt arguments from lectures notes by Skinner from 2002 which treat the case of weight $k = 2$ (making explicit Wiles' argument in the proof of the totally real Iwasawa Main Conjecture).

If $\eta(\tilde{\psi}, k) \in \mathcal{O}^\times$ then there is nothing to prove. So assume $\mathrm{val}_\varpi(\eta(\tilde{\psi}, k)) > 0$. Let ϕ be a non-trivial Dirichlet character of conductor M such that $\phi(-1) = (-1)^l$ for $l \geq 1$. Set

$$E_l(\phi) = \frac{L(\phi, 1-l)}{2} + \sum_{n=1}^{\infty} \left(\sum_{d|n} \phi(d) d^{l-1} \right) q^n \in M_l(M, \phi)$$

to be the Eisenstein series of weight l whose constant term is $L(\phi, 1-l)/2$ (cf. [Miy89], Theorem 4.7.1).

Proposition 5.4 ([Oza17] Proposition 0.3)**.** *If $l = 2$ assume that $\phi \neq 1$. The constant term of $E_l(\phi)$ at the cusp $[u : v] \in \mathbf{P}^1(\mathbf{Q})$ equals $\phi(u)^{-1}L(\phi, 1-l)/2$ if $M \mid v$ and zero otherwise.*

By a generalisation of a result of Washington (see [Sun10] Theorem 4) we know that there exists an auxiliary character φ of conductor ℓ^m for some $m > 0$ (which we fix from now on) with $\varphi(-1) = (-1)^{k-1}$ such that

$$L(\tilde{\psi}\varphi, 0)L(\varphi^{-1}, 2-k) \in \mathcal{O}^\times. \tag{5.1}$$

Then we put

$$G := E_1(\tilde{\psi}\varphi) \cdot E_{k-1}(\varphi^{-1}) \in M_k(N\ell^m, \tilde{\psi})$$

and deduce that its constant terms are

$$\begin{cases} \tilde{\psi}^{-1}(u)\frac{L(\tilde{\psi}\varphi,0)L(\varphi^{-1},2-k)}{4} & \text{if } N\ell^m \mid v \\ 0 & \text{else.} \end{cases}$$

In the following we will use G, which clearly has p-integral Fourier coefficients and a constant term which is a p-unit, to prove a congruence of the following Eisenstein series to a cusp form. Put

$$F_m(z) := E_k(\tilde{\psi})(\ell^{m-1}z) - \tilde{\psi}(\ell)\ell^k E_k(\tilde{\psi})(\ell^m z).$$

We apply Proposition 1.2 in [BM16] (generalized to $k \geq 2$ (and $\psi \neq 1$ if $k = 2$) in [BM18] Proposition 4) with $M = \ell^{m-1}$ (for $E_k(\tilde{\psi})(\ell^{m-1}z)$) and $M = \ell^m$ (for $E_k(\ell^m z)$) to compute that the constant term of F_m at the cusp $[u : v]$ equals

$$-\tilde{\psi}(u)^{-1}\frac{B_{k,\tilde{\psi}}}{2k}(1 - \tilde{\psi}(\ell)\ell^k) = \tilde{\psi}(u)^{-1}\frac{L(\tilde{\psi}, 1-k)}{2}(1 - \tilde{\psi}(\ell)\ell^k)$$

if $N\ell^m \mid v$ and zero otherwise.

This now allows us to get a bound on $\mathbf{T}/J$: Define

$$H = F_m - \frac{\eta(\tilde{\psi}, k)}{a_0(G)k} \cdot G,$$

where $a_0(G)$ denotes the constant term of G at infinity (which is a p-unit - see above). Then the previous discussion shows that $H \in S_k(N\ell^m, \tilde{\psi})$ with q-expansion coefficients in $\mathcal{O}$.

We can then define a surjective $\mathcal{O}$-algebra homomorphism $\phi : \mathbf{T}/J \twoheadrightarrow \mathcal{O}/\eta(\tilde{\psi}, k)$ such that $T_q \mapsto 1 + \tilde{\psi}(q)q^{k-1}$ for all primes $q \nmid N\ell p$ as follows:

First note that H has a Fourier coefficient which is a p-unit. To see this, note $a_{\ell^{m-1}}(F_m) = a_1(E_k(\tilde{\psi})) = 1$, so

$$a_{\ell^{m-1}}(H) = 1 - \frac{\eta(\tilde{\psi}, k)}{a_0(G)k} \cdot a_{\ell^{m-1}}(G) \in \mathcal{O}^\times,$$

where a_n denotes the n-th Fourier coefficient of the respective modular form.

This allows us to extend H to an $\mathcal{O}$-basis of $S_k(\ell^m N, \mathcal{O})$, say $m_0 = H, m_1, \dots m_r$. Let $t \in \mathbf{T}$. Then

$$tm_0 = \sum_{i=0}^{r} \lambda_i(t) m_i, \text{ for } \lambda_i(t) \in \mathcal{O}.$$

We can now define the (surjective) $\mathcal{O}$-module homomorphism $\phi : \mathbf{T} \to \mathcal{O}/\eta(\tilde{\psi}, k)$ by $\phi(t) = \lambda_0(t) \pmod{\eta(\tilde{\psi}, k)}$, and it is easy to check that this, in fact, is even a ring homomorphism, and that it factors through $\mathbf{T}/J$ since $T_q - 1 - \tilde{\psi}(q)q^{k-1}$ annihilates F_m. □

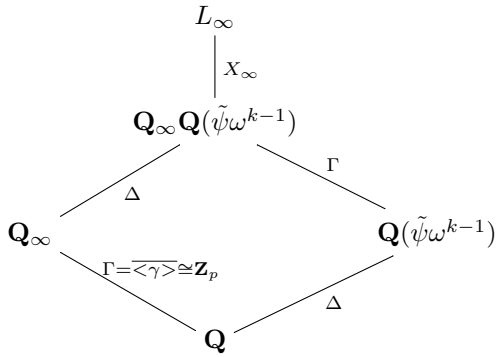
Remark 5.5. Dummigan-Fretwell [DF14], Billerey-Menares [BM18], and Spencer [Spe18] use similar linear combinations of Eisenstein series to prove mod p congruences using the Deligne-Serre lifting lemma. Note, however, that our F_m has non-vanishing constant terms only for $N\ell^m \mid v$, which makes it possible to remove them by using the auxiliary G and prove the full expected $\mathbf{T}/J$ bound. By [BKK14] Proposition 4.3 this gives a lower bound on the amount and depth of Eisenstein congruences:

For a Hecke eigensystem $\lambda : \mathbf{T} \to \mathcal{O}$ write m_λ for the depth of its p-adic congruence with $E_k(\tilde{\psi})$, i.e., m_λ is the largest integer s such that $\lambda(T_\ell) \equiv 1 + \tilde{\psi}(\ell)\ell^{k-1} \pmod{\varpi^s}$ for every $\ell \notin \Sigma$. Write e for the ramification index of $\mathcal{O}$ over $\mathbf{Z}_p$. Then combining Proposition5.2 with [BKK14] Proposition 4.3 we obtain

$$\frac{1}{e}\sum_{\lambda} m_\lambda \geq \mathrm{val}_p(\#\mathbf{T}/J) \geq \mathrm{val}_p(\#\mathcal{O}/\eta(\tilde{\psi}, k)).$$

Proposition 5.6. *One has* $\#H^1_\Sigma(\mathbf{Q}, \tilde{\chi}^{-1} \otimes E/\mathcal{O}) \leq \#\mathcal{O}/\eta(\tilde{\psi}, k)$.

Proof. Consider the following diagram of fields with corresponding Galois groups:



Here $\mathbf{Q}(\tilde{\psi}\omega^{k-1})$ denotes the splitting field of $\tilde{\psi}\omega^{k-1}$ and L_∞ is the maximal abelian extension of $\mathbf{Q}_\infty\mathbf{Q}(\tilde{\psi}\omega^{k-1})$ unramified everywhere.

We first prove that

$$\#H^1_{\{p\}}(\mathbf{Q}, \tilde{\chi}^{-1}\otimes E/\mathcal{O}) \leq \#\mathcal{O}/B_k(\tilde{\psi}). \tag{5.2}$$

This follows from the Main Conjecture of Iwasawa theory proven my Mazur-Wiles, as we briefly explain for the convenience of the reader: For $K = \mathbf{Q}$ or $\mathbf{Q}_\infty$ and φ a character of G_K put

$$H^1_{\mathrm{Gr}}(K, E/\mathcal{O}(\varphi)) := \ker(H^1(K, E/\mathcal{O}(\varphi)) \to \prod_v H^1(I_v, E/\mathcal{O}(\varphi))).$$

A result of Flach (see [Och00] Proposition 4.1(1)) tells us that

$$H^1_{\{p\}}(\mathbf{Q}, E/\mathcal{O}(\tilde{\psi}^{-1}\epsilon^{1-k})) \subseteq H^1_{\mathrm{Gr}}(\mathbf{Q}, E/\mathcal{O}(\tilde{\psi}^{-1}\epsilon^{1-k})).$$

Let $\Psi = \tilde{\psi}^{-1}\omega^{1-k}$ and $X_{\infty,\Psi}$ be the Ψ-isotypical component of X_∞ for the action of Δ. We have $X_{\infty,\Psi} = \mathrm{Hom}(H^1_{\mathrm{Gr}}(\mathbf{Q}_\infty, E/\mathcal{O}(\Psi)), E/\mathcal{O})$. Using the Γ-module structure of $X_{\infty,\Psi}$ from this we get

$$X_{\infty,\Psi}/(T-(\kappa_0^{1-k}-1)) = \mathrm{Hom}(H^1_{\mathrm{Gr}}(\mathbf{Q}, E/\mathcal{O}(\Psi(\epsilon/\omega)^{1-k})), E/\mathcal{O}),$$

where $\kappa_0 = (\epsilon/\omega)(\gamma)$. Since both modules are finite and $\Psi(\epsilon/\omega)^{1-k} = \tilde{\psi}^{-1}\epsilon^{1-k}$ we get

$$\#H^1_{\mathrm{Gr}}(\mathbf{Q}, E/\mathcal{O}(\tilde{\psi}^{-1}\epsilon^{1-k})) = \#X_{\infty,\Psi}/(T-(\kappa_0^{1-k}-1)).$$

Since $X_{\infty,\Psi}$ has no finite $\Lambda := \mathbf{Z}_p[[\Gamma]]$-submodules (see [MW84] Proposition 1 on p. 193) one obtains

$$\#X_{\infty,\Psi}/(T-(\kappa_0^{1-k}-1)) \leq \#\Lambda/(g_\Psi, T-(\kappa_0^{1-k}-1)),$$

where $g_\Psi \in \Lambda$ is the characteristic power series of $X_{\infty,\Psi}$. By the Main Conjecture (see [MW84] Theorem p. 214) we have

$$g_\Psi(\kappa_0^s - 1) = L_p(\omega\Psi^{-1}, s),$$

where the latter is the p-adic L-function with the following interpolation property (see [Was97] Theorem 5.11):

$$L_p(\omega\Psi^{-1}, 1-n) = -(1-\tilde{\psi}(p)p^{n-1})\frac{B_n(\tilde{\psi})}{n}, \text{ for } n \geq 1.$$

Setting $n = k$ and observing that $(1-\tilde{\psi}(p)p^{k-1}) \in \mathcal{O}^\times$ we obtain (5.2).

A repeated application of Lemma 6.2 in the next section (by selecting s in that lemma to be sufficiently large and taking n in that lemma to be $k-1$) leads us now to the bound by $\eta(\tilde{\psi}, k)$ on $H^1_\Sigma(\mathbf{Q}, \tilde{\chi}^{-1}\otimes E/\mathcal{O})$. □

From now on assume that $\tilde{\psi}$, Σ and $\mathbf{T}$ are as in Proposition 5.2. By combining Propositions 3.10, 5.2 and 5.6 we obtain the following corollary.

Corollary 5.7. *We have*

$$\#\mathbf{T}/J = \#\mathcal{O}/\eta(\tilde{\psi}, k) = \#H^1_\Sigma(\mathbf{Q}, \tilde{\chi}^{-1}\otimes E/\mathcal{O}).$$

Then in the case $F = \mathbf{Q}$ we obtain the following stronger versions of Theorem 4.8 and Corollary 4.9.

Corollary 5.8. *If* $\dim_{\mathbf{F}} H^1_\Sigma(\mathbf{Q}, \chi) = 1$ *and the Eisenstein ideal J is not principal, then* $\#\mathfrak{T}_{\mathrm{mod}} > \dim_{\mathbf{F}} H^1_\Sigma(\mathbf{Q}, \chi^{-1})$.

Remark 5.9. Suppose we consider the set of extensions $\overline{\rho} = \begin{bmatrix} 1 & * \\ & \chi \end{bmatrix} : G_{\Sigma'} \to \mathrm{GL}_2(\mathbf{F})$ with χ ramified at all primes in $\Sigma' \supset \{p\}$. Then Corollary 5.8 can be viewed as asserting that more than $\dim_{\mathbf{F}} H^1_\Sigma(\mathbf{Q}, \chi^{-1})$ of these extensions arise from modular representations ρ_f which are ramified at no more than one additional prime (the prime ℓ in Proposition 5.2, i.e., $\Sigma = \Sigma' \cup \{\ell\}$) as long as J is not principal and $\dim_{\mathbf{F}} H^1_\Sigma(\mathbf{Q}, \chi) = 1$.

Corollary 5.10. *Suppose that* $\dim_{\mathbf{F}} H^1_\Sigma(\mathbf{Q}, \chi) = \dim_{\mathbf{F}} H^1_\Sigma(\mathbf{Q}, \chi^{-1}) = 1$. *Then J is principal.*

5.2. **Congruence criterion.** The assumption that the Eisenstein ideal is not principal may be difficult to check directly, so we will translate it here into a criterion that relies on counting congruences. We still let $\tilde{\psi}$, Σ and $\mathbf{T}$ be as in Proposition 5.2.

For a Hecke eigensystem $\lambda : \mathbf{T} \to \mathcal{O}$ write m_λ for the depth of its p-adic congruence with $E_k(\tilde{\psi})$, i.e., m_λ is the largest integer s such that $\lambda(T_\ell) \equiv 1 + \tilde{\psi}(\ell)\ell^{k-1} \bmod \varpi^s$ for every $\ell \notin \Sigma$. Write e for the ramification index of $\mathcal{O}$ over $\mathbf{Z}_p$.

Theorem 5.11. *Assume that* $\dim_{\mathbf{F}} H^1_\Sigma(\mathbf{Q}, \chi) = 1$. *If*

$$\frac{1}{e} \sum_\lambda m_\lambda > \mathrm{val}_p(\#\mathcal{O}/\eta(\tilde{\psi}, k))$$

then J is not principal and $\#\mathfrak{T}_{\mathrm{mod}} > \dim_{\mathbf{F}} H^1_\Sigma(\mathbf{Q}, \chi^{-1})$.

Proof. Assume J is principal. Writing $T_\lambda = \mathcal{O}$, $J_\lambda = \varpi^{m_\lambda}\mathcal{O}$, $T = \mathbf{T}$ and J as before for the Eisenstein ideal, we can apply Corollary 2.7 in [BKK14] (again note as in Proposition 3.9 that the principality of the J_λs) to conclude that then

$$\mathrm{val}_\varpi(\#T/J) = \mathrm{val}_\varpi\left(\#\prod_\lambda T_\lambda/J_\lambda\right) = \frac{[E : \mathbf{Q}_p]}{e} \sum_\lambda m_\lambda.$$

The left-hand side equals $\mathrm{val}_\varpi(\#\mathcal{O}/\eta(\tilde{\psi}, k))$ by Corollary 5.7. Replacing ϖ-adic valuations with p-adic ones we get $\frac{1}{e}\sum_\lambda m_\lambda = \mathrm{val}_p(\#\mathcal{O}/\eta(\tilde{\psi}, k))$, which contradicts our assumption. So we conclude that J is not principal and the proposition follows by applying Proposition 3.9. □

6. Analysis of $H^1_\Sigma(\mathbf{Q}, \mathbf{F}(n))$

In this section we prove bounds on certain Selmer groups. The assumption that $\ell \not\equiv 1 \pmod p$ for all $\ell \mid N$ is not needed for Proposition 6.1 and Lemma 6.2.

Proposition 6.1. *For $2 \le k \le p-1$ and k even we have*

$$\mathrm{val}_p(\#H^1_\Sigma(\mathbf{Q}, \mathbf{F}(1-k))) \ge [\mathbf{F} : \mathbf{F}_p](\min\{\mathrm{val}_p(B_{1,\omega^{k-1}}), 1\} + \sum_{\ell \in \Sigma - \{p\}} \min\{\mathrm{val}_p(1-\ell^k), 1\}).$$

Proof. By Fontaine-Laffaille theory (see e.g. [Bre01] Proposition 9.1.2(i)) any Fontaine-Laffaille D_p extension

$$0 \to \mathbf{F} \to \overline{\rho} \to \mathbf{F}(k-1) \to 0$$

is split on I_p, so $H^1_f(\mathbf{Q}_p, \mathbf{F}(1-k)) = H^1_{\mathrm{ur}}(\mathbf{Q}_p, \mathbf{F}(1-k)) := (\ker(H^1(\mathbf{Q}_p, \mathbf{F}(1-k)) \to H^1(I_p, \mathbf{F}(1-k)))$. We therefore have

$$H^1_{\{p\}}(\mathbf{Q}, \mathbf{F}(1-k)) = \ker\left(H^1(\mathbf{Q}, \mathbf{F}(1-k)) \to \prod_{\ell} H^1(I_\ell, \mathbf{F}(1-k))\right).$$

As in section 2 of [Ski06] we can argue that restriction to $G_{\mathbf{Q}(\mu_p)}$ gives

$$H^1_{\{p\}}(\mathbf{Q}, \mathbf{F}(1-k)) = \mathrm{Hom}_{\mathrm{Gal}(\mathbf{Q}(\mu_p)/\mathbf{Q})}(C_{\mathbf{Q}(\mu_p)}, \mathbf{F}(1-k)),$$

where $C_{\mathbf{Q}(\mu_p)}$ denotes the class group of $\mathbf{Q}(\mu_p)$.

The p-primary part of $C_{\mathbf{Q}(\mu_p)}$ on which the action of $\mathrm{Gal}(\mathbf{Q}(\mu_p)/\mathbf{Q})$ is via ω^{1-k} has order given by $L(0, \omega^{k-1}) = -B_{1,\omega^{k-1}}$ by [MW84] Theorem 2 p. 216 (see also [Ski06] Theorem 2.1.3). This shows that $\#H^1_{\{p\}}(\mathbf{Q}, \mathbf{F}(1-k)) \geq (\#\mathbf{F}_p/B_{1,\omega^{k-1}})^{[\mathbf{F}:\mathbf{F}_p]}$ (equality holds if $C^{\omega^{1-k}}_{\mathbf{Q}(\mu_p)}$ is cyclic).

The proposition now follows from Lemma 6.2 below applied with $n = k-1$. $\square$

Lemma 6.2. *Let $n \neq 0$ be an integer and set $m := \mathrm{val}_p(\tilde{\psi}(\ell)\ell^{n+1} - 1)$ for ψ a Dirichlet character unramified away from $\Sigma - \{p\}$. Let $s \geq me$ be an integer, where e is the ramification index of $\mathcal{O}$ over $\mathbf{Z}_p$. Set $W = E/\mathcal{O}(\tilde{\psi}^{-1}\epsilon^{-n})$ and $W_s = W[\varpi^s]$. Suppose $\ell \in \Sigma - \{p\}$ and let $\Sigma' \subset \Sigma$ with $\ell \notin \Sigma'$. Then one has*

$$\#H^1_{\Sigma' \cup \{\ell\}}(\mathbf{Q}, W_s) \leq (\#\mathcal{O}/p^m\mathcal{O})\#H^1_{\Sigma'}(\mathbf{Q}, W_s).$$

Proof. First assume that W is ramified at ℓ. Then $W^{I_\ell} = 0$ and we use [BK13] Lemma 5.6 to conclude that

$$H^1_{\Sigma' \cup \{\ell\}}(\mathbf{Q}, W_s) = H^1_{\Sigma'}(\mathbf{Q}, W_s).$$

From now on assume that W is unramified at ℓ. By [Rub00], Theorem 1.7.3 we have an exact sequence

$$0 \to H^1_{\Sigma'}(\mathbf{Q}, W_s) \to H^1_{\Sigma' \cup \{\ell\}}(\mathbf{Q}, W_s) \to \frac{H^1(\mathbf{Q}_\ell, W_s)}{H^1_{\mathrm{ur}}(\mathbf{Q}_\ell, W_s)}.$$

Lemma 1.3.8(ii) in [Rub00] tells us that $H^1_{\mathrm{ur}}(\mathbf{Q}_\ell, W_s) = H^1_f(\mathbf{Q}_\ell, W_s)$, where $H^1_{\mathrm{un}}(\mathbf{Q}_\ell, W_s) := \ker(H^1(\mathbf{Q}_\ell, W_s) \to H^1(I_\ell, W_s))$. We also get

$$H^1(I_\ell, W_s) = \mathrm{Hom}(I_\ell^{\mathrm{ab}}, W_s) = \mathrm{Hom}(\mathbf{Z}_p(1), W_s) = W_s(-1). \tag{6.1}$$

This gives an upper bound of $(\#\mathbf{F})^s = \#W_s$ on the order of the quotient $\frac{H^1(\mathbf{Q}_\ell, W_s)}{H^1_{\mathrm{ur}}(\mathbf{Q}_\ell, W_s)}$. To prove the claim it is enough to show that the image of the map $H^1(\mathbf{Q}_\ell, W_s) \to H^1(I_\ell, W_s)$ has order not greater than $\#\mathcal{O}/p^m\mathcal{O}$. To do so consider the inflation-restriction sequence (where we set $G := \mathrm{Gal}(\mathbf{Q}_\ell^{\mathrm{ur}}/\mathbf{Q}_\ell)$):

$$H^1(G, W_s) \to H^1(\mathbf{Q}_\ell, W_s) \to H^1(I_\ell, W_s)^G \to H^2(G, W_s).$$

The last group in the above sequence is zero since $G \cong \hat{\mathbf{Z}}$ and $\hat{\mathbf{Z}}$ has cohomological dimension one. This means that the image of the restriction map $H^1(\mathbf{Q}_\ell, W_s) \to H^1(I_\ell, W_s)$ equals $H^1(I_\ell, W_s)^G$. Let us show that the latter module has order $\leq \#\mathcal{O}/p^m\mathcal{O}$. Indeed,

$$\begin{aligned} H^1(I_\ell, W_s)^G &= \mathrm{Hom}_G(I_\ell, W_s) = \mathrm{Hom}_G(I_\ell^{\mathrm{tame}}, W_s) \\ &= \mathrm{Hom}_G(\mathbf{Z}_p(1), p^{-s}\mathcal{O}/\mathcal{O}(\tilde{\psi}^{-1}\epsilon^{-n})) = \mathrm{Hom}_G(\mathbf{Z}_p, p^{-s}\mathcal{O}/\mathcal{O}(\tilde{\psi}^{-1}\epsilon^{-n-1})). \end{aligned} \tag{6.2}$$

So, $\phi \in H^1(I_\ell, W_s)$ lies in $H^1(I_\ell, W_s)^G = \mathrm{Hom}_G(\mathbf{Z}_p, p^{-s}\mathcal{O}/\mathcal{O}(\tilde{\psi}^{-1}\epsilon^{-n-1}))$ if and only if $\phi(x) = g \cdot \phi(g^{-1} \cdot x) = g \cdot \phi(x) = \tilde{\psi}^{-1}\epsilon^{-n-1}(g)\phi(x)$ for every $x \in I_\ell$ and every $g \in G$, i.e., if and only if

$$(\tilde{\psi}^{-1}\epsilon^{-n-1}(g) - 1)\phi(x) \in \mathcal{O} \quad \text{for every } x \in I_\ell,\ g \in G. \tag{6.3}$$

Since Frob_ℓ topologically generates G, we see that (6.3) holds if and only if it holds for every $x \in I_\ell$ and for $g = \mathrm{Frob}_\ell$. So condition (6.3) becomes

$$(1 - \tilde{\psi}^{-1}(\ell)\ell^{-n-1})\phi(x) \in \mathcal{O} \quad \text{for every } x \in I_\ell. \tag{6.4}$$

Since $\mathrm{val}_p(1-\tilde{\psi}^{-1}(\ell)\ell^{-n-1}) = \mathrm{val}_p(\tilde{\psi}(\ell)\ell^{n+1}-1) = m$, we get that $\phi(x) \in p^{-m}\mathcal{O}/\mathcal{O}$, as claimed. □

When $s = 1$ and $\psi = 1$ we prove a stronger result.

Lemma 6.3. *Let $n \neq 0$ be an integer. Suppose $\ell \in \Sigma - \{p\}$ and $m := \min\{\mathrm{val}_p(\ell^{n+1}-1), 1\}$. Let $\Sigma' \subset \Sigma$ with $\ell \notin \Sigma'$. Write $q = \#\mathbf{F}$. Then one has*

$$\#H^1_{\Sigma'\cup\{\ell\}}(\mathbf{Q}, \mathbf{F}(-n)) = q^m \#H^1_{\Sigma'}(\mathbf{Q}, \mathbf{F}(-n)).$$

Proof. If $m = 0$ the inequality

$$\#H^1_{\Sigma'\cup\{\ell\}}(\mathbf{Q}, \mathbf{F}(-n)) \leq q^m \#H^1_{\Sigma'}(\mathbf{Q}, \mathbf{F}(-n)) \tag{6.5}$$

follows directly from Lemma 6.2, while the opposite inequality is clear.

As before, set $W = E/\mathcal{O}(-n)$ and $W_s = W[\varpi^s]$. Then for $m = 1$, [Rub00], Theorem 1.7.3 gives us again an exact sequence

$$0 \to H^1_{\Sigma'}(\mathbf{Q}, W_1) \to H^1_{\Sigma'\cup\{\ell\}}(\mathbf{Q}, W_1) \to \frac{H^1(\mathbf{Q}_\ell, W_1)}{H^1_{\mathrm{ur}}(\mathbf{Q}_\ell, W_1)}, \tag{6.6}$$

and as in the proof of Lemma 6.2 we see that the oder of the module on the right is bounded by q. This yields (6.5).

We now show that the third arrow (which we call loc^s following [Rub00], section 1.7) in (6.6) is surjective if $\mathrm{val}_p(\ell^{n+1} - 1) > 0$ and is the zero-map otherwise.

As, before, since W is unramified at ℓ, Lemma 1.3.5(iv) in [Rub00] implies that $H^1_{\mathrm{ur}}(\mathbf{Q}_\ell, W) = H^1_f(\mathbf{Q}_\ell, W)$, where $H^1_{\mathrm{un}}(\mathbf{Q}_\ell, W) := \ker(H^1(\mathbf{Q}_\ell, W) \to H^1(I_\ell, W))$. Similarly, this time using Lemma 1.3.8(ii) in [Rub00] we get that $H^1_{\mathrm{ur}}(\mathbf{Q}_\ell, W_1) = H^1_f(\mathbf{Q}_\ell, W_1)$, where $H^1_{\mathrm{un}}(\mathbf{Q}_\ell, W_1) := \ker(H^1(\mathbf{Q}_\ell, W_1) \to H^1(I_\ell, W_1))$.

Write $\mathcal{S}_{\Sigma'}(\mathbf{Q}, W_1^*)$ for the kernel of the map $H^1_{\Sigma'}(\mathbf{Q}, W_1^*) \to \bigoplus_{v\in\Sigma'} H^1(\mathbf{Q}_v, W_1^*)$ (cf. [Rub00], p.21-22) and analogously for $\mathcal{S}_{\Sigma'\cup\{\ell\}}$. Here $W_1^* = \mathrm{Hom}(W_1, \mathbf{F})(1) = \mathbf{F}(n+1)$. The cup product induces a perfect pairing $H^1(\mathbf{Q}_v, W_1) \times H^1(\mathbf{Q}_v, W_1^*) \to H^2(\mathbf{Q}_v, \mathbf{F}(1)) \cong \mathbf{F}(1)$. Theorem 1.7.3(ii) in [Rub00] yields an exact sequence

$$0 \to \mathcal{S}_{\Sigma'\cup\{\ell\}}(\mathbf{Q}, W_1^*) \to \mathcal{S}_{\Sigma'}(\mathbf{Q}, W_1^*) \xrightarrow{\mathrm{loc}_f} H^1_f(\mathbf{Q}_\ell, W_1^*) \tag{6.7}$$

where the last module again equals $H^1_{\mathrm{ur}}(\mathbf{Q}_\ell, W_1^*)$ as above. By the same theorem the image of loc^s is the largest subspace of $\frac{H^1(\mathbf{Q}_\ell, W_1)}{H^1_{\mathrm{ur}}(\mathbf{Q}_\ell, W_1)}$ having the property that all of its elements pair to zero with any element of the image of loc_f. Thus to show surjectivity of loc^s, it is enough to show that loc_f is the zero map, i.e., that $\mathcal{S}_{\Sigma'\cup\{\ell\}}(\mathbf{Q}, W_1^*) = \mathcal{S}_{\Sigma'}(\mathbf{Q}, W_1^*)$. Consider the inclusion $\mathcal{S}_{\Sigma'\cup\{\ell\}}(\mathbf{Q}, W_1^*) \subset \mathcal{S}_{\Sigma'}(\mathbf{Q}, W_1^*)$ and assume that $\phi \in \mathcal{S}_{\Sigma'}(\mathbf{Q}, W_1^*)$. This in particular means that $\phi|_{G_{\mathbf{Q}_\ell}} \in H^1_{\mathrm{ur}}(\mathbf{Q}_\ell, W_1^*)$. If we can show that this forces $\phi|_{G_{\mathbf{Q}_\ell}}$ to be zero, then we get $\phi \in \mathcal{S}_{\Sigma'\cup\{\ell\}}(\mathbf{Q}, W_1^*)$ as desired. This will follow if we show that $\frac{H^1(\mathbf{Q}_\ell, W_1^*)}{H^1_{\mathrm{ur}}(\mathbf{Q}_\ell, W_1^*)} = 0$, i.e.,

that $H^1_{\Sigma'}(\mathbf{Q}, W_1^*) = H^1_{\Sigma'\cup\{\ell\}}(\mathbf{Q}, W_1^*)$. Clearly, all we need is $\#H^1_{\Sigma'\cup\{\ell\}}(\mathbf{Q}, W_1^*) \leq \#H^1_{\Sigma'}(\mathbf{Q}, W_1^*)$, which will follow from (6.5) applied to W_1^*, i.e., replacing $-n$ by $n+1$ as long as we can show that the corresponding value of m, which for W_1^* will be $\min\{\mathrm{val}_p(\ell^{-n}-1), 1\}$ is zero. This follows if we show $\mathrm{val}_p(\ell^n - 1) = 0$. Suppose that $\ell^n \equiv 1 \pmod{p}$. Then by our assumption that $\mathrm{val}_p(\ell^{n+1} - 1) > 0$ we get $1 \equiv \ell^{n+1} \equiv \ell \pmod{p}$ which contradicts the assumption that $\ell \not\equiv 1 \bmod p$. This completes the proof. □

For $H^1_\Sigma(\mathbf{Q}, \mathbf{F}(k-1))$ on the other hand it is in general not possible to relate to pieces of class groups, as $H^1_f(\mathbf{Q}_p, \mathbf{F}(k-1)) \neq H^1_{\mathrm{ur}}(\mathbf{Q}_p, \mathbf{F}(k-1))$ (but see [Rub00] Proposition 1.6.4(ii) for $k = 1$).

Proposition 6.4. *One has*

$$\mathrm{val}_p(\#H^1_\Sigma(\mathbf{Q}, \mathbf{F}(k-1))) \leq \mathrm{val}_p(\#H^1(\mathrm{Gal}(\mathbf{Q}_{\{p\}}/\mathbf{Q}), \mathbf{F}(k-1))) + [\mathbf{F} : \mathbf{F}_p] \sum_{\ell\in\Sigma-\{p\}} \min\{\mathrm{val}_p(1-\ell^{k-2}), 1\}. \tag{6.8}$$

Proof. Let us first assume that one has

$$\mathrm{val}_p(\#H^1_\Sigma(\mathbf{Q}, \mathbf{F}(k-1))) \leq \mathrm{val}_p(\#H^1_{\{p\}}(\mathbf{Q}, \mathbf{F}(k-1))) + [\mathbf{F} : \mathbf{F}_p] \sum_{\ell\in\Sigma-\{p\}} \min\{\mathrm{val}_p(1-\ell^{k-2}), 1\}. \tag{6.9}$$

The Selmer group $H^1_{\{p\}}(\mathbf{Q}, \mathbf{F}(k-1))$ is certainly no larger than the Selmer group where all the classes are unramified away from p and we impose no condition at p. This last Selmer group is isomorphic to $H^1(\mathrm{Gal}(\mathbf{Q}_{\{p\}}/\mathbf{Q}), \mathbf{F}(k-1))$. Here $\mathbf{Q}_{\{p\}}$ stands for the maximal algebraic extension of $\mathbf{Q}$ unramified away from p. This gives us the claim of the Proposition. Hence it remains to prove (6.9), but this follows by (a possibly repeated application of) Lemma 6.3 where we set $n = 1-k$ and note that $\mathrm{val}_p(\ell^{k-2} - 1) = \mathrm{val}_p(\ell^{2-k} - 1)$. □

We will use the following proposition with $r = k - 1$.

Proposition 6.5. *Suppose $r \in \mathbf{Z}$, $r > 1$ and that the ϵ^r-eigenspace of the p-part C of the class group of $\mathbf{Q}(\mu_p)$ is trivial. Then* $\dim_{\mathbf{F}} H^1(\mathrm{Gal}(\mathbf{Q}_{\{p\}}/\mathbf{Q}), \mathbf{F}(r)) \leq 1$.

Proof. Write G for $\mathrm{Gal}(\mathbf{Q}_{\{p\}}/\mathbf{Q})$. Using the inflation-restriction sequence we need to show that

$$\dim_{\mathbf{F}} \mathrm{Hom}_G((\ker \overline{\epsilon}^r)^{\mathrm{ab}}, \mathbf{F}(r)) \leq 1.$$

By Class Field Theory this reduces the problem to studying the units for the splitting field of $\chi_0 := \overline{\epsilon}^r$ as a $\mathrm{Gal}(\mathbf{Q}(\chi_0)/\mathbf{Q})$-module. A similar analysis has been carried in section 3 of [BK09] for imaginary quadratic fields. The current situation is simpler, so we will only sketch the argument here and refer the reader to [BK09] for details. Write M for the group of local (at p - note that p ramifies totally in $\mathbf{Q}(\chi_0)$) units of $\mathbf{Q}(\chi_0)$ and T for its torsion subgroup. Then M/T is a free $\mathbf{Z}_p$-module of rank $d := [\mathbf{Q}(\chi_0) : \mathbf{Q}]$. Since the $\overline{\epsilon}^r$-eigenspace of C is trivial, by Proposition 13.6 in [Was97] we see that any element of $\mathrm{Hom}_G((\ker \chi_0)^{\mathrm{ab}}, \mathbf{F}(r))$ gives rise to a G-equivariant homomorphism from M to $\mathbf{F}(r)$. As $T \cong \mu_p$ and so G acts on T by $\overline{\epsilon}$ we see that such a homomorphism will factor through M/T as $r \neq 1$. Using $M/T \cong 1 + \mathfrak{P}$, where $\mathfrak{P}$ is the prime of $\mathbf{Q}(\chi_0)$ lying over p, it is enough to decompose $\mathfrak{P}$ as a G-module. One easily sees that $\mathfrak{P} = \bigoplus_{i=0}^{p-2} \mathbf{F}(\overline{\epsilon}^i)$. □

7. Example

We end with an example, where the conditions of Theorem 5.11 are satisfied.

Let $p = 37$, $k = 32$, $\Sigma = \{31, 37\}$, and consider $\chi = \omega^{k-1}$ (i.e. $\psi = 1$). Since $p \nmid (1-31^{30})$ we have by Lemma 6.3 that $H^1_\Sigma(\mathbf{Q}, \chi) = H^1_{\{p\}}(\mathbf{Q}, \chi)$. By Propositions 6.4 and 6.5 we know that the latter is at most 1-dimensional since the relevant piece of the class group of $\mathbf{Q}(\mu_p)$ is trivial as $p \nmid B_6$ by Herbrand's theorem. Using MAGMA [BCP97] one confirms that there are cuspforms of weight 32 of level 1 congruent to Eisenstein series, so by Ribet's lattice construction we know that there exists a non-trivial crystalline extension $\begin{pmatrix} \chi & * \\ 0 & 1 \end{pmatrix}$, so $\dim_{\mathbf{F}} H^1_\Sigma(\mathbf{Q}, \chi) = 1$.

While our arguments below (together with Theorem 5.11) imply in particular that $\dim_{\mathbf{F}} H^1_\Sigma(\mathbf{Q}, \chi^{-1}) \geq 2$ (so the question of the number of modular extensions becomes relevant) we note that this also follows from Proposition 6.1 since $p \mid B_{32}$ (which by the Kummer congruences implies $p \mid B_{1,\omega^{31}}$) and $p \mid (1 - 31^{32})$.

Since $\eta(\mathbf{1}, 32) = B_{32}(1-31^{32})$ has $\mathrm{val}_{37} = 2$ Proposition 5.2 implies that $\#\mathbf{T}/J \geq \#\mathcal{O}/p^2$ for $\mathbf{T}$ the completion of the Hecke algebra acting on $S_{32}(\Gamma_0(31))$, as one can check using SAGE [The18] that there exists a character of conductor 31 satisfying (5.1) (so $m = 1$ in the statement of Proposition 5.2).

MAGMA calculations further show that $S_{32}(\Gamma_0(31))$ has 2 Galois conjugacy classes of newforms. One of these has a coefficient field of degree 37 over $\mathbf{Q}$. We were not able to calculate its integer ring, but we could check that 37 factors over this field as $\mathfrak{P}_1\mathfrak{P}_2\mathfrak{P}_3\mathfrak{P}_4\mathfrak{P}_5\mathfrak{P}_6$, where only $\mathfrak{P}_1$ and $\mathfrak{P}_2$ have inertia degree 1. Using MAGMA we calculated the absolute norm of $(a_n(f) - (1 + n^{31}))$ mod 37 for the newforms $f \in S_{32}(\Gamma_0(31))$ and $n = 2, 3, 5$. This gives zero for all 37 Galois conjugates, but not zero modulo 37^2. This means that all 37 conjugates in the first class are congruent to the Eisenstein series modulo a prime of inertia degree 1 (but not the square of this prime). They could alternate between the two primes of inertia degree 1, but for one of these (say $\mathfrak{P}_1$) there are at least 19 forms congruent to the Eisenstein series.

For $\mathcal{O}$ the completion of the coefficient field at $\mathfrak{P}_1$ we therefore have a surplus of Eisenstein congruences, since

$$1/e \sum m_\lambda > 18 > \mathrm{val}_{37}(\#\mathcal{O}/\eta(\mathbf{1}, 32)) = 2$$

(the valuation hasn't gone up in the extension from $\mathbf{Z}_p$ to $\mathcal{O}$ since the inertia degree and ramification index of the prime $\mathfrak{P}_1$ are 1).

It is not a priori clear that the representations associated to these cuspforms are not all isomorphic modulo p. But since the assumptions of Theorem 5.11 are satisfied, we can deduce the existence of more than $\dim_{\mathbf{F}} H^1_\Sigma(\mathbf{Q}, \chi^{-1})$ modular lines in $H^1_\Sigma(\mathbf{Q}, \chi^{-1})$ and we have also proved that the Eisenstein ideal is not principal.

References

BC09. J. Bellaïche and G. Chenevier, *p-adic families of Galois representations and higher rank Selmer groups*, Astérisque (2009), no. 324.

BCP97. W. Bosma, J. Cannon, and C. Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), no. 3-4, 235–265, Computational algebra and number theory (London, 1993).

BK90. S. Bloch and K. Kato, *L-functions and Tamagawa numbers of motives*, The Grothendieck Festschrift, Vol. I, Progr. Math., vol. 86, Birkhäuser Boston, Boston, MA, 1990, pp. 333–400.

BK09. T. Berger and K. Klosin, *A deformation problem for Galois representations over imaginary quadratic fields*, Journal de l'Institut de Math. de Jussieu **8** (2009), no. 4, 669–692.

BK13. ———, *On deformation rings of residually reducible Galois representations and $R = T$ theorems*, Math. Ann. **355** (2013), no. 2, 481–518.

BK15. ———, *On lifting and modularity of reducible residual Galois representations over imaginary quadratic fields*, Int. Math. Res. Not. IMRN (2015), no. 20, 10525–10562.

BKK14. T. Berger, K. Klosin, and K. Kramer, *On higher congruences between automorphic forms*, Math. Res. Lett. **21** (2014), no. 1, 71–82.

BM16. N. Billerey and R. Menares, *On the modularity of reducible* mod l *Galois representations*, Math. Res. Lett. **23** (2016), no. 1, 15–41.

BM18. ———, *Strong modularity of reducible Galois representations*, Trans. Amer. Math. Soc. **370** (2018), no. 2, 967–986.

Bre01. C. Breuil, *p-adic Hodge theory, deformations and local Langlands*, 2001, http://www.ihes.fr/ breuil/PUBLICATIONS/Barcelone.pdf.

CHT08. L. Clozel, M. Harris, and R. Taylor, *Automorphy for some l-adic lifts of automorphic mod l Galois representations*, Publ. Math. Inst. Hautes Études Sci. (2008), no. 108, 1–181, With Appendix A, summarizing unpublished work of Russ Mann, and Appendix B by Marie-France Vignéras.

DDT97. H. Darmon, F. Diamond, and R. Taylor, *Fermat's last theorem*, Elliptic curves, modular forms & Fermat's last theorem (Hong Kong, 1993), Internat. Press, Cambridge, MA, 1997, pp. 2–140.

DF14. N. Dummigan and D. Fretwell, *Ramanujan-style congruences of local origin*, J. Number Theory **143** (2014), 248–261.

Eis95. D. Eisenbud, *Commutative algebra with a view toward algebraic geometry*, Graduate Texts in Mathematics, vol. 150, Springer-Verlag, New York, 1995.

HR08. S. Hamblen and R. Ramakrishna, *Deformations of certain reducible Galois representations. II*, Amer. J. Math. **130** (2008), no. 4, 913–944.

Klo09. K. Klosin, *Congruences among automorphic forms on* $\mathrm{U}(2,2)$ *and the Bloch-Kato conjecture*, Annales de l'institut Fourier **59** (2009), no. 1, 81–166.

Maz77. B. Mazur, *Modular curves and the Eisenstein ideal*, Inst. Hautes Études Sci. Publ. Math. (1977), no. 47, 33–186 (1978).

Miy89. T. Miyake, *Modular forms*, Springer-Verlag, Berlin, 1989, Translated from the Japanese by Yoshitaka Maeda.

MW84. B. Mazur and A. Wiles, *Class fields of abelian extensions of* $\mathbf{Q}$, Invent. Math. **76** (1984), no. 2, 179–330.

Och00. T. Ochiai, *Control theorem for Bloch-Kato's Selmer groups of p-adic representations*, J. Number Theory **82** (2000), no. 1, 69–90.

Oht14. M. Ohta, *Eisenstein ideals and the rational torsion subgroups of modular Jacobian varieties II*, Tokyo J. Math. **37** (2014), no. 2, 273–318.

Oza17. T. Ozawa, *Constant terms of Eisenstein series over a totally real field*, Int. J. Number Theory **13** (2017), no. 2, 309–324.

Rub00. K. Rubin, *Euler systems*, Annals of Mathematics Studies, vol. 147, Princeton University Press, Princeton, NJ, 2000, Hermann Weyl Lectures. The Institute for Advanced Study.

Ski06. C. M. Skinner, *Main conjectures and modular forms*, Current developments in mathematics, 2004, Int. Press, Somerville, MA, 2006, pp. 141–161.

Spe18. D. Spencer, *Congruences of local origin for higher levels*, Ph.D. thesis, University of Sheffield, 2018.

Sun10. Hae-Sang Sun, *Cuspidal class number of the tower of modular curves* $X_1(Np^n)$, Math. Ann. **348** (2010), no. 4, 909–927.

SW97. C. M. Skinner and A. J. Wiles, *Ordinary representations and modular forms*, Proc. Nat. Acad. Sci. U.S.A. **94** (1997), no. 20, 10520–10527.

SW99. ———, *Residually reducible representations and modular forms*, Inst. Hautes Études Sci. Publ. Math. (1999), no. 89, 5–126 (2000).

The18. The Sage Developers, *Sagemath, the Sage Mathematics Software System (Version 8.3)*, 2018, `http://www.sagemath.org`.

Urb01. E. Urban, *Selmer groups and the Eisenstein-Klingen ideal*, Duke Math. J. **106** (2001), no. 3, 485–525.

Was97. L. C. Washington, *Introduction to cyclotomic fields*, second ed., Graduate Texts in Mathematics, vol. 83, Springer-Verlag, New York, 1997.

WWE18. P. Wake and C. Wang-Erickson, *The Eistenstein ideal with squarefree level*, Preprint (2018), arXiv: 1804.06400.

Yoo16. H. Yoo, *The index of an Eisenstein ideal and multiplicity one*, Math. Z. **282** (2016), no. 3-4, 1097–1116.