A modular construction of unramified p-extensions of Q(N1/P)

Jaclyn Lang, Preston Wake

PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY, SERIES B
Volume 9, Pages 415–431 (October 31, 2022)
https://doi.org/10.1090/bproc/141

A MODULAR CONSTRUCTION OF UNRAMIFIED p-EXTENSIONS OF $\mathbb{Q}(N^{1/p})$

JACLYN LANG AND PRESTON WAKE

(Communicated by Romyar T. Sharifi)

Abstract. We show that for primes $N, p \geq 5$ with $N \equiv -1 \bmod p$, the class number of $\mathbb{Q}(N^{1/p})$ is divisible by p. Our methods are via congruences between Eisenstein series and cusp forms. In particular, we show that when $N \equiv -1 \bmod p$, there is always a cusp form of weight 2 and level $\Gamma_0(N^2)$ whose ℓth Fourier coefficient is congruent to $\ell + 1$ modulo a prime above p, for all primes ℓ. We use the Galois representation of such a cusp form to explicitly construct an unramified degree-p extension of $\mathbb{Q}(N^{1/p})$.

1. Introduction

Throughout this paper, N and p denote prime numbers such that $p \geq 5$.

1.1. Main results.

We give a proof of the following theorem via congruences between Eisenstein series and cuspidal modular forms.

Theorem A. *If $N \equiv -1 \bmod p$ then p divides the class number of $\mathbb{Q}(N^{1/p})$.*

This was first proven by Iimura [Iim86, Corollary to Theorem 2.3][1]. An alternate proof of Theorem A using Galois cohomology was sketched by Calegari on his blog [Cal17]. Calegari asks whether there is a direct proof of Theorem A and whether there is "an easy way to construct the relevant unramified extension of degree p". The purpose of this paper is to do exactly that.

We give an explicit construction of the corresponding unramified extension of degree p of $\mathbb{Q}(N^{1/p})$ using the Galois representation of a modular form. Explicitly, we prove the following.

Received by the editors January 21, 2022, and, in revised form, September 7, 2022.
2020 *Mathematics Subject Classification.* Primary 11F33, 11F80, 11R29, 11R37.
Key words and phrases. Eisenstein ideal, class group, Galois representation.
The second author was supported by the NSF grant DMS-1901867.

[1] We were unaware of the work of Iimura when writing an earlier draft of this article. Theorem A was conjectured by Kobayashi [Kob16, Conjecture 1], to whom the result of Iimura was apparently also unknown.

Theorem B. *Assume that $N \equiv -1 \bmod p$.*

(a) *There is a newform f of weight 2 and level $\Gamma_0(N^2)$ and a prime ideal $\mathfrak{p}$ over p in the ring of integers $\mathcal{O}_f$ of the Hecke field of f such that for all primes ℓ,*

$$a_\ell(f) \equiv 1 + \ell \bmod \mathfrak{p}. \tag{1}$$

(b) *Moreover, if s is the largest integer such that $a_\ell(f) \equiv 1 + \ell \bmod \mathfrak{p}^s$ for all primes $\ell \neq N$ and $t_f : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathcal{O}_{f,\mathfrak{p}}$ denotes the trace of the Galois representation of f, then*

$$t_f | G_{\mathbb{Q}(N^{1/p})} \equiv \chi\epsilon + \chi^{-1} \bmod \mathfrak{p}^{s+1}, \tag{2}$$

where $\chi : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}(N^{1/p})) \to (\mathcal{O}_{f,\mathfrak{p}}/\mathfrak{p}^{s+1})^\times$ is a nontrivial everywhere unramified character with $\chi \equiv 1 \bmod \mathfrak{p}^s$ and ϵ is the p-adic cyclotomic character.

Note that Theorem B implies Theorem A by class field theory, because χ cuts out a degree-p unramified extension of $\mathbb{Q}(N^{1/p})$. Theorem B may be thought of as an explicit version of Theorem A because the Fourier coefficients of the newform f can often be efficiently computed. Extra information about the class field of $\mathbb{Q}(N^{1/p})$ can be read off from this data, as we illustrate in Section 3.2.

The values $1 + \ell$ on the right hand side of (1) are the Hecke eigenvalues of an Eisenstein series, so we say that a form f satisfying (1) for all primes $\ell \neq N$ is *congruent to an Eisenstein series*, and say (1) is an *Eisenstein congruence*, modulo p.

The idea of using Eisenstein congruences to construct unramified extensions goes back to the seminal work of Ribet [Rib76] in which he used this idea to prove the converse to Herbrand's theorem. Variants of Ribet's method have been used to great effect to construct interesting cohomology classes (see, for instance, [MW84] or [DDP11]). In our situation, the cohomology class produced from Ribet's method is something we already know: it is the Kummer class cutting out the extension $\mathbb{Q}(N^{1/p})/\mathbb{Q}$. The novel idea here is that when we restrict our Galois representation to the Galois group of the splitting field of this cohomology class, then the representation becomes *extra* reducible, as expressed in (2). For an application of extra reducibility in another context, see [Wak22].

Remark 1.1. For level $\Gamma_0(M)$ with M prime, Mazur [Maz77, Proposition II.9.7, pg. 96] gave a necessary and sufficient condition for an Eisenstein congruence to exist. For squarefree M, partial necessary and sufficient conditions have been found by Ribet [Rib10] (see also [Yoo19a]) using geometry of modular Jacobians, and by the second author and Wang-Erickson [WWE21] using Galois deformation theory. For some nonsquarefree M, sufficient conditions have been proven by Martin [Mar17] using Jacquet–Langlands theory and necessary conditions by Yoo [Yoo19b] using geometry of modular Jacobians. However, both those works do not consider the case where M is the square of a prime. The case where M is the square of a prime has been considered by Gross–Lubin [GL86] and Calegari [Cal06], but only when $p \mid M$. △

1.2. **The $N \equiv 1 \bmod p$ case.** To understand the context for Theorems A and B, we recall what is known in the case when $N \equiv 1 \bmod p$ — a congruence condition we impose throughout Section 1.2. In this case, it is easy to see that $\mathrm{Cl}(\mathbb{Q}(N^{1/p}))[p]$

— the p-torsion in the class group of $\mathbb{Q}(N^{1/p})$ — is nontrivial: there is a degree-p subextension $\mathbb{Q}(\zeta_N^{(p)})$ of $\mathbb{Q}(\zeta_N)/\mathbb{Q}$ and $\mathbb{Q}(\zeta_N^{(p)}, N^{1/p})/\mathbb{Q}(N^{1/p})$ is unramified. Letting

$$r_{\mathrm{Cl}} = \dim_{\mathbb{F}_p} \mathrm{Cl}(\mathbb{Q}(N^{1/p}))[p]$$

we can see $r_{\mathrm{Cl}} \geq 1$, but the exact value of r_{Cl} is interesting. In particular, it is interesting to ask when $r_{\mathrm{Cl}} > 1$, or, in other words, when there is an unramified p-extension of $\mathbb{Q}(N^{1/p})$ that is not explained by genus theory.

On the modular forms side, Mazur [Maz77, Proposition II.9.7] proved that there is a cusp form f of weight 2 and level $\Gamma_0(N)$ that is congruent to the Eisenstein series modulo p if and only if $N \equiv 1 \pmod{p}$. Letting $S_2(\Gamma_0(N); \mathbb{Z}_p)_{\mathrm{Eis}}$ denote the completion of the space of cusp forms at the Eisenstein maximal ideal, and letting

$$r_{\mathrm{Eis}} = \mathrm{rank}_{\mathbb{Z}_p} S_2(\Gamma_0(N); \mathbb{Z}_p)_{\mathrm{Eis}},$$

Mazur's result implies $r_{\mathrm{Eis}} \geq 1$, but he also asked about the significance of r_{Eis} in general [Maz77, Section II.19, page 140].

The first result about r_{Eis} was obtained by Mazur [Maz77, Proposition II.19.2, pg. 140], who showed that $r_{\mathrm{Eis}} = 1$ if and only if the Weil pairing on $J_0(N)$ has a certain property. Merel used modular symbols and Mazur's result to prove a remarkable numerical criterion for r_{Eis} to equal 1 [Mer96, Théorème 2]. Recently, Lecouturier has greatly generalized Merel's techniques to relate the value of r_{Eis} to "higher Merel invariants".

Calegari and Emerton [CE05] were the first to find a relationship between r_{Eis} and r_{Cl}. They proved

$$r_{\mathrm{Cl}} = 1 \Longrightarrow r_{\mathrm{Eis}} = 1 \tag{3}$$

using Galois deformation theory and explicit class field theory. Later, Lecouturier [Lec18] used Merel's result to give a new proof of (3) by purely algebraic-number-theoretic methods.

The second author and Wang-Erickson refined Calegari and Emerton's method to precisely determine the value of r_{Eis} in terms of vanishing of a certain cup product (or, more generally, Massey product) in Galois cohomology [WWE20]. In particular, they show that $r_{\mathrm{Eis}} > 1$ if and only if a certain cup product vanishes [WWE20, Theorem 1.2.1]. They also show that the vanishing of this cup product implies $r_{\mathrm{Cl}} > 1$, hence giving a new proof of (3). Schaefer and Stubley [SS19] built upon this cup product technique and the results of [Lec18] to prove more precise bounds on r_{Cl}.

1.3. **Comparing $N \equiv 1 \bmod p$ and $N \equiv -1 \bmod p$.** When $N \equiv -1 \pmod{p}$, in contrast to the previous section, the genus field of $\mathbb{Q}(N^{1/p})$ is trivial. Hence Theorem A is analogous to "$r_{\mathrm{Cl}} > 1$" in Section 1.2.

When $N \equiv -1 \pmod{p}$, then Mazur's results imply that $S_2(\Gamma_0(N); \mathbb{Z}_p)_{\mathrm{Eis}}$ is trivial. Instead, we study $S_2(\Gamma_0(N^2); \mathbb{Z}_p[\zeta_N])_{\mathrm{Eis}}$ and Theorem B implies that this is nontrivial. We think of this as being analogous to "$r_{\mathrm{Eis}} > 1$" of the previous section.

The surprising thing is that, although "$r_{\mathrm{Cl}} > 1$" and "$r_{\mathrm{Eis}} > 1$" do not always hold for $N \equiv 1 \bmod p$, their analogs for $N \equiv -1 \pmod{p}$ *do* always hold. Just as "$r_{\mathrm{Cl}} > 1$" and "$r_{\mathrm{Eis}} > 1$" are related to the vanishing of a cup product, their analogs for $N \equiv -1 \bmod p$ are also related to the vanishing of a cup product. The difference is that, when $N \equiv -1 \bmod p$, the relevant cup product *always vanishes* because

the codomain H^2 group vanishes. Indeed, this is the observation that Calegari made after attending a lecture by the second author about the work of [WWE20] explaining the relation between cup products and the class group of $\mathbb{Q}(N^{1/p})$ that allowed him to give a Galois cohomology proof of Theorem A using the methods of [WWE20].

1.4. **Eisenstein congruences in the case $N \equiv -1 \bmod p$.** The purpose of this paper is to show that, just as in [WWE20], the abstract Galois cochain used in [Cal17] actually appears in the Galois representation associated to a newform. The newform we need has to be congruent to an Eisenstein series, but Mazur's theorem implies that there is no such newform of level $\Gamma_0(N)$ when $N \equiv -1 \bmod p$. Our motivation came from considering the obstruction, from the point of view of Galois deformation theory, to producing the relevant Galois representation. The observation we made is that there is no obstruction to producing such a representation that is unramified outside N and p; the only obstruction comes from making it be Steinberg at N. Consequently, if we relax the local condition at N by considering forms of level $\Gamma_0(N^2)$, we expect to find a newform that is congruent to the Eisenstein series. Although these deformation-theoretic considerations led us to conjecture that Theorem B should be true, the proof does not use deformation theory; it is a direct computation using Eisenstein series.

Remark 1.2. In fact, Iimura's result [Iim86, Corollary to Theorem 2.3] implies that for any p-power-free positive integer m, the p-rank of the class group of $\mathbb{Q}(m^{1/p})$ is bounded below by the number of distinct prime divisors of m that are congruent to ± 1 modulo p. Calegari explains how to use cup products to prove a result in this direction as well [Cal17]. We believe a modular approach is also possible by combining the methods of the current paper with those of the second author and Wang-Erickson in [WWE21], but we have elected not to do so in this paper for simplicity. △

1.5. **Layout.** In Section 2 we establish the Eisenstein congruence promised in Theorem B(a). There are no Galois representations in this section; the main calculation is to compute the constant terms at the cusps of an Eisenstein series. We then derive the consequences of this congruence for Galois representations and the class group of $\mathbb{Q}(N^{1/p})$ in Section 3, thus proving Theorem B(b) and hence Theorem A. We end by showing, in Section 3.2, how explicit information about the Fourier coefficients of the modular form found in Theorem B gives explicit information about the primes that split in the class field of $\mathbb{Q}(N^{1/p})$, thus demonstrating the advantages of a modular proof of Theorem A.

Notation. For a positive integer n, let ζ_n denote a primitive nth root of unity. When S is a subset of $M_2(\mathbb{R})$, we write S^+ for the subset of S with positive determinant. For a field F of characteristic 0, fix an algebraic closure $\overline{F}$. Write $G_F \coloneqq \mathrm{Gal}(\overline{F}/F)$, which we may implicitly view as a subgroup of $G_{\mathbb{Q}}$ when F is a number field. Let $G_{\mathbb{Q},Np}$ denote the Galois group of the maximal extension of $\mathbb{Q}$ that is unramified outside Np. We fix an embedding $\overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_p$ and let I_p denote the corresponding inertia subgroup of $G_{\mathbb{Q}}$. Let $\varepsilon : G_{\mathbb{Q}} \to \mathbb{Z}_p^\times$ be the p-adic cyclotomic character and ω its mod p reduction. We write $\overline{\mathbb{Z}}_p$ for the elements in $\overline{\mathbb{Q}}_p$ that are integral over $\mathbb{Z}_p$. If X is a scheme, then $\mathcal{O}_X$ denotes its structure sheaf.

2. Eisenstein series and residues

In this section we prove Theorem B(a). To do this, we need to consider an Eisenstein series of weight 2 and level $\Gamma_0(N^2)$ with T_ℓ-eigenvalue $1+\ell$ for all primes $\ell \neq N$. There is a 2-dimensional space of such Eisenstein series; we consider U_N-eigenvalues to narrow the search. Since Mazur's result [Maz77, Proposition II.9.7, pg. 96] implies that any cusp form f satisfying (1) cannot come from level $\Gamma_0(N)$ (that is, f must be new of level $\Gamma_0(N^2)$), we know that f, if it exists, must have U_N-eigenvalue 0. Hence we only consider Eisenstein series with U_N-eigenvalue 0, and this gives us a unique normalized form we call E.

Now we continue by a standard argument. We show that the residue of E at each cusp of $X_0(N^2)$ is divisible by p. This residue calculation is done by computing the Hecke action on the cusps, which suffices since E is an eigenform and the residue map is Hecke equivariant. We show that the part of the module of degree-0 divisors supported on the cusps with the same Hecke eigenvalues as E is generated by the residue of another modular form F. Thus the residue of E must be a constant c times the residue of F, and we show c is divisible by p by computing the residue of E at the zero cusp. Hence $E - cF$ is a cusp form that is congruent to E modulo p, which implies that the maximal ideal of the Hecke algebra generated by p and the annihilator of E is contained in the support of the cuspidal Hecke algebra. Since the cuspidal Hecke algebra is finite-flat over $\mathbb{Z}_p$, this implies that it has a height one prime ideal contained in this maximal ideal, and this height one prime corresponds to the cuspidal eigenform f required in Theorem B(a).

2.1. **The modular curve $X_0(N^2)$ and its cusps.** Recall that N and p always denote distinct primes, and $p \geq 5$. Define

$$\Gamma \coloneqq \Gamma_0(N^2) \coloneqq \left\{ \left(\begin{smallmatrix} a & b \\ N^2 c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z}) \colon c \in \mathbb{Z} \right\},$$

which acts on the upper half complex plane $\mathfrak{h}$ by Möbius transformations. The open Riemann surface $\Gamma\backslash\mathfrak{h}$ can be compactified to $\Gamma\backslash\mathfrak{h}^*$ by adding the cusps $\Gamma\backslash\mathbb{P}^1(\mathbb{Q})$. The complex curves $\Gamma\backslash\mathfrak{h} \subset \Gamma\backslash\mathfrak{h}^*$ descend to $\mathbb{Q}$ and admit a smooth model over $\mathbb{Z}[1/N]$. Let $Y \coloneqq Y_0(N^2) \subset X \coloneqq X_0(N^2)$ denote the base change of these smooth models to $\mathbb{Z}_p[\zeta_N]$.

Let $C \coloneqq X \setminus Y$ denote the scheme of cusps on X. A standard calculation shows that there are $N+1$ geometric points of C [DS05, §3.8], all defined over $\mathbb{Z}_p[\zeta_N]$ [DR73, §VI.5], represented by the following elements in $\mathbb{P}^1(\mathbb{Q}) = \mathbb{Q} \cup \{\infty\}$:

$$\infty, 0, 1/N, 2/N, \ldots, (N-1)/N. \tag{4}$$

We sometimes conflate C with its set of geometric points. It will be convenient to consider $(\mathbb{Z}/N\mathbb{Z})^\times$ as the indexing set for the set $C \setminus \{\infty, 0\}$. For $x \in (\mathbb{Z}/N\mathbb{Z})^\times$, we define $[x] \in C$ to be the class of $\tilde{x}/N \in \mathbb{P}^1(\mathbb{Q})$, where $1 \leq \tilde{x} \leq N-1$ such that $\tilde{x} \equiv x \bmod N$. Similarly, write $[0]$ for the cusp 0 to avoid confusion. We write $\mathrm{Div}(C; \mathbb{Z}_p[\zeta_N])$ for the divisor group supported on the cusps and $\mathrm{Div}^0(C; \mathbb{Z}_p[\zeta_N])$ for the degree-0 part.

2.2. **Modular forms and the residue sequence.** Let $\Omega = \Omega^1_X$ be the invertible sheaf of 1-forms on X over $\mathbb{Z}_p[\zeta_N]$. Viewing C as a divisor on X we have the sheaf $\Omega(C) = \Omega \otimes \mathcal{O}_X(C)$ of 1-forms on X where we allow simple poles at C. Define the space of modular forms (respectively, cusp forms) of weight 2 and level Γ with coefficients in $\mathbb{Z}_p[\zeta_N]$ by $M_2(\Gamma; \mathbb{Z}_p[\zeta_N]) \coloneqq H^0(X, \Omega(C))$ (respectively,

$S_2(\Gamma;\mathbb{Z}_p[\zeta_N]) \coloneqq H^0(X,\Omega)$). Note that this definition is compatible with the usual definition. That is, fixing an isomorphism $\overline{\mathbb{Q}}_p \cong \mathbb{C}$, we can identify $M_2(\Gamma;\mathbb{Z}_p[\zeta_N])$ with the subspace of $M_2(\Gamma;\mathbb{C})$ whose q-expansions have $\mathbb{Z}_p[\zeta_N]$-coefficients since $p \nmid N^2$ [Maz77, Lemma II.4.5].

Proposition 2.1. *There is an exact sequence*

$$0 \to S_2(\Gamma;\mathbb{Z}_p[\zeta_N]) \to M_2(\Gamma;\mathbb{Z}_p[\zeta_N]) \xrightarrow{\mathrm{Res}} \mathrm{Div}(C;\mathbb{Z}_p[\zeta_N]) \xrightarrow{\Sigma} \mathbb{Z}_p[\zeta_N] \to 0, \tag{5}$$

where Res *sends a modular form to the formal sum of its residues at the cusps, and* Σ *is the sum map.*

Proof. This is certainly well known, though we could only find a convenient reference when the coefficients are a field, namely [Oht99, Lemma 3.1.13(ii)]. The proof comes from the long exact sequence in cohomology associated to the exact sequence of sheaves coming from the inclusions $\iota_c : c \to X$ for $c \in C$, namely

$$0 \to H^0(X,\Omega) \to H^0(X,\Omega(C)) \to \bigoplus_{c\in C} H^0(X,\Omega(C)\otimes \iota_{c*}(\mathbb{Z}_p[\zeta_N])) \to H^1(X,\Omega). \tag{6}$$

The main thing that needs to be checked is that $H^1(X,\Omega) = \mathbb{Z}_p[\zeta_N]$, which follows from the fact that X is a smooth curve over $\mathbb{Z}_p[\zeta_N]$. □

We briefly recall the formula for the residue map Res in terms of constant terms of q-expansions of modular forms; see [Oht99, §4.5] for more details. Given $c \in C(\mathbb{Z}_p[\zeta_N])$, its width is a positive integer h_c such that, up to sign, the stabilizer of c in Γ can be conjugated to

$$\left\langle \begin{pmatrix} 1 & h_c \\ 0 & 1 \end{pmatrix} \right\rangle.$$

In our case, ∞ has width 1, [0] has width N^2, and all the other cusps of X have width N. The Fourier expansion of $f \in M_2(\Gamma;\mathbb{Z}_p[\zeta_N])$ at c is of the form

$$f = \sum_{n=0}^{\infty} a_n^c(f) q^{n/h_c},$$

and

$$\mathrm{Res}(f) = \sum_{c\in C(\mathbb{Z}_p[\zeta_N])} h_c a_0^c(f) c.$$

That is, writing $\mathrm{Res}_c(f)$ for the coefficient of c in $\mathrm{Res}(f)$, we have $\mathrm{Res}_c(f) = h_c a_0^c(f)$. Note that for the cusp [0], the Atkin-Lehner involution w_{N^2} incorporates the width of [0], and hence $\mathrm{Res}_{[0]}(f) = a_0^\infty(w_{N^2} f)$.

2.3. **Hecke operators.** The Hecke operators T_ℓ for primes $\ell \nmid N$ and U_N act on $M_2(\Gamma;\mathbb{Z}_p[\zeta_N])$ and this action preserves $S_2(\Gamma;\mathbb{Z}_p[\zeta_N])$. By sequence (5), this gives an induced action on $\mathrm{Div}^0(C;\mathbb{Z}_p[\zeta_N])$. In fact, this action extends to $\mathrm{Div}(C;\mathbb{Z}_p[\zeta_N])$ in a way that makes (5) Hecke-equivariant, as Proposition 2.2 makes explicit. While the proof is quite standard, we include a sketch to warn the reader that the U_N-action is *not* the "standard" one, but rather the adjoint action.

Proposition 2.2. *Define an action of the Hecke operators* T_ℓ *with* $\ell \nmid N$ *and* U_N *on* $\mathrm{Div}(C;\mathbb{Z}_p[\zeta_N])$ *as follows:*

(1) *For a prime $\ell \neq N$ and $c \in C$ let*

$$T_\ell c = \begin{cases} (\ell+1)c & \text{if } c = 0, \infty \\ \ell[\ell x] + [\ell^{-1}x] & \text{if } c = [x] \text{ for } x \in (\mathbb{Z}/N\mathbb{Z})^\times. \end{cases}$$

(2) *For $c \in C$ let*

$$U_N c = \begin{cases} N \cdot [0] & c \neq \infty \\ \infty + \sum_{x \in (\mathbb{Z}/N\mathbb{Z})^\times} [x] & c = \infty. \end{cases}$$

Then sequence (5) *is Hecke-equivariant.*

Proof. Note that, to prove the proposition, it suffices to work with $\mathbb{Q}_p$-coefficients (or even $\mathbb{C}$-coefficients), so this is entirely classical. To explain why the adjoint of the "standard" action appears, we must fix our conventions for Hecke operators.

For any $\alpha \in \mathrm{GL}_2(\mathbb{Q})^+$, let $\Gamma_\alpha = \Gamma \cap \alpha^{-1}\Gamma\alpha$. Then we have two maps $\Gamma_\alpha\backslash\mathfrak{h}^* \to \Gamma\backslash\mathfrak{h}^*$:

$$\varphi_\alpha \colon \Gamma_\alpha z \mapsto \Gamma z \text{ and } \psi_\alpha \colon \Gamma_\alpha z \mapsto \Gamma\alpha z.$$

Define $O_\alpha \coloneqq \psi_{\alpha *}\varphi_\alpha^*$ as an operator on all of the cohomology groups in (6) (base-changed to $\mathbb{C}$). For any prime ℓ, let $\alpha_\ell \coloneqq \left(\begin{smallmatrix} 1 & 0 \\ 0 & \ell \end{smallmatrix}\right)$, and let $T_\ell \coloneqq O_{\alpha_\ell}$ and define $U_N \coloneqq T_N$. With this definition, it is clear that (5) is Hecke-equivariant. To prove the proposition, it remains to see what this action is on $\mathrm{Div}(C)$.

We now consider the standard action of Hecke operators on $\mathrm{Div}(C)$. We have the identifications

$$C = \Gamma\backslash\mathbb{P}^1(\mathbb{Q}) \xrightarrow{\sim} \Gamma\backslash \mathrm{SL}_2(\mathbb{Z})/B(\mathbb{Z}) \xrightarrow{\sim} \Gamma\backslash \mathrm{GL}_2(\mathbb{Q})^+/B(\mathbb{Q})^+,$$

where $B \subset \mathrm{SL}_2$ is the upper-triangular Borel. The inverse of the first map is given by sending the class of $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ to $[a\colon c] \in \mathbb{P}^1(\mathbb{Q})$, and the second map is induced by the natural inclusion $\mathrm{SL}_2(\mathbb{Z}) \hookrightarrow \mathrm{GL}_2(\mathbb{Q})^+$. For an element $\gamma \in \mathrm{GL}_2(\mathbb{Q})^+$, let $[\gamma] \in C$ denote its class. For $\alpha \in \mathrm{GL}_2(\mathbb{Q})^+$, the standard action of O_α on C is given by $O_\alpha([\gamma]) = \sum_i [\alpha^{(i)}\gamma]$, where $\Gamma\alpha\Gamma = \coprod_i \Gamma\alpha^{(i)}$.

The key observation, which we learned from [Oht99, Proposition 3.4.12], is that the identification of $\oplus_{c\in C} H^0(X_\mathbb{C}, \Omega(C)_\mathbb{C} \otimes \iota_{c*,\mathbb{C}}(\mathbb{C}))$ with $\mathrm{Div}(C)$ swaps standard Hecke operators with their adjoints. (Intuitively, this is because

$$\oplus_{c\in C} H^0(X_\mathbb{C}, \Omega(C)_\mathbb{C} \otimes \iota_{c*,\mathbb{C}}(\mathbb{C}))$$

is the Serre-dual of $H^0(C, \mathcal{O}_C)$.) Equivalently, to make (5) Hecke-equivariant, T_ℓ has to act on $\mathrm{Div}(C)$ via the standard action of O_{β_ℓ}, where $\beta_\ell = \left(\begin{smallmatrix} \ell & 0 \\ 0 & 1 \end{smallmatrix}\right)$.

Given this, the proposition follows from the following two lemmas, whose simple proofs we omit.

Lemma 2.3. *For a prime ℓ, let $\beta_\ell = \left(\begin{smallmatrix} \ell & 0 \\ 0 & 1 \end{smallmatrix}\right)$.*

(1) *Let $\ell \neq N$ be a prime. A set of representatives for $\Gamma\backslash\Gamma\beta_\ell\Gamma$ is given by β_ℓ together with any ℓ matrices of the form*

$$\beta_\ell \left(\begin{smallmatrix} a & b \\ N^2 & d \end{smallmatrix}\right)$$

where $ad - bN^2 = 1$ and d ranges over a set of representatives of $\mathbb{Z}/\ell\mathbb{Z}$.

(2) *A set of representatives for $\Gamma\backslash\Gamma\beta_N\Gamma$ is given by the N matrices*

$$\beta_N \left(\begin{smallmatrix} 1 & 0 \\ iN^2 & 1 \end{smallmatrix}\right)$$

for $i = 0, \ldots, N-1$.

Lemma 2.4. *For an element $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{Q})^+$, we can determine its class in C as follows. If $c = 0$ then the class of γ is ∞. If $c \neq 0$, write $\frac{a}{c} = \frac{x}{y}$ with $x, y \in \mathbb{Z}$ coprime.*

- *If $N^2 \mid y$, then the class of γ is ∞;*
- *if $N \nmid y$, then the class of γ is $[0]$;*
- *if $y = uN$ with $N \nmid u$, then the class of γ is $[ux \bmod N]$.* □

2.4. **Eisenstein series.** To prove Theorem B(a), we consider congruences between elements of $S_2(\Gamma; \mathbb{Z}_p[\zeta_N])$ and an Eisenstein series with T_ℓ-eigenvalue $\ell + 1$ for all primes $\ell \neq N$. There are two such Eisenstein series in $M_2(\Gamma; \mathbb{Z}_p[\zeta_N])$, both old forms. We write them explicitly.

Define

$$E_2(z) \coloneqq \frac{-1}{24} + \sum_{n \geq 1} \sigma(n) q^n,$$

where $\sigma(n) \coloneqq \sum_{0<d|n} d$. It is nearly holomorphic of weight 2 and level 1. Then

$$E_{2,N}(z) \coloneqq E_2(z) - N E_2(Nz)$$

defines the unique Eisenstein series of weight 2 and level $\Gamma_0(N)$; its T_ℓ-eigenvalue is $\ell + 1$ for all primes $\ell \neq N$ and its U_N-eigenvalue is 1. The constant term of $E_{2,N}$ is $\frac{N-1}{24}$. Let

$$E(z) \coloneqq N E_{2,N}(z) - N E_{2,N}(Nz) \in M_2(\Gamma; \mathbb{Z}_p[\zeta_N]),$$

which has T_ℓ-eigenvalue $\ell + 1$ for all primes $\ell \neq N$ and U_N-eigenvalue 0. The constant term of its q-expansion at ∞ is 0.

To understand congruences between these Eisenstein series and elements in $S_2(\Gamma; \mathbb{Z}_p[\zeta_N])$, we need to calculate the constant terms of their q-expansions at all cusps, not only ∞. To do this, we make use of the Hecke action on the residue sequence (5).

Let $\mathbb{T}$ be the $\mathbb{Z}_p[\zeta_N]$-subalgebra of $\mathrm{End}_{\mathbb{Z}_p[\zeta_N]}(M_2(\Gamma; \mathbb{Z}_p[\zeta_N]))$ generated by T_ℓ for $\ell \nmid N$ and U_N, and let $\mathbb{T}' \subset \mathbb{T}$ be the subalgebra generated just by the T_ℓ. We consider $\mathrm{Div}^0(C; \mathbb{Z}_p[\zeta_N])$ as a $\mathbb{T}$-module via the action described in Proposition 2.2, so there is an exact sequence of $\mathbb{T}$-modules

$$0 \to S_2(\Gamma; \mathbb{Z}_p[\zeta_N]) \to M_2(\Gamma; \mathbb{Z}_p[\zeta_N]) \xrightarrow{\mathrm{Res}} \mathrm{Div}^0(C; \mathbb{Z}_p[\zeta_N]) \to 0. \tag{7}$$

Let I be the ideal of $\mathbb{T}'$ generated by the elements $T_\ell - \ell - 1$ for $\ell \neq N$ prime and $\mathfrak{m}' = (I, p) \subset \mathbb{T}'$, which is maximal. Write

$$\mathfrak{c} \coloneqq \sum_{x \in (\mathbb{Z}/N\mathbb{Z})^\times} ([x] - [0]) \in \mathrm{Div}^0(C; \mathbb{Z}_p[\zeta_N]).$$

Proposition 2.5. *When $N \not\equiv 1 \bmod p$, the localization $\mathrm{Div}^0(C; \mathbb{Z}_p[\zeta_N])_{\mathfrak{m}'}$ is a free $\mathbb{Z}_p[\zeta_N]$-module of rank 2 with basis*

$$\{\infty - [0] + \mathfrak{c}, \mathfrak{c}\}$$

that is annihilated by I. Moreover, U_N acts by $U_N(\infty - [0] + \mathfrak{c}) = \infty - [0] + \mathfrak{c}$ and $U_N \mathfrak{c} = 0$.

Proof. Set $W = \mathbb{Z}_p[\zeta_N]$. Let P be the W-span of $\infty - [0] + \mathfrak{c}$ and $\mathfrak{c}$ in $\mathrm{Div}^0(C; W)$. The facts that P is annihilated by I and U_N acts as described follow from Proposition 2.2. Since $N \not\equiv 1 \bmod p$, the same lemma shows that the section $s : \mathrm{Div}^0(C; W) \to P$ that is the identity on $\infty - [0]$ and sends $[x] - [0]$ to $\frac{1}{N-1}\mathfrak{c}$

for $x \in (\mathbb{Z}/N\mathbb{Z})^\times$ is $\mathbb{T}'$-equivariant. Letting $Q = \ker s$, we have a $\mathbb{T}'$-equivariant splitting $\mathrm{Div}^0(C; W) = P \oplus Q$.

To complete the proof, it is enough to show that $\mathrm{Div}^0(C; W/p)[\mathfrak{m}'] = P \otimes W/p$. Indeed, this implies that $(Q \otimes W/p)[\mathfrak{m}'] = 0$, from which we deduce that $(Q \otimes W/p)_{\mathfrak{m}'} = 0$ since $(\mathbb{T}'/p\mathbb{T}')_{\mathfrak{m}'}$ is an Artin local ring, and hence $Q_{\mathfrak{m}'} = 0$.

Suppose $\mathfrak{a} = a_\infty(\infty - [0]) + \sum_{x \in (\mathbb{Z}/N\mathbb{Z})^\times} a_x([x] - [0]) \in \mathrm{Div}^0(C; W/p)$ is annihilated by $\mathfrak{m}'$. Equivalently, $\mathfrak{a}$ is annihilated by $t_\ell \coloneqq T_\ell - \ell - 1$ for all primes $\ell \neq N$. We will use the formulas from Proposition 2.2 to show this implies that $a_x = a_1$ for all $x \in (\mathbb{Z}/N\mathbb{Z})^\times$. Hence we will have

$$\mathfrak{a} = a_\infty(\infty - [0]) + a_1 \mathfrak{c} \in P \otimes_W W/p.$$

To show that $a_x = a_1$ for all $x \in (\mathbb{Z}/N\mathbb{Z})^\times$, choose a prime ℓ such that $\ell \equiv -1 \pmod p$ and such that ℓ is a primitive root modulo N. Then, since $t_\ell \mathfrak{a} = 0$, we have $a_{\ell x} = a_{\ell^{-1} x}$ for all x. Since ℓ is a primitive root, this implies that $a_x = a_1$ if x is a square, and $a_x = a_\ell$ if x is a nonsquare. Now take $q \not\equiv -1 \pmod p$ to be a prime that is a not a square modulo N. Then, since $t_q \mathfrak{a} = 0$, we have

$$(q+1)a_1 = q a_{q^{-1}} + a_q.$$

Since q is not a square, $a_q = a_{q^{-1}} = a_\ell$, so we have

$$(q+1)a_1 = (q+1)a_\ell$$

which implies $a_1 = a_\ell$ because $q \not\equiv -1 \pmod p$. Hence $a_x = a_1$ for all $x \in (\mathbb{Z}/N\mathbb{Z})^\times$, so $\mathfrak{a}$ is in $P \otimes W/p$. □

Corollary 2.6. *We have* $\mathrm{Res}(E) = \frac{N^2-1}{24}\mathfrak{c}$ *and* $\mathrm{Res}(E_{2,N}) = \frac{N-1}{24}(\infty - [0] + \mathfrak{c})$.

Proof. Since Res is Hecke equivariant, it follows that $\mathrm{Res}(E_{2,N}) = \beta(\infty - [0] + \mathfrak{c})$, and $\mathrm{Res}(E) = \alpha\mathfrak{c}$, where $\alpha = \frac{1}{N-1}\mathrm{Res}_{[0]} E$ and $\beta = \mathrm{Res}_\infty(E_{2,N}) = a_0(E_{2,N})$. This proves the claim for $E_{2,N}$. Letting w_{N^2} be the Atkin-Lehner operator, we can calculate $\mathrm{Res}_{[0]} E = a_0(w_{N^2} E)$. As $(w_{N^2} E)(z) = E_{2,N} - N^2 E_{2,N}(Nz)$, we see that $a_0(w_{N^2} E) = (1 - N^2) a_0(E_{2,N}) = \frac{(1-N^2)(N-1)}{24}$ and hence $\alpha = \frac{N^2-1}{24}$. □

For $i \in \{0, 1\}$, let $\mathfrak{m}_i \subset \mathbb{T}$ be the maximal ideal generated by $\mathfrak{m}'$ and $U_N - i$. We consider the localizations at these two maximal ideals. Write $E_1 = E_{2,N}$ and $E_0 = E$ so that $U_N E_i = i E_i$. The results about $\mathfrak{m}_1$ and E_1 below are due to Mazur [Maz77]; we include them simply to draw parallels between the cases when $i = 1$ and $i = 0$.

Lemma 2.7. *For $i = 0, 1$, we have $S_2(\Gamma; \mathbb{Z}_p[\zeta_N])_{\mathfrak{m}_i} \neq 0$ if and only if there is a form $f \in S_2(\Gamma; \mathbb{Z}_p[\zeta_N])$ such that $a_n(f) \equiv a_n(E_i) \bmod p$ for all $n \geq 1$.*

Proof. This follows from the Deligne–Serre lifting lemma [DS74, Lemma 6.11]. □

Theorem 2.8. *Assume $N \not\equiv 1 \bmod p$. Then $S_2(\Gamma; \mathbb{Z}_p[\zeta_N])_{\mathfrak{m}_1} = 0$ and there is a $\mathbb{T}_{\mathfrak{m}_0}$-equivariant short exact sequence*

$$0 \to S_2(\Gamma; \mathbb{Z}_p[\zeta_N])_{\mathfrak{m}_0} \to M_2(\Gamma; \mathbb{Z}_p[\zeta_N])_{\mathfrak{m}_0} \xrightarrow{\mathrm{Res}_{\mathfrak{m}_0}} \mathbb{Z}_p[\zeta_N] \cdot \mathfrak{c} \to 0. \tag{8}$$

Moreover, $S_2(\Gamma; \mathbb{Z}_p[\zeta_N])_{\mathfrak{m}_0} = 0$ if and only if $N \not\equiv -1 \bmod p$.

In particular, there exists $f = \sum_{n \geq 1} a_n q^n \in S_2(\Gamma; \mathbb{Z}_p[\zeta_N])$ such that $a_\ell \equiv \ell + 1 \bmod p$ for all primes $\ell \neq N$ if and only if $N \equiv -1 \bmod p$.

Proof. Suppose that $S_2(\Gamma;\mathbb{Z}_p[\zeta_N])_{\mathfrak{m}_1} \neq 0$. Then, by Lemma 2.7, there is an $f \in S_2(\Gamma;\mathbb{Z}_p[\zeta_N])$ with $a_n(f) \equiv a_n(E_{2,N}) \bmod p$ for all $n \geq 1$. Since $a_0(E_{2,N})$ is not 0 mod p, this implies that there is a nonzero constant in $M_2(\Gamma;\mathbb{F}_p(\zeta_N))$, a contradiction.

The exact sequence (8) follows directly from (7) and Proposition 2.5. If $N \equiv -1 \pmod p$, then let $g \in M_2(\Gamma;\mathbb{Z}_p[\zeta_N])_{\mathfrak{m}_0}$ be such that $\mathrm{Res}_{\mathfrak{m}_0}(g) = \mathfrak{c}$ and let $f = E - \frac{N^2-1}{24}g$. Then $f \equiv E \pmod p$ and, since $\mathrm{Res}_{\mathfrak{m}_0}(f) = 0$, we have $f \in S_2(\Gamma;\mathbb{Z}_p[\zeta_N])_{\mathfrak{m}_0}$. Note that $f \neq 0$ since $p \mid N^2-1$ and so $g \neq \frac{24}{N^2-1}E$ since the latter does not have integral coefficients.

Conversely, suppose that $N \not\equiv \pm 1 \pmod p$ and, for the sake of contradiction, that $S_2(\Gamma;\mathbb{Z}_p[\zeta_N])_{\mathfrak{m}_0} \neq 0$. Let $\bar{E} \in M_2(\Gamma;\mathbb{F}_p(\zeta_N))$ be the reduction of E modulo p. By Lemma 2.7, there is an $f \in S_2(\Gamma;\mathbb{F}_p(\zeta_N))$ with $a_n(f) = a_n(\bar{E})$ for all $n \geq 1$. Since also $a_0(\bar{E}) = a_0(f) = 0$, this implies that $f = \bar{E}$ by the q-expansion principle. This implies $\bar{E} \in S_2(\Gamma;\mathbb{F}_p(\zeta_N))$, but $\mathrm{Res}_{\mathfrak{m}_0}(\bar{E}) \neq 0$ by Corollary 2.6, a contradiction.

For the final statement, simply note that such an f must belong to $S_2(\Gamma;\mathbb{Z}_p[\zeta_N])_{\mathfrak{m}'}$ and that

$$S_2(\Gamma;\mathbb{Z}_p[\zeta_N])_{\mathfrak{m}'} = S_2(\Gamma;\mathbb{Z}_p[\zeta_N])_{\mathfrak{m}_1} \oplus S_2(\Gamma;\mathbb{Z}_p[\zeta_N])_{\mathfrak{m}_0}$$

since $\mathfrak{m}_1$ and $\mathfrak{m}_0$ are the only maximal ideals of $\mathbb{T}$ containing $\mathfrak{m}'$. □

Now set $\mathfrak{m} = \mathfrak{m}_0$ and let $\mathbb{T}^0_{\mathfrak{m}}$ be the maximal quotient of $\mathbb{T}_{\mathfrak{m}}$ acting faithfully on $S_2(\Gamma;\mathbb{Z}_p[\zeta_N])_{\mathfrak{m}}$. Recall that by duality, minimal prime ideals $\mathfrak{P}$ of $\mathbb{T}^0_{\mathfrak{m}}$ are in one-to-one correspondence with Galois conjugacy classes of normalized eigenforms in $S_2(\Gamma;\overline{\mathbb{Z}}_p)$ that are congruent to E modulo the unique prime above p in the p-adic ring $\mathbb{T}^0_{\mathfrak{m}}/\mathfrak{P}$. By Theorem 2.8, we know that $\mathbb{T}^0_{\mathfrak{m}} \neq 0$ when $N \equiv -1 \bmod p$. Moreover, we know that the eigenform corresponding to any minimal prime must be a newform because, by Mazur's theorem, there are no oldforms that are congruent to E. Thus we have the following corollary, which gives Theorem B(a).

Corollary 2.9. *Assume that $N \equiv -1 \bmod p$. Then there is a newform f of weight 2 and level $\Gamma_0(N^2)$ and a prime ideal $\mathfrak{p}$ over p in the ring of integers $\mathcal{O}_f$ of the Hecke field of f such that $a_\ell(f) \equiv 1 + \ell \bmod \mathfrak{p}$ for all primes ℓ.*

Remark 2.10. Let $I^0 \subset \mathbb{T}^0$ be the image of I in $\mathbb{T}^0$. Just as in [WWE20, Lemma 3.2.2], the exact sequence (8) together with duality imply that the map $\mathbb{T}_{\mathfrak{m}} \to \mathbb{Z}_p/\operatorname{Res}_{\mathfrak{m}}(E)\mathbb{Z}_p$ given by $T \mapsto a_1(TE)$ induces an isomorphism $\mathbb{T}^0_{\mathfrak{m}}/I^0_{\mathfrak{m}} \cong \mathbb{Z}_p/\operatorname{Res}_{\mathfrak{m}}(E)\mathbb{Z}_p = \mathbb{Z}_p/(N+1)\mathbb{Z}_p$ and moreover that the natural map $\mathbb{T}_{\mathfrak{m}} \to \mathbb{T}^0_{\mathfrak{m}} \times_{\mathbb{T}^0_{\mathfrak{m}}/I^0_{\mathfrak{m}}} \mathbb{T}_{\mathfrak{m}}/I_{\mathfrak{m}}$ is an isomorphism. In particular, we see that $\mathbb{T}^0_{\mathfrak{m}} \neq 0$ if and only if $p \mid (N+1)$. △

3. An unramified p-extension of $\mathbb{Q}(N^{1/p})$ when $N \equiv -1 \bmod p$

In this section we use a congruence between a cusp form and the Eisenstein series E from Corollary 2.9 to give a modular construction of a degree-p unramified extension of $\mathbb{Q}(N^{1/p})$ when $N \equiv -1 \bmod p$, thus proving Theorem A and Theorem B(b). Throughout this section we assume $N \equiv -1 \bmod p$.

As in Corollary 2.9, fix an eigenform $f \in S_2(\Gamma;\overline{\mathbb{Z}}_p)$ that is congruent to E modulo the prime $\mathfrak{p}$ lying over p. Let $\mathbb{Q}_p(f)/\mathbb{Q}_p$ be the field generated by the Hecke eigenvalues of f, $\mathcal{O}$ its ring of integers, ϖ a uniformizer, and $\mathbb{F} = \mathcal{O}/\varpi$. Let $s \geq 1$ be the largest integer such that $f \equiv E \bmod \varpi^s$, so s is the largest integer such

that $a_\ell(f) \equiv 1 + \ell \bmod \varpi^s$ for all primes $\ell \neq N$. The goal of this section is to prove Theorem B(b), which in turn implies Theorem A. In particular, we show the following.

Theorem 3.1. *There is character $\chi : G_{\mathbb{Q}(N^{1/p})} \to (\mathcal{O}/\varpi^{s+1})^\times$ that is everywhere unramified, has order p, and satisfies $t_f|G_{\mathbb{Q}(N^{1/p})} \equiv \chi\epsilon + \chi^{-1} \bmod \varpi^{s+1}$.*

A key observation is Lemma 3.3, where we use Ribet's method to produce a cocycle from the Galois representation of the Eisenstein-congruent cusp form and identify it as the Kummer cocycle cutting out the extension $\mathbb{Q}(N^{1/p})/\mathbb{Q}$. Crucial to this identification is the fact that the level of the cusp form is prime-to-p, so the Galois representation is crystalline at p. In this case, the crystalline property forces the mod-p reduction to be *finie* in the sense of Serre's conjecture [Ser87], which allows us to explicitly identify the cocycle.

3.1. **Constructing an unramified p-extension.** We recall a Galois-theoretic interpretation of the integer s. Let $\rho_f \colon G_{\mathbb{Q},Np} \to \mathrm{GL}(V_f) \cong \mathrm{GL}_2(\mathbb{Q}_p(f))$ the Galois representation corresponding to f and let $t_f = \mathrm{tr}(\rho_f) : G_{\mathbb{Q},Np} \to \mathcal{O}$ be its trace. Recall the *reducibility ideal* of t_f, as defined in [BC09, Section 1.5]: it is the smallest ideal $J \subset \mathcal{O}$ such that $t_f \equiv \psi_1 + \psi_2 \bmod J$ for characters $\psi_i : G_{\mathbb{Q}} \to (\mathcal{O}/J)^\times$.

Lemma 3.2. *The reducibility ideal of t_f is $\varpi^s\mathcal{O}$.*

Proof. Let $J \subset \mathcal{O}$ be the reducibility ideal of t_f and write $t_f \equiv \psi_1 + \psi_2 \bmod J$ for characters $\psi_i : G_{\mathbb{Q}} \to (\mathcal{O}/J)^\times$. Since $\det(\rho_f) = \epsilon$, we can write $\psi_1 = \psi\epsilon$ and $\psi_2 = \psi^{-1}$ for a character $\psi : G_{\mathbb{Q},Np} \to (\mathcal{O}/J)^\times$ with $\psi \equiv 1 \bmod \varpi\mathcal{O}$. In particular, ψ has p-power order. We claim that ψ is trivial. Assuming this claim, we see that $J = \varpi^t\mathcal{O}$ for the largest integer t such that $t_f \equiv \epsilon + 1 \bmod \varpi^t$, so $t = s$ by Chebotarov density.

To see that ψ is trivial, note that f is ordinary since $a_p(f) \equiv a_p(E) \equiv 1 \bmod \varpi\mathcal{O}$. Hence we have $t_f|I_p = \epsilon + 1$, so we see that ψ is unramified at p. Then ψ factors through the maximal unramified-outside-N abelian pro-p extension of $\mathbb{Q}$, which is trivial since $N \not\equiv 1 \bmod p$. Hence ψ is trivial. □

For a $G_{\mathbb{Q}}$-stable $\mathcal{O}$-lattice $T \subset V_f$, let $\rho_T \colon G_{\mathbb{Q},Np} \to \mathrm{GL}(T)$ denote the corresponding representation. Recall the isomorphism $\mathbb{Q}^\times \otimes_{\mathbb{Z}} \mathbb{Z}_p \cong H^1(\mathbb{Q}, \mathbb{Z}_p(1))$ of Kummer theory. For $m \in \mathbb{Q}^\times$, we say that a cocycle $\kappa_m : G_{\mathbb{Q}} \to \mathbb{Z}_p(1)$ is a *Kummer cocycle for m* if the class of κ_m corresponds to m under the Kummer isomorphism. Choices of κ_m are given by $\kappa_m(\sigma) \equiv \frac{\sigma m^{1/p^r}}{m^{1/p^r}} \pmod{p^r}$ for a choice of p^rth root of m.

Lemma 3.3. *There is a $G_{\mathbb{Q}}$-stable lattice $T \subset V_f$ such that*

$$\rho_T \bmod \varpi^s = \begin{pmatrix} \epsilon & \kappa_N \\ 0 & 1 \end{pmatrix},$$

where κ_N is a Kummer cocycle for N. Moreover, writing $\rho_T = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$, the set $\{c(\sigma)|\sigma \in G_{\mathbb{Q}}\}$ generates $\varpi^s\mathcal{O}$.

Proof. Using Ribet's lemma [Rib76, Proposition 2.1], we choose T such that

$$\rho_T \bmod \varpi = \begin{pmatrix} \omega & \bar{b} \\ 0 & 1 \end{pmatrix}$$

where $\bar{b}\colon G_{\mathbb{Q}} \to \mathbb{F}(1)$ is a cocycle with nontrivial cohomology class. Write the entries of ρ_T as $\rho_T = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$. By Lemma 3.2 and [BC09, Proposition 1.5.1, pg. 35], we see that $BC = \varpi^s\mathcal{O}$, where $B, C \subset \mathcal{O}$ are the ideals generated by $b(\sigma)$ and $c(\sigma)$, respectively, for all $\sigma \in G_{\mathbb{Q},Np}$. Since $\bar{b}$ is nontrivial, we see that B is the unit ideal, so $C = \varpi^s\mathcal{O}$. From this we see that $\rho_T \bmod \varpi^s$ has the desired upper-triangular shape, and it remains to describe the cocycle $b \bmod \varpi^s$.

The class of $b \bmod \varpi^s$ belongs to $H^1(G_{\mathbb{Q},Np}, (\mathcal{O}/\varpi^s)(1))$, which is generated by the Kummer classes κ_N and κ_p of N and p by Kummer theory. Note that ρ_T is *finie* in the sense of Serre [Ser87] (that is, it comes from the generic fiber of a finite flat group scheme over $\mathbb{Z}_p$) since it comes from a modular form of weight 2 and level prime-to-p, hence corresponds to the p-torsion of an abelian variety with good reduction at p. It follows that $\rho_T \bmod \varpi$ has Serre weight 2 and hence is *peu ramifié* [Ser87, Proposition 3, 4]. Since $\bar{b}$ is nontrivial, we see that the only way $\rho_T \bmod \varpi$ can be peu ramifié is for $b \bmod \varpi^s$ to be a unit multiple of κ_N, and we can change basis to ensure that $\rho_T \bmod \varpi^s$ has the desired form. □

Fix a lattice $T \subset V_f$ as in Lemma 3.3, and let $\rho = \rho_T = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ and $\bar{b} = b \bmod \varpi$. Since $\bar{b}$ is the Kummer cocycle associated to N, we see that $\bar{b}|G_F = 0$, where $F \coloneqq \mathbb{Q}(N^{1/p})$. This implies that $b|G_F$ takes values in $\varpi\mathcal{O}$. Since we also know that c takes values in $\varpi^s\mathcal{O}$, we see that the reducibility ideal (in the sense of [BC09, Section 1.5]) of $t_f|G_F$ is contained in ϖ^{s+1}. This implies that

$$a|G_F \bmod \varpi^{s+1} : G_F \to (\mathcal{O}/\varpi^{s+1})^\times$$

is a group homomorphism. Define a character $\chi : G_F \to (\mathcal{O}/\varpi^{s+1})^\times$ by

$$\chi\epsilon = a|G_F \bmod \varpi^{s+1}.$$

Note that, since $\det(\rho) = \epsilon$, we have $d|G_F \bmod \varpi^{s+1} = \chi^{-1}$, so

$$t_f|G_F = \chi\epsilon + \chi^{-1} \bmod \varpi^{s+1}. \tag{9}$$

To complete the proof of Theorem 3.1, it suffices to prove that χ has order p and is unramified everywhere, which we prove in the following two propositions.

Proposition 3.4. *The character χ is nontrivial.*

Proof. Let $r = \rho \bmod \varpi^{s+1}$. Suppose, for the sake of contradiction, that χ is trivial. Then we have

$$r(G_{F(\zeta_p)}) \subset \left\{ \begin{pmatrix} x & \varpi y \\ \varpi^s z & 1 \end{pmatrix} \in \mathrm{GL}_2(\mathcal{O}/\varpi^{s+1}) \right\}.$$

Now choose $\sigma \in G_{\mathbb{Q}}$ such that $\bar{b}(\sigma) \neq 0$, and let $\tau \in G_{F(\zeta_p)}$ and write $r(\tau) = \left(\begin{smallmatrix} x & \varpi y \\ \varpi^s z & 1 \end{smallmatrix}\right)$. Since $x, d(\sigma) \equiv 1 \bmod \varpi$, we compute that

$$r(\sigma) \begin{pmatrix} x & \varpi y \\ \varpi^s z & 1 \end{pmatrix} r(\sigma)^{-1} = \begin{pmatrix} * & * \\ * & 1 - zb(\sigma)\det(r(\sigma))^{-1}\varpi^s \end{pmatrix}.$$

As $r(G_{F(\zeta_p)})$ is normal in $r(G_{\mathbb{Q}})$, we see that $zb(\sigma)\det(r(\sigma))^{-1}\varpi^s \equiv 0 \bmod \varpi^{s+1}$. Since $b(\sigma)$ and $\det(r(\sigma))$ are units, we conclude that $z \in \varpi\mathcal{O}/\varpi^{s+1}$. Thus for any $\tau \in G_{F(\zeta_p)}$, we have $c(\tau) \equiv 0 \bmod \varpi^{s+1}$.

By Lemma 3.3, we can write $c = \varpi^s\tilde{c}$ for a cochain $\tilde{c} : G_{\mathbb{Q},Np} \to \mathcal{O}$ such that $\bar{c} \coloneqq \tilde{c} \bmod \varpi$ is nontrivial. It follows that $\bar{c}$ is a cocycle $\bar{c} : G_{\mathbb{Q}} \to \mathbb{F}(-1)$ with nontrivial class. Then $\bar{c}|G_{\mathbb{Q}(\zeta_p)}$ is a homomorphism cutting out a degree-p extension $K/\mathbb{Q}(\zeta_p)$ such that $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ acts on $\mathrm{Gal}(K/\mathbb{Q}(\zeta_p))$ via ω^{-1}. But, since

we assume that χ is trivial, the previous paragraph shows that $\bar{c}(\tau) = 0$ for all $\tau \in G_{F(\zeta_p)}$, so $K = F(\zeta_p)$. But $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ acts on $\mathrm{Gal}(F(\zeta_p)/\mathbb{Q}(\zeta_p))$ via ω, so this implies $\omega = \omega^{-1}$, which contradicts $p > 3$. □

Proposition 3.5. *The character χ is unramified everywhere.*

Proof. Since ρ is unramified outside Np, χ is as well. It remains to show that χ is unramified at N and p. We first consider ramification at N. By local class field theory, the maximal abelian tame quotient of the inertia group at N in G_F has order $N - 1$, which is prime-to-p by our assumptions that $N \equiv -1 \bmod p$ and $p > 2$. Since the image of χ has order p, this implies that χ is unramified at N.

Finally, to see that χ is unramified at p we need to show that $\chi|I_p \cap G_F = 0$. By Lemma 3.3 and the definition of χ, we can write $\chi = 1 + \alpha\varpi^s$ for an additive character $\alpha : G_F \to \mathbb{F}$, and we need to show that $\alpha|I_p \cap G_F = 0$. In this notation, (9) says

$$t_f|G_F \equiv \varepsilon + 1 + (\varepsilon - 1)\alpha\varpi^s \bmod \varpi^{s+1}.$$

On the other hand, as we noted in the proof of Lemma 3.2, the fact that f is ordinary implies that $t_f|I_p = \epsilon + 1$. Combining these two, we have $(\varepsilon - 1)\alpha\varpi^s = 0$ on $I_p \cap G_F$. This is equivalent to $(\omega - 1)\alpha = 0$ as functions $I_p \cap G_F \to \mathbb{F}$. If $\sigma \in I_p \cap G_F \setminus \ker\omega$, then it follows that $\alpha(\sigma) = 0$. For $\sigma \in I_p \cap G_F \cap \ker\omega$, choose any $\tau \in I_p \cap G_F \setminus \ker\omega$. Then $\omega(\tau) \neq 1$ and $\alpha(\tau) = 0$, so we obtain

$$0 = (\omega(\sigma\tau) - 1)\alpha(\sigma\tau) = (\omega(\sigma)\omega(\tau) - 1)(\alpha(\sigma) + \alpha(\tau)) = (\omega(\tau) - 1)\alpha(\sigma),$$

and thus $\alpha(\sigma) = 0$. □

3.2. **Explicit class field theory encoded by f.** Keep the notation from the previous section. In particular, N, p, f are all fixed. From f, there is an associated character χ of $G_{\mathbb{Q}(N^{1/p})}$ as in Theorem B(b), or equivalently as defined prior to Proposition 3.5. Let L be the degree-p extension of $\mathbb{Q}(N^{1/p})$ cut out by character χ, so $L/\mathbb{Q}(N^{1/p})$ is an everywhere unramified degree-p extension. In this section we show how the Fourier coefficients of f (modulo ϖ^{s+1}) carry information about how primes of $\mathbb{Q}(N^{1/p})$ split in L as well as when N is not a pth power modulo ℓ when $\ell \equiv 1 \bmod p$. This explicit information shows the advantage of our modular methods compared to Calegari's abstract cup product argument (cf. Section 1.3).

We begin by understanding how rational primes split in $\mathbb{Q}(N^{1/p})$. For each prime ℓ, fix a discrete logarithm $\log_\ell : \mathbb{F}_\ell^\times \to \mathbb{Z}/(\ell - 1)\mathbb{Z}$, so $a \in \mathbb{F}_\ell^\times$ is a pth power if and only if $\log_\ell(a) \equiv 0 \bmod p$, which is automatic whenever $\ell \not\equiv 1 \bmod p$.

Lemma 3.6. *Let $\ell \neq p, N$ be prime and let r be the multiplicative order of ℓ in $\mathbb{F}_p^\times$. If $\log_\ell(N) \not\equiv 0 \bmod p$, then ℓ is inert in $\mathbb{Q}(N^{1/p})$. Otherwise, there are $\frac{p-1}{r} + 1$ primes of $\mathbb{Q}(N^{1/p})$ lying over ℓ, one with residue degree 1 and the rest having residue degree r.*

Proof. Note that the only prime factors dividing the discriminant of the order $\mathbb{Z}[N^{1/p}]$ are p and N — the same prime divisors of the discriminant of $\mathbb{Q}(N^{1/p})$. Thus we can understand the splitting behavior of ℓ in $\mathbb{Q}(N^{1/p})$ by considering how $x^p - N$ factors over $\mathbb{F}_\ell$.

First suppose $\log_\ell(N) \not\equiv 0 \bmod p$, so N is not a pth power in $\mathbb{F}_\ell$. Then it is well known that $x^p - N$ is irreducible over $\mathbb{F}_\ell$ (see [Lan02, Theorem VI.9.1, pg. 297], for example).

Now suppose $\log_\ell(N) \equiv 0 \bmod p$, so $N = a^p$ for some $a \in \mathbb{F}_\ell^\times$. Using the substitution $x \mapsto ay$, we get

$$\frac{\mathbb{F}_\ell[x]}{(x^p - N)} \cong \frac{\mathbb{F}_\ell[y]}{(y^p - 1)} \cong \mathbb{F}_\ell \times \frac{\mathbb{F}_\ell[y]}{(\Phi_p(y))} \cong \mathbb{F}_\ell \times \mathbb{F}_{\ell^r}^{(p-1)/r},$$

where $\Phi_p(y)$ is the cyclotomic polynomial. For the last isomorphism, note that $\Phi_p(y)$ divides $y^{\ell^r} - y$ but $\gcd(\Phi_p(y), y^{\ell^d} - y) = 1$ for any $d < r$, so the irreducible factors of $\Phi_p(y)$ all have degree r. □

Proposition 3.7. *Let $\ell \neq N, p$ be prime.*

1. *If $\ell \equiv 1 \bmod p$ and $a_\ell(f) \not\equiv 1 + \ell \bmod \varpi^{s+1}$, then $\log_\ell(N) \not\equiv 0 \bmod p$, so ℓ is inert in $\mathbb{Q}(N^{1/p})$ and $\ell\mathcal{O}_{\mathbb{Q}(N^{1/p})}$ splits completely in L (in fact, in the Hilbert class field of $\mathbb{Q}(N^{1/p})$).*
2. *If $\ell \not\equiv 1 \bmod p$, then the unique prime of $\mathbb{Q}(N^{1/p})$ lying over ℓ of residue degree 1 splits in L if and only if $a_\ell(f) \equiv \ell + 1 \bmod \varpi^{s+1}$.*

Proof. Write the character χ from Theorem B(b) as $\chi = 1 + \varpi^s\alpha$ with $\alpha : G_{\mathbb{Q}(N^{1/p})} \to \mathbb{F}$ an additive character. Then

$$t_f|G_{\mathbb{Q}(N^{1/p})} \equiv \epsilon\chi + \chi^{-1} \equiv 1 + \epsilon + \varpi^s(\epsilon - 1)\alpha \bmod \varpi^{s+1}.$$

Suppose that $\log_\ell(N) \equiv 0 \bmod p$ so that ℓ has a prime λ of $\mathbb{Q}(N^{1/p})$ lying above it of residue degree 1. Up to conjugation we may take $\mathrm{Frob}_\ell = \mathrm{Frob}_\lambda \in G_{\mathbb{Q}(N^{1/p})}$. Thus by (9), we have

$$a_\ell(f) = t_f(\mathrm{Frob}_\lambda) \equiv 1 + \ell + \varpi^s(\ell - 1)\alpha(\mathrm{Frob}_\lambda) \bmod \varpi^{s+1} \tag{10}$$

whenever $\log_\ell(N) \equiv 0 \bmod p$.

When $\ell \not\equiv 1 \bmod p$, we see that $a_\ell(f) \equiv \ell + 1 \bmod \varpi^{s+1}$ if and only if $\alpha(\mathrm{Frob}_\lambda) = 0$. Since L is cut out by $\ker\chi = \ker\alpha$, it follows that λ splits in L if and only if $a_\ell(f) \equiv \ell + 1 \bmod \varpi^{s+1}$, proving (2).

In contrast, when $\ell \equiv 1 \bmod p$, (10) shows that $a_\ell(f) \equiv 1 + \ell \bmod \varpi^{s+1}$ under the assumption that $\log_\ell(N) \equiv 0 \bmod p$, thus establishing the contrapositive of (1). The last part of (1) follows from Lemma 3.6 and the fact that the principal ideals of $\mathbb{Q}(N^{1/p})$ are exactly those that split completely in its Hilbert class, which contains L. □

Remark 3.8. Note that if a prime ℓ satisfies $a_\ell(f) \equiv \ell+1 \bmod \varpi^{s+1}$, then T_ℓ cannot generate the Eisenstein ideal since that would force the entire Eisenstein congruence to persist modulo ϖ^{s+1}, contradicting the definition of s. △

If we impose the hypothesis that the class number of $\mathbb{Q}(N^{1/p})$ is p, so L is its Hilbert class field, then we can further interpret our results in a classical style suggestive of results in explicit class field theory in the case of imaginary quadratic fields. While this hypothesis on the class number is certainly not always satisfied, it holds in many examples. For instance, the hypothesis holds when $p = 5$ and

$$N \in \{19, 29, 59, 79, 89, 109, 139, 149, 199\}$$

and when $p = 7$ and $N \in \{13, 41, 97, 139, 181\}$.

Corollary 3.9. *Assume that $\mathbb{Q}(N^{1/p})$ has class number p. Let λ be a prime of $\mathbb{Q}(N^{1/p})$ lying over $\ell \neq N, p$.*

(1) *If $\ell \not\equiv 1 \bmod p$ and either $\#\mathcal{O}_{\mathbb{Q}(N^{1/p})}/\lambda = \ell$ or $\#\mathcal{O}_{\mathbb{Q}(N^{1/p})}/\lambda = \ell^{p-1}$, then the following are equivalent:*
   (a) *λ is a principal $\mathcal{O}_{\mathbb{Q}(N^{1/p})}$-ideal;*
   (b) *λ splits completely in L over $\mathbb{Q}(N^{1/p})$;*
   (c) *ℓ is a norm from $\mathbb{Q}(N^{1/p})$;*
   (d) *$a_\ell(f) \equiv \ell + 1 \bmod \varpi^{s+1}$.*

(2) *If $\ell \equiv 1 \bmod p$ and $a_\ell(f) \not\equiv \ell + 1 \bmod \varpi^{s+1}$, then ℓ is inert in $\mathbb{Q}(N^{1/p})$ and then splits in L. In this case ℓ is not a norm from $\mathbb{Q}(N^{1/p})$.*

Proof. Write $F := \mathbb{Q}(N^{1/p})$, and suppose that $\ell \not\equiv 1 \bmod p$ and $\#\mathcal{O}_F/\lambda = \ell$. The equivalence of (a) and (b) follows from the fact that the primes that split in the Hilbert class field L of F are exactly the principal ideals. The equivalence of (a) and (c) follows from the fact that the norm of an element is equal to the norm of the ideal it generates. The equivalence of (b) and (d) follows from the first part of Proposition 3.7.

The second part follows from Proposition 3.7 and the fact that L is the Hilbert class field of F. □

Example 3.10. We finish with an example when $p = 5$ and $N = 19$. We compute that $\mathbb{Q}(19^{1/5})$ has class number 5, so Corollary 3.9 applies. In this case f has LMFDB label 361.2.a.f and Hecke field $\mathbb{Q}(\sqrt{5})$. The Eisenstein congruence holds modulo $\varpi = \sqrt{5}$, but not modulo $\varpi^2 = 5$, so $s = 1$ in this case. Set $\beta = \frac{1+\sqrt{5}}{2}$. Table 1 contains the first sixty prime-index coefficients for f. The ones in bold are those for which the Eisenstein congruence persists modulo 5, and the circled primes ℓ are those for which Corollary 3.9 implies that there exists a principal prime ideal of F lying over ℓ. (We also circle 19 since the principal ideal generated by $19^{1/5}$ clearly lies over it.) Moreover, in this example we can calculate that $\mathcal{O}_F = \mathbb{Z}[19^{1/5}]$ and hence it is easy to write the norm form explicitly. In particular, the four equivalent conditions on ℓ in Corollary 3.9(1) are also equivalent to

$$\begin{aligned}\ell = {} & a^5 - 95a^3be - 95a^3cd + 95a^2b^2d + 95a^2bc^2 + 1805a^2ce^2 + 1805a^2d^2e - 95ab^3c + 1805ab^2e^2 \\ & - 1805abcde - 1805abd^3 - 1805ac^3e + 1805ac^2d^2 - 34295ade^3 + 19b^5 - 1805b^3de \\ & + 1805b^2c^2e + 1805b^2cd^2 - 1805bc^3d - 34295bce^3 + 34295bd^2e^2 + 361c^5 + 34295c^2de^2 \\ & - 34295cd^3e + 6859d^5 + 130321e^5\end{aligned}$$

for some $(a, b, c, d, e) \in \mathbb{Z}^5$.

△

Acknowledgments

We thank Frank Calegari for asking the question that inspired this work and for his encouragement. We also thank Pedro Lemos and Samit Dasgupta for helpful conversations related to this project, Pip Goodman for bringing the paper [Iim86] to our attention, and Bruce Jordan, Lillian Pierce, Victor Rotger, and the anonymous referee for feedback on an earlier version.

References

[BC09] Joël Bellaïche and Gaëtan Chenevier, *Families of Galois representations and Selmer groups*, Astérisque, **324** (2009), xii+314.

TABLE 1. Prime-index coefficients of 361.2.a.f, with $\beta = \frac{1+\sqrt{5}}{2}$

ℓ	$a_\ell(f)$	ℓ	$a_\ell(f)$	ℓ	$a_\ell(f)$	ℓ	$a_\ell(f)$
2	β	53	$5-7\beta$	127	$9-2\beta$	199	$6-12\beta$
3	$2-\beta$	59	$-11+7\beta$	131	$\mathbf{7+5\beta}$	211	$1-3\beta$
5	2β	61	$-7-2\beta$	137	$1+4\beta$	223	$11-14\beta$
7	$\mathbf{3}$	67	$\mathbf{-7}$	139	$-3+11\beta$	227	$-3+12\beta$
11	$-\beta$	71	$-1-4\beta$	149	$\mathbf{-10+5\beta}$	229	$-12-\beta$
13	$\mathbf{-1}$	73	$7-6\beta$	151	$\mathbf{-13-5\beta}$	233	$11-4\beta$
17	$4-2\beta$	79	$-6+12\beta$	157	$-13-3\beta$	239	$11-7\beta$
19	$\mathbf{0}$	83	$2+4\beta$	163	$5-2\beta$	241	$\mathbf{-13+10\beta}$
23	$7-\beta$	89	$-11+2\beta$	167	$17+2\beta$	251	$\mathbf{7-20\beta}$
29	$-2-\beta$	97	$9+3\beta$	173	$6-4\beta$	257	$\mathbf{-12+20\beta}$
31	$-4-3\beta$	101	$\mathbf{7-10\beta}$	179	$9+2\beta$	263	$-2-8\beta$
37	$4+3\beta$	103	$3+7\beta$	181	$\mathbf{12}$	269	$19+7\beta$
41	$\mathbf{-3}$	107	$-3+12\beta$	191	$11+2\beta$	271	$6-3\beta$
43	$5+3\beta$	109	$-1+6\beta$	193	$18-8\beta$	277	$-8+12\beta$
47	$\mathbf{3}$	113	$10-2\beta$	197	$\mathbf{3}$	281	$-2-17\beta$

[Cal17] Frank Calegari, *Persiflage blog*, https://www.galoisrepresentations.com/2017/03/29/pseudo-representations-and-the-eisenstein-ideal/, https://www.galoisrepresentations.com/2017/06/10/elementary-class-groups-updated/, 2017.

[Cal06] Frank Calegari, *Eisenstein deformation rings*, Compos. Math. **142** (2006), no. 1, 63–83, DOI 10.1112/S0010437X05001661. MR2196762

[CE05] Frank Calegari and Matthew Emerton, *On the ramification of Hecke algebras at Eisenstein primes*, Invent. Math. **160** (2005), no. 1, 97–144, DOI 10.1007/s00222-004-0406-z. MR2129709

[DDP11] Samit Dasgupta, Henri Darmon, and Robert Pollack, *Hilbert modular forms and the Gross-Stark conjecture*, Ann. of Math. (2) **174** (2011), no. 1, 439–484, DOI 10.4007/annals.2011.174.1.12. MR2811604

[DR73] P. Deligne and M. Rapoport, *Les schémas de modules de courbes elliptiques* (French), Modular functions of one variable, II (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972), Lecture Notes in Math., Vol. 349, Springer, Berlin, 1973, pp. 143–316. MR0337993

[DS74] Pierre Deligne and Jean-Pierre Serre, *Formes modulaires de poids* 1 (French), Ann. Sci. École Norm. Sup. (4) **7** (1974), 507–530 (1975). MR379379

[DS05] Fred Diamond and Jerry Shurman, *A first course in modular forms*, Graduate Texts in Mathematics, vol. 228, Springer-Verlag, New York, 2005. MR2112196

[GL86] Benedict H. Gross and Jonathan Lubin, *The Eisenstein descent on $J_0(N)$*, Invent. Math. **83** (1986), no. 2, 303–319, DOI 10.1007/BF01388965. MR818355

[Iim86] Kiyoaki Iimura, *On the l-rank of ideal class groups of certain number fields*, Acta Arith. **47** (1986), no. 2, 153–166, DOI 10.4064/aa-47-2-153-166. MR867494

[Kob16] Hirotomo Kobayashi, *Class numbers of pure quintic fields*, J. Number Theory **160** (2016), 463–477, DOI 10.1016/j.jnt.2015.09.017. MR3425217

[Lan02] Serge Lang, *Algebra*, 3rd ed., Graduate Texts in Mathematics, vol. 211, Springer-Verlag, New York, 2002, DOI 10.1007/978-1-4613-0041-0. MR1878556

[Lec18] Emmanuel Lecouturier, *On the Galois structure of the class group of certain Kummer extensions*, J. Lond. Math. Soc. (2) **98** (2018), no. 1, 35–58, DOI 10.1112/jlms.12123. MR3847231

[Mar17] Kimball Martin, *The Jacquet-Langlands correspondence, Eisenstein congruences, and integral L-values in weight 2*, Math. Res. Lett. **24** (2017), no. 6, 1775–1795, DOI 10.4310/MRL.2017.v24.n6.a11. MR3762695

[Maz77] B. Mazur, *Modular curves and the Eisenstein ideal*, Inst. Hautes Études Sci. Publ. Math. **47** (1977), 33–186 (1978). With an appendix by Mazur and M. Rapoport. MR488287

[Mer96] Loïc Merel, *L'accouplement de Weil entre le sous-groupe de Shimura et le sous-groupe cuspidal de $J_0(p)$* (French), J. Reine Angew. Math. **477** (1996), 71–115, DOI 10.1515/crll.1996.477.71. MR1405312

[MW84] B. Mazur and A. Wiles, *Class fields of abelian extensions of* $\mathbf{Q}$, Invent. Math. **76** (1984), no. 2, 179–330, DOI 10.1007/BF01388599. MR742853

[Oht99] Masami Ohta, *Ordinary p-adic étale cohomology groups attached to towers of elliptic modular curves*, Compositio Math. **115** (1999), no. 3, 241–301, DOI 10.1023/A:1000556212097. MR1674001

[Rib76] Kenneth A. Ribet, *A modular construction of unramified p-extensions of $Q(\mu_p)$*, Invent. Math. **34** (1976), no. 3, 151–162, DOI 10.1007/BF01403065. MR419403

[Rib10] Kenneth A. Ribet, *Non-optimal levels of reducible mod ℓ Galois representations*, Lecture at CRM, slides available at `https://math.berkeley.edu/~ribet/crm.pdf`, 2010.

[Ser87] Jean-Pierre Serre, *Sur les représentations modulaires de degré* 2 *de* $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ (French), Duke Math. J. **54** (1987), no. 1, 179–230, DOI 10.1215/S0012-7094-87-05413-5. MR885783

[SS19] Karl Schaefer and Eric Stubley, *Class groups of Kummer extensions via cup products in Galois cohomology*, Trans. Amer. Math. Soc. **372** (2019), no. 10, 6927–6980, DOI 10.1090/tran/7746. MR4024543

[Wak22] Preston Wake, *The Eisenstein ideal for weight k and a Bloch-Kato conjecture for tame families*, J. Eur. Math. Soc. Published online `https://doi.org/10.4171/jems/1251`, 2022.

[WWE20] Preston Wake and Carl Wang-Erickson, *The rank of Mazur's Eisenstein ideal*, Duke Math. J. **169** (2020), no. 1, 31–115, DOI 10.1215/00127094-2019-0039. MR4047548

[WWE21] Preston Wake and Carl Wang-Erickson, *The Eisenstein ideal with squarefree level*, Adv. Math. **380** (2021), Paper No. 107543, 62, DOI 10.1016/j.aim.2020.107543. MR4200464

[Yoo19a] Hwajong Yoo, *Non-optimal levels of a reducible* mod ℓ *modular representation*, Trans. Amer. Math. Soc. **371** (2019), no. 6, 3805–3830, DOI 10.1090/tran/7314. MR3917209

[Yoo19b] Hwajong Yoo, *On rational Eisenstein primes and the rational cuspidal groups of modular Jacobian varieties*, Trans. Amer. Math. Soc. **372** (2019), no. 4, 2429–2466, DOI 10.1090/tran/7645. MR3988582

Temple University, Department of Mathematics, Philadelphia, PA 19122
Email address: `jaclyn.lang@temple.edu`

Michigan State University, Department of Mathematics, East Lansing, MI 48824
Email address: `wakepres@msu.edu`