SERRE'S CONJECTURES

BRYDEN CAIS

1. Introduction

The goal of these notes is to provide an introduction to Serre's conjecture concerning odd irreducible 2-dimensional mod p Galois representations. The primary reference is Serre's excellent paper [24]. We follow Serre's suggestion in that paper and work systematically with modular forms in the sense of Katz, and must therefore modify Serre's definitions of the weight of a Galois representation as in [10]. The first part of these notes gives an overview of the algebro-geometric theory of modular forms: such a viewpoint is essential in order to prove results later on down the road. Next, we explain the precise form of Serre's conjecture specifying the level, weight, and character of an odd irreducible mod p Galois representation and motivate this recipe with the deep theorems of Deligne, Fontaine, Carayol and others describing the existence and properties of mod p representations associated to modular forms. Finally, we give evidence—both theoretical and computational–for Serre's conjecture. In particular, we treat the general case of icosahedral mod 2 Galois representations, and correct several mistakes in Mestre's original development [20] of these examples.

2. Modular forms

2.1. **Elliptic curves.**

Definition 2.1.1. For any scheme S, an *elliptic curve* $\pi : E \to S$ is a proper smooth (relative) curve with geometrically connected fibers of genus 1, equipped with a section e:

$$\begin{tikzcd} E \arrow[d, "\pi"'] \\ S \arrow[u, bend right, "e"'] \end{tikzcd}$$

One shows [18, 2.1.2] that E/S has a unique structure of an S-group scheme with identity section e, and it is commutative.

Remark 2.1.2. In the sequel, we will work with the more general notion of *generalized elliptic curves*. Roughly speaking, a generalized elliptic curve E over a base S is a family of curves that are either elliptic curves in the usual sense or "degenerate" elliptic curves (Néron polygons) such that the relative smooth locus E^{sm} has the structure of a commutative group scheme extending to an action on E such that the translation action by rational points on geometric fibers rotates the polygon. For the precise definition, see [7, II 1.12].

For a positive integer $N \geq 1$ and a generalized elliptic curve E/S, we let E_N denote the kernel of multiplication by N on E^{sm}. This is a finitely presented flat S-group scheme that is moreover étale if and only if N is a unit in $\Gamma(S, \mathscr{O}_S)$, and it is finite if and only if the number of connected components of each nonsmooth geometric fiber of E^{sm} is a multiple of N. In such cases, E_N is étale-locally isomorphic to $(\mathbf{Z}/N\mathbf{Z})^2$ if N is a unit on S.

For an elliptic curve E, define the $\mathscr{O}_S$-module

$$\omega_{E/S} := \pi_* \Omega^1_{E/S}.$$

This is an invertible sheaf on S whose formation commutes with base change on S and that is canonically dual to $R^1\pi_*\mathscr{O}_{E/S}$ [18, 2.2]. By replacing $\Omega^1_{E/S}$ with the relative dualizing sheaf in the sense of Grothendieck duality

Date: November 26, 2009.

Thanks to Brian Conrad, for reviewing several versions of these notes and suggesting many improvements, and for providing the proof of Lemma 2.7.4. I am grateful to Kevin Buzzard for pointing out an error in the original manuscript, and for suggesting the reference [1].

[5], one can also define a pushforward sheaf $\omega_{E/S}$ for any generalized elliptic curve; it is again invertible and its formation commutes with any base change. Concretely, $\omega_{E/S} = e^*\Omega^1_{E/S}$ in general (with $e \in E^{\mathrm{sm}}(S)$ the identity section), though this latter definition is *ad hoc.*

For a generalized elliptic curve $\pi : E \to S$ there is a (possibly non-reduced) closed subscheme structure $S_\infty \hookrightarrow S$ on the closed set of $s \in S$ such that E_s is not smooth; the formation of S_∞ commutes with any base change on S (see [4, 2.1.7–2.1.13]). We call S_∞ the *scheme of non-smoothness* for $E \to S$.

Definition 2.1.3. We call $E \to S$ *degenerate* if $S_\infty = S$.

2.2. Moduli of elliptic curves.

Definition 2.2.1. Let E/S be a generalized elliptic curve and $N \geq 1$ an integer such that S is a $\mathbf{Z}[1/N]$-scheme. By a $\Gamma_1(N)$-*structure* α on E/S we mean an immersion of S-group schemes

$$\alpha : \mu_N \hookrightarrow E_N \subseteq E^{\mathrm{sm}}$$

whose associated inverse ideal sheaf on E is fiberwise ample; that is, the image meets every irreducible component in each geometric fiber of E.

We remark that one could also make this definition using the group scheme $\mathbf{Z}/N\mathbf{Z}$ rather than μ_N, and for applications over $\operatorname{Spec}\mathbf{Z}$ (rather than $\operatorname{Spec}\mathbf{Z}[1/N]$) this turns out to be more fruitful.

Let R be any ring in which N is a unit. We form a category $[\Gamma_1(N)]_R$ whose *objects* are pairs $(E/S/R, \alpha)$, where E/S is a generalized elliptic curve over the R-scheme S, and α is a $\Gamma_1(N)$-structure on E/S. The *morphisms* of $[\Gamma_1(N)]_R$ between two objects $(E'/S'/R, \alpha')$ and $(E/S/R, \alpha)$ are cartesian squares

$$\begin{tikzcd} E' \arrow[r] \arrow[d] & E \arrow[d] \\ S' \arrow[r] & S \end{tikzcd}$$

that are compatible with α, α'. For $N > 4$, $\Gamma_1(N)$-structures have no nontrivial automorphisms.

Theorem 2.2.2. *Suppose $N > 4$. The functor which assigns to each $\mathbf{Z}[1/N]$-scheme S the set of isomorphism classes of pairs (E, α) consisting of a generalized elliptic curve E/S and a $\Gamma_1(N)$-structure α on E/S is represented by a smooth and proper curve $X_1(N)$ over* $\operatorname{Spec}\mathbf{Z}[1/N]$ *with geometrically connected fibers. The functor which assigns to such S the set of isomorphism classes of elliptic curves equipped with $\Gamma_1(N)$-structure is represented by an affine open subscheme $Y_1(N)$ of $X_1(N)$ whose complement is $\mathbf{Z}[1/N]$-finite.*

Proof. See [4], especially §4, or [7, IV, 3.5.1] together with [14, Prop. 2.1]. ■

We remark that the complement of $Y_1(N)$ in $X_1(N)$, given its reduced structure, is a finite disjoint union of schemes $\operatorname{Spec}\mathbf{Z}[1/N, \zeta_d]$ for various $d|N$ (with some repetitions). This is the closed subscheme of *cusps*, denoted $\mathbf{c}$*usps*, and it coincides with the scheme of non-smoothness $X_1(N)_\infty$ for the universal family over $X_1(N)$. After base change to $\operatorname{Spec}\mathbf{Z}[1/N, \zeta_N]$, the subscheme $\mathbf{c}$*usps* "breaks up" into a disjoint union of sections.

Remark 2.2.3. Another way of stating Theorem 2.2.2 is that for $N > 4$ the category $[\Gamma_1(N)]_{\mathbf{Z}[1/N]}$ has a final object

$$(\underline{E}/X_1(N), \underline{\alpha}).$$

The same holds over any $\mathbf{Z}[1/N]$-algebra R by base change.

2.3. Modular forms.

Definition 2.3.1. Let $N \geq 1$ and k be integers and R any ring in which N is a unit. A *modular form* f of weight k for $\Gamma_1(N)$, defined over R, is a rule that assigns to every object $(E/S, \alpha)$ of $[\Gamma_1(N)]_R$ a section $f(E/S, \alpha)$ of $\omega^{\otimes k}_{E/S}$ that is compatible with morphisms in $[\Gamma_1(N)]_R$. We denote the R-module of modular forms of weight k for $\Gamma_1(N)$ by $M(k, N)_R$.

Observe that $M(0, N)_R = R$ for $N > 4$ because $X_1(N)_R \to \operatorname{Spec} R$ is smooth and proper with geometrically connected fibers.

We need of course only define a modular form f as a rule on generalized elliptic curves E/S for *affine* $S = \operatorname{Spec} A$. In this situation, given a modular form f and any basis ω of $\omega_{E/A}$ (which may be found by Zariski-localization of

A), we obtain an element $f(E/A, \alpha)/\omega^{\otimes k} \in A$. We therefore see that a modular form as above is equivalent to a rule f that assigns to every triple $(E/A, \alpha, \omega)$ consisting of a generalized elliptic curve E over an R-algebra A, a $\Gamma_1(N)$-structure α on E/A, and a basis ω of $\omega_{E/A}$ an element $f(E/A, \alpha, \omega) \in A$ that is functorial in the triple $(E/A, \alpha, \omega)$ and is "homogenous of weight $-k$ in ω" i.e. $f(E/A, \alpha, \lambda\omega) = \lambda^{-k} f(E/A, \alpha, \omega)$ for all $\lambda \in A^\times$. The key here is that the line bundle on E whose pushforward defines $\omega_{E/S}$ is canonically the pullback of $\omega_{E/S}$ to E.

Let us show that this recovers the usual definition of a modular form over $\mathbf{C}$. Recall that every elliptic curve over $\mathbf{C}$ has the form $E_\tau = \mathbf{C}/\Lambda_\tau$ with $\Lambda_\tau = \mathbf{Z} \oplus \mathbf{Z}\tau$ for some $\tau \in \mathbf{C} - \mathbf{R}$. After picking a primitive N^{th} root of unity ζ, we put a $\Gamma_1(N)$-structure α on E_τ via

$$\begin{aligned} \alpha_\zeta : \mu_N(\mathbf{C}) &\to \frac{1}{N}\Lambda_\tau/\Lambda_\tau \\ \zeta &\mapsto \frac{1}{N}. \end{aligned}$$

Two pairs (E_τ, α) and $(E_{\tau'}, \alpha)$ with τ, τ' in the same connected component of $\mathbf{C} - \mathbf{R}$ are isomorphic if and only if $\tau' = \gamma\tau$ for some $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_1(N)$, and the isomorphism is given by

$$\begin{aligned} (\mathbf{C}/\Lambda_{\gamma\tau}, 1/N) &\to (\mathbf{C}/\Lambda_\tau, 1/N) \\ z &\mapsto (c\tau + d)z, \end{aligned}$$

where $z \in \mathbf{C}$. It follows that the isomorphism class of the triple $(E_\tau, \alpha_\zeta, \omega)$ is precisely the set of triples $\left(E_{\gamma\tau}, \alpha_\zeta, \frac{1}{(c\tau+d)}\omega\right)$ for γ as above. Therefore,

$$f(E_\tau, \alpha_\zeta, \omega) = f\left(E_{\gamma\tau}, \alpha_\zeta, \frac{1}{(c\tau + d)}\omega\right) = (c\tau + d)^{-k} f(E_{\gamma\tau}, \alpha_\zeta, \omega)$$

for all $\gamma \in \Gamma_1(N)$. Defining $F(\tau) = f(E_\tau, \alpha_\zeta, dz)$, we find that F must satisfy

$$F(\gamma\tau) = (c\tau + d)^k F(\tau)$$

for all $\tau \in \mathbf{C} - \mathbf{R}$ and $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_1(N)$, and $F(\tau) = F(-\tau)$. Moreover, F is holomorphic on $\mathbf{C} - \mathbf{R}$ because $f(E_\tau, \alpha_\zeta, dz) \cdot (d\tau)^{\otimes k}$ is a section of the holomorphic "line bundle" of $\omega_{E_\tau/\operatorname{Spec}\mathbf{C}}$'s that arises from the universal *algebraic* elliptic curve over the algebraic curve $Y_1(N)_{\mathbf{C}}$. The condition of "holomorphicity at the cusps" on F follows from the fact that f may be evaluated on generalized elliptic curves (we will say more about this shortly). Using $\zeta = e^{2\pi i/N}$ recovers the classical theory on the connected component of $i = \sqrt{-1}$ in $\mathbf{C} - \mathbf{R}$.

Proposition 2.3.2. *Let $N > 4$ and k be integers and R a ring in which $1/N$ is a unit. Let $(\underline{E} \to X_1(N), \underline{\alpha})$ be the final object of $[\Gamma_1(N)]_R$, and set $\underline{\omega} := \omega_{\underline{E}/X_1(N)}$. Then*

$$M(k, N)_R = H^0(X_1(N)_R, \underline{\omega}_R^{\otimes k}).$$

Proof. This follows easily from Remark 2.2.3. ■

Remark 2.3.3. We would of course like a similar description of $M(k, N)_R$ when $N \leq 4$, but unfortunately the functor of Theorem 2.2.2 is not representable for these values of N. Rather than resort to the language of stacks (see [10] for such an approach), we describe $M(k, N)_R$ when $N \leq 4$ and some integer $n \geq 3$ relatively prime to N is invertible in R (we may suppose this to be the case by working Zariski-locally on R) as follows. The moduli scheme $X(N; n)_R$, classifies triples $(E/S/R, \alpha, \beta)$ where:

- E is a generalized elliptic curve over the R-scheme S,
- α is an embedding of S-group schemes
$$\alpha : \mu_N \to E_N$$
- β is an isomorphism of S-group schemes
$$\beta : (\mathbf{Z}/n\mathbf{Z})^2 \xrightarrow{\sim} E_n$$
- The relative effective Cartier divisor $\alpha + \beta$ is ample on geometric fibers of E over S; i.e. $\alpha(\mu_N) + \beta((\mathbf{Z}/N\mathbf{Z})^2)$ meets all irreducible components of E in all geometric fibers

The scheme $X(N;n)_R$ is smooth and proper over R, and there is a "universal generalized elliptic curve"

$$\pi : \underline{E} \to X(N;n)_R$$

with α, β as above that is a final object in the category of such triples. We define $\underline{\omega}$ as before, and the group $G_n := \mathrm{GL}_2(\mathbf{Z}/n\mathbf{Z})$ acts on the R-module $H^0(X(N;n)_R, \underline{\omega}_R^{\otimes k})$. We define $M(k,N)_R$ as the G_n-invariant submodule:

$$M(k,N)_R := H^0(X(N;n)_R, \underline{\omega}_R^{\otimes k})^{G_n}.$$

That this definition is naturally independent of $n \in R^\times$ with $(n,N) = 1$ and recovers the preceding definition of $M(k,N)_R$ when $N > 4$ must be checked; we omit it.

Definition 2.3.4. A *cusp form* of level N and weight k over R is a modular form over R that vanishes on each degenerate generalized elliptic curve. Equivalently, for $N > 4$, a cusp form is a section of $\underline{\omega}_R^{\otimes k}$ that vanishes along the subscheme of cusps in $X_1(N)_R$. We denote the R-module of cusp forms for $\Gamma_1(N)$ of weight k over R by $S(N,k)_R$; it is a R-submodule of $M(N,k)_R$. We will also refer to cusp forms as *cuspidal* modular forms over R.

Taking $R = \mathbf{C}$, arguments with Serre's GAGA Theorem and the analytic theory shows that this recovers the classical analytic theory of cusp forms.

2.4. **q-expansions.** Over the base $\mathrm{Spec}\,\mathbf{Z}[\![q]\!]$ there is a distinguished generalized elliptic curve $\mathrm{Tate}(q)$ that becomes an elliptic curve after the base change $\mathrm{Spec}\,\mathbf{Z}(\!(q)\!) \to \mathrm{Spec}\,\mathbf{Z}[\![q]\!]$ and has formal group canonically identified with $\widehat{\mathbf{G}}_m$ over $\mathbf{Z}[\![q]\!]$. Its scheme of non-smoothness is cut out by the ideal (q), and it is a regular scheme. Let $\mathrm{Tate}(q^n)^{\mathrm{reg}}$ over $\mathbf{Z}[\![q]\!]$ denote the minimal regular resolution of the base change $\mathrm{Tate}(q^n)$ by $\mathbf{Z}[\![q]\!] \to \mathbf{Z}[\![q]\!]$ defined via $q \mapsto q^n$; this *is* a generalized elliptic curve over $\mathbf{Z}[\![q]\!]$. Over $\mathbf{Z}(\!(q)\!)$, $\mathrm{Tate}(q^n)^{\mathrm{reg}}$ and $\mathrm{Tate}(q^n)$ coincide. The $\mathbf{Z}[\![q]\!]$-module $\omega_{\mathrm{Tate}(q)^{\mathrm{reg}}/\mathbf{Z}[\![q]\!]}$ is equipped with a unique generator ω_{can} that pulls back to dt/t on the formal group $\widehat{\mathbf{G}}_m$. For $N > 4$, the formal completion of the $\mathbf{Z}[1/N]$-scheme $X_1(N)$ along each connected component of the scheme of cusps has the form $\mathrm{Spec}\,\mathbf{Z}[1/N, \zeta_d][\![q]\!]$ or $\mathrm{Spec}\,\mathbf{Z}[1/N, \zeta_d]^+[\![q]\!]$ for various $d|N$, over which the universal generalized elliptic curve is $\mathrm{Tate}(q^{d'})^{\mathrm{reg}}$ for some $d'|(N/d)$, equipped with some $\Gamma_1(N)$-structure α, and its scheme of non-smoothness is cut out by the ideal (q). (In contrast, $\mathrm{Tate}(q^{d'})$ over $\mathbf{Z}[\![q]\!]$ has scheme of non-smoothness cut out by the ideal $(q^{d'})$.) We may evaluate any modular form f for $\Gamma_1(N)$ of weight k over a $\mathbf{Z}[1/N]$-algebra R on the pair $(\mathrm{Tate}(q^d)^{\mathrm{reg}}_{R[\zeta_d]}, \alpha_{R[\zeta_d]})$ to obtain a unique element $f_{d',\alpha}(q) \in \mathbf{Z}[1/N][\![q]\!] \otimes_{\mathbf{Z}} R[\zeta_d]$ such that

$$f(\mathrm{Tate}(q^{d'})^{\mathrm{reg}}_{R[\zeta_d]}, \alpha_{R[\zeta_d]}) = f_{d',\alpha}(q) \cdot {\omega_{\mathrm{can}}}^{\otimes k}_{R[\zeta_d]}.$$

(We write $R[\zeta_d]$ to denote $R \otimes_{\mathbf{Z}} \mathbf{Z}[\zeta_d]$.) We call the power series $f_{d',\alpha}(q)$ the *q-expansion* of f at the cusp corresponding to (d', α). On the $\mathbf{Z}[1/N][\![q]\!]$-scheme of $\Gamma_1(N)$-structures on $\mathrm{Tate}(q)$ there is a connected component $\mathrm{Spec}\,\mathbf{Z}[1/N][\![q]\!]$ corresponding to the $\Gamma_1(N)$-structure $\mu_N \to \mathrm{Tate}(q)^{\mathrm{sm}}$ (and the canonical realization of μ_N as $\widehat{\mathbf{G}}_m[N]$). This gives rise to a *canonical* connected component $\mathrm{Spec}\,\mathbf{Z}[1/N]$ of the scheme of cusps; this cusp is denoted ∞.

For $N > 4$, we may think of the power series $f_{d',\alpha}(q)$ as a description of the section f of $\underline{\omega}^{\otimes k}$ in a formal neighborhood of the corresponding connected component of the cusps in $X_1(N)$ [14, §2]. Over $\mathrm{Spec}\,\mathbf{C}$, it is a nontrivial exercise using the construction of $\mathrm{Tate}(q)$ via formal schemes to check that this definition of q-expansion at a cusp coincides with the one obtained from the analytic theory of modular forms (especially at ∞). One has the so-called "q-expansion principle":

Proposition 2.4.1 (cf. [16, 1.6.1,1.6.2], [14, Prop. 2.7])**.** *Let N, k, and d be integers with $d|N$ and $N > 4$. For any $\mathbf{Z}[1/N]$-algebra R and any any (d', α) as above, the map*

$$H^0(X_1(N)_R, \underline{\omega}_R^{\otimes k}) \to R[\zeta_d][\![q]\!]$$

taking f to its q-expansion at (d', α) is injective. The same holds under composition with projection from $R[\zeta_d]$ to any R-algebra factor ring.

It follows (see [16, Corollary 1.6.2]) that for any $\mathbf{Z}[1/N]$ sub-algebra R_0 of R, a modular form $f \in M(k,N)_R$ lies in the subspace $M(k,N)_{R_0}$ if and only if the q-expansion of f at ∞ is in $R_0[\![q]\!]$.

Remark 2.4.2. By faithful flatness arguments, Definition 2.3.4 can be given using *only* elliptic curves as test objects if we also demand that all q-expansions on $\mathrm{Tate}(q^{d'})$'s over $R[\zeta_d](\!(q)\!)$ as above lie in $R[\zeta_d][\![q]\!]$.

2.5. **Base change.** Let $N > 4, k$ be integers, and R any $\mathbf{Z}[1/N]$-algebra, and R' any R-algebra. Then there is an obvious natural map

$$H^0(X_1(N)_R, \underline{\omega}_R^{\otimes k}) \otimes_R R' \to H^0(X_1(N)_{R'}, \underline{\omega}_{R'}^{\otimes k}) \tag{2.1}$$

Theorem 2.5.1. *If $k \geq 2$ then the map* (2.1) *is an isomorphism of R'-modules.*

Proof. By consideration of $\varinjlim$ and Čech cohomology, we may assume R and R' are noetherian, and then even local (with $R \to R'$ a local map).

For the sake of clarity, we consider the following more general setup. Let $(A, \mathfrak{m}, \kappa)$ and $(A', \mathfrak{m}', \kappa')$ be noetherian local rings, with A' a local A-algebra. Let X be a proper A-scheme, and let X' be the base extension of X to $\operatorname{Spec} A'$. We consider a coherent sheaf $\mathscr{F}$ on X that is flat over A, and denote by $\mathscr{F}'$ the pullback of $\mathscr{F}$ to X'. We denote the closed fibers of X, X' by X_0, X_0', and the pullback of $\mathscr{F}, \mathscr{F}'$ to these schemes by $\mathscr{F}_0, \mathscr{F}_0'$. We claim that to show that the natural map

$$\phi : H^0(X, \mathscr{F}) \otimes_A A' \to H^0(X, \mathscr{F} \otimes A')$$

is an isomorphism, it suffices to prove that $H^1(X_0, \mathscr{F}_0) = 0$. Indeed, suppose this is the case, so likewise (since κ'/κ is flat) $H^1(X_0', \mathscr{F}_0') \simeq \kappa' \otimes_\kappa H^1(X_0, \mathscr{F}_0) = 0$. Then the natural map $H^1(X, \mathscr{F}) \otimes \kappa \to H^1(X_0, \mathscr{F}_0)$ is surjective, hence by [15, Theorem 12.11] (valid in the proper case by the same proof, due to cohomology of higher direct images in the proper case) is an isomorphism. By NAK, we conclude that $H^1(X, \mathscr{F}) = 0$. Therefore, $H^1(X, \mathscr{F})$ is *free*, so by [15, Theorem 12.11] the map $H^0(X, \mathscr{F}) \otimes \kappa \to H^0(X_0, \mathscr{F}_0)$ is surjective, hence an isomorphism. The same holds over A' and κ'. Since $H^{-1}(X_0, \mathscr{F}_0) = 0$, it follows that $H^0(X, \mathscr{F})$ is A-flat, hence A-free. We then have a commutative diagram

$$\begin{tikzcd}
H^0(X', \mathscr{F}') \otimes_{A'} \kappa' \arrow[r] & H^0(X_0', \mathscr{F}_0') \\
(A' \otimes_A H^0(X, \mathscr{F})) \otimes_{A'} \kappa' \arrow[u, "\phi\otimes 1"] \arrow[r] & H^0(X_0, \mathscr{F}_0) \otimes_\kappa \kappa' \arrow[u]
\end{tikzcd}$$

where the horizontal arrows are isomorphisms. As κ'/κ is flat, the right vertical arrow is an isomorphism, so we conclude that $\phi \otimes 1$ is an isomorphism, and then by NAK again that ϕ is an isomorphism.

Returning to our situation of interest, let us show that when $k \geq 2$, we have $H^1(X_1(N)_\kappa, \underline{\omega}_\kappa^{\otimes k}) = 0$ for any field κ in which N is a unit. The Kodaira-Spencer map gives an isomorphism of line bundles [16, A1.3.17]

$$\underline{\omega}_\kappa^{\otimes 2} \simeq \Omega^1_{X_1(N)_\kappa/\kappa}(\mathbf{c}usps_\kappa),$$

so for $k \geq 2$, we have

$$\deg_\kappa \underline{\omega}_\kappa^{\otimes k} \geq \deg_\kappa \Omega^1_{X_1(N)_\kappa/\kappa}(\mathbf{c}usps_\kappa) > \deg \Omega^1_{X_1(N)_\kappa/\kappa} = 2g - 2, \tag{2.2}$$

where g is the genus of $X_1(N)_\kappa$ and we have used the fact that $\mathbf{c}usps_\kappa$ is nonempty. On the other hand, $H^1(X_1(N)_\kappa, \underline{\omega}_\kappa^{\otimes k})$ has the same dimension as $H^0(X_1(N)_\kappa, \Omega^1_{X_1(N)_\kappa/\kappa} \otimes \underline{\omega}_\kappa^{\otimes(-k)})$ by Serre duality. This latter space is 0 as

$$\deg_\kappa \underline{\omega}_\kappa^{\otimes(-k)} + \deg_\kappa \Omega^1_{X_1(N)_\kappa/\kappa} < (2 - 2g) + (2g - 2) = 0.$$

This completes the proof. ■

Remark 2.5.2. When $k = 1$ this map need not be an isomorphism. We will give an explicit example of this in §2.7.

2.6. **Hecke operators.** For any integers N, k, and $\mathbf{Z}[1/N]$-algebra R, there exists a commutative ring $\mathbf{T}_R$ of endomorphisms of the R-module $M(k, N)_R$ generated by *Hecke operators* T_m and diamond operators $\langle d \rangle$ for $d \in (\mathbf{Z}/N\mathbf{Z})^\times$. These operators are defined *algebro-geometrically*, using correspondences on $X_1(N)$ over $\mathbf{Z}[1/N]$ when $N > 4$ (and by the same "trick" of considering modular forms of level $N \leq 4$ as certain invariant sections of $\underline{\omega}^{\otimes k}$ over $X(N; n)$ with $n > 3$ as in Remark 2.3.3), and one computes by using Tate curve families that they agree with the usual Hecke and diamond operators in the classical setting with $R = \mathbf{C}$. In particular, if $a_m(f)$ denotes the coefficient of q^m in the q-expansion of a modular form f at the cusp ∞, then

$$a_1 (T_m(f)) = a_m(f). \tag{2.3}$$

The proof of Theorem 2.5.1 gives $R \otimes_{\mathbf{Z}[1/N]} \mathbf{T}_{\mathbf{Z}[1/N]} \simeq \mathbf{T}_R$ when $k \geq 2$. We will denote by $\mathbf{T}$ the flat $\mathbf{Z}$-algebra generated by these operators inside $\mathbf{T}_{\mathbf{Z}[1/N]}$; by using a stronger theory over $\mathbf{Z}$ (not just $\mathbf{Z}[1/N]$) one sees that this ring is $\mathbf{Z}$-finite. We refer the reader to [4, §4.5] for the construction and properties of the ring $\mathbf{T}$. One may also consult [14, §3] and [11] for a discussion of some of the subtleties involved.

Definition 2.6.1. Let $N \geq 1$ and k be integers, R any ring in which N is a unit, and

$$\varepsilon : (\mathbf{Z}/N\mathbf{Z})^{\times} \to \overline{\mathbf{F}}_p^{\times}$$

any character. An *eigenform of type* (N, k, ε) over R is an element $f \in M(k, N)_R$ that is an eigenform for all Hecke operators T_m, and such that the diamond operators $\langle d \rangle$ act on f via

$$\langle d \rangle f = \varepsilon(d) f.$$

We moreover say that f is *normalized* if $a_1(f) = 1$. Often the ring R will be implicit, and will not be mentioned.

2.7. **Modular forms** $(\operatorname{mod} p)$**.** Fix a prime p and let $N \geq 1$ be any integer not divisible by p. By a *modular form* $(\operatorname{mod} p)$, we mean an element of $M(k, N)_F$ for a field F of characteristic p. It follows from Theorem 2.5.1 that for $k \geq 2$, the space $M(k, N)_{\mathbf{F}_p}$ is just the reduction mod p of $M(k, N)_{\mathbf{Z}[1/N]}$. When $k = 1$ this is sometimes not, in fact, the case:

Example 2.7.1. There is an important modular form $A \in M(p-1, 1)_{\mathbf{F}_p}$ called the *Hasse invariant*, which we construct as follows. For an elliptic curve $\pi : E \to S$ with S a scheme of characteristic p, the relative Frobenius morphism

$$\begin{tikzcd}
E \arrow[rr, "F_{E/S}"] \arrow[dr, "\pi"'] & & E^{(p)} \arrow[dl, "\pi^{(p)}"] \\
& S &
\end{tikzcd}$$

gives an $\mathscr{O}_S$-linear pullback map on cohomology

$$F_{E/S}^{*} : R^1\pi_*^{(p)}\mathscr{O}_{E^{(p)}} \to R^1\pi_*\mathscr{O}_E \tag{2.4}$$

which a calculation [15, 4.2.1] shows to be zero for only finitely many elliptic curves over $\overline{\mathbf{F}}_p$ (the supersingular ones). Dualizing, and using the canonical duality between $R^1\pi_*\mathscr{O}_E$ and $\omega_{E/S}$, we obtain an $\mathscr{O}_S$-linear map

$$\omega_{E/S} \to \omega_{E^{(p)}/S}.$$

As the formation of $\omega_{E/S}$ is compatible with base change, we have $\omega_{E/S}^{(p)} \simeq F_S^*\omega_{E/S}$, (with $F_S : S \to S$ the absolute Frobenius map). For any line bundle $\mathscr{L}$ on an $\mathbf{F}_p$-scheme S we have canonically $F_S^*\mathscr{L} \simeq \mathscr{L}^{\otimes p}$, as may be checked by an explicit calculation with trivializing data of the invertible sheaf $\mathscr{L}$. Thus, we have an $\mathscr{O}_S$-linear morphism

$$\omega_{E/S} \to \omega_{E/S}^{\otimes p},$$

which we interpret as a map $\mathscr{O}_S \to \omega_{E/S}^{\otimes(p-1)}$; that is, as a section of $\omega_{E/S}^{\otimes(p-1)}$. We define A to be the rule that associates to any elliptic curve E/S this section. An explicit calculation [16, 2.0] on $\mathrm{Tate}(q)/\mathbf{F}_p((q))$ shows that $A(\mathrm{Tate}(q)/\overline{\mathbf{F}}_p((q)), \alpha, \omega_{\mathrm{can}}) = 1$ for every α. Hence, by Remark 2.4.2, this is therefore a modular form of level 1 and weight $p-1$ over $\mathbf{F}_p$.

For $p = 2, 3$, we note that the Hasse invariant provides an example of a modular form over $\overline{\mathbf{F}}_p$ that does not lift to a modular form over $\overline{\mathbf{Z}}_{(p)}$ (and likewise over a p-adic localization of $\overline{\mathbf{Z}}$). Indeed, there are no nonzero modular forms over $\mathbf{C}$ of weight less than 4 and level 1 (and hence none over $\overline{\mathbf{Q}}$ or $\mathbf{Q}$).

Define

$$M(N) := \bigoplus_{k \geq 0} M(k, N)_{\overline{\mathbf{F}}_p};$$

it is a graded $\overline{\mathbf{F}}_p$-algebra. This has a descending homogenous filtration by the subspaces $A^i M(N)_{\overline{\mathbf{F}}_p}$ for $i \geq 0$. We denote by $S(N)$ the $\overline{\mathbf{F}}_p$-subalgebra of $M(N)$ with k^{th} graded piece equal to $S(k, N)_{\overline{\mathbf{F}}_p}$

Definition 2.7.2. The *filtration* $w(f)$ of an element $f \in M(k,N)_{\overline{\mathbf{F}}_p}$ is the minimal weight $k' = k - i(p-1)$ such that $f \in A^i M(k',N)_{\overline{\mathbf{F}}_p}$. In words, when we view f as a section of $\underline{\omega}_{\overline{\mathbf{F}}_p}^{\otimes k}$ on $X_1(N)_{\overline{\mathbf{F}}_p}$, the integer $i \leq k/(p-1)$ is taken as large as possible without exceeding the order of f at the supersingular points (at which the section A of $\underline{\omega}_{\overline{\mathbf{F}}_p}^{\otimes(p-1)}$ has simple zeros, by a deformation theory argument [18]).

Proposition 2.7.3. *The kernel of the $\overline{\mathbf{F}}_p$-algebra homomorphism*

$$M(N) \to \overline{\mathbf{F}}_p[\![q]\!] \tag{2.5}$$

that takes $f \in M(k,N)_{\overline{\mathbf{F}}_p}$ to its q-expansion at ∞ is the principal ideal $(A-1)M(N)$.

We first prove a general lemma.

Lemma 2.7.4. *Let X be a proper normal connected scheme over a base ring R and $\mathscr{L}$ an ample line bundle on X. Put $S = \oplus_{n\geq 0} H^0(X, \mathscr{L}^n)$ and let s be a global section of $\mathscr{L}^k$ for some $k > 0$ that is a unit in R. If the section s has at least one simple zero then $s-1$ generates a prime ideal in S.*

Proof. Since $\mathscr{L}^k$ is ample, the subset X_s of X where s generates $\mathscr{L}^k$ is affine, and by Chapter 2, Lemma 5.14 of [15], the natural map of graded rings

$$S[1/s] \to \bigoplus_{n\in\mathbf{Z}} H^0(X_s, \mathscr{L}^n)$$

is an isomorphism. The closed subset $V(s-1) \subset \operatorname{Spec} S$ obviously lies inside $\operatorname{Spec} S[1/s]$, and corresponds to the subset $Z := V(s-1) \subset \operatorname{Spec} H^0(X_s, \oplus_{n\in\mathbf{Z}}\mathscr{L}^n)$. Restricting to an open affine subset $\operatorname{Spec} A$ of X_s where $\mathscr{L}$ is trivial, say with generator T, we identify $H^0(X_s, \oplus_{n\in\mathbf{Z}}\mathscr{L}^n)$ with $A[T,1/T]$ and the section $s-1$ corresponds to $uT^k - 1$ for some unit $u \in A^\times$. Since k is a unit on the base, we see that Z is étale over $\operatorname{Spec} A$, hence over X_s and consequently over X as well. Since X is normal, Serre's "$R_1 + S_2$" criterion implies that Z is normal.

We claim that Z is furthermore connected. Since X_s is irreducible, the various $\operatorname{Spec} A$'s as above have nontrivial intersections, so it is enough to show that the scheme $\operatorname{Spec} A[T,1/T]/(uT^k-1) \simeq \operatorname{Spec} A[z]/(z^k-u)$ is connected for $u \in A^\times$. As we have seen, each connected component of $\operatorname{Spec} A[z]/(z^k-u)$ is étale over $\operatorname{Spec} A$, so contributes at least one point to the generic fiber; whence we can check connectivity by verifying that it holds on the generic fiber. We thus wish to show that $z^k - u \in A[z]$ is irreducible over the fraction field F of the normal domain A. But the generic points of the zero scheme of s have codimension 1 by the Hauptidealsatz, and since X is normal the local rings at such points are discrete valuation rings. By hypothesis, s has a simple zero, so the zero scheme of s is cut out by a uniformizer in one of these local rings $\mathscr{O}_{X,x}$. Considering F as the fraction field of $\mathscr{O}_{X,x}$, the element $u \in F$ is a uniformizer of $\mathscr{O}_{X,x}$, whence $z^k - u$ is irreducible over F by Eisenstein's criterion.

Since Z is therefore connected and normal, the ideal $(s-1)S$ is prime. ■

Proof of proposition 2.7.3. If $N > 4$, we proceed as follows. Since $\underline{\omega}$ is ample by the calculation (2.2), one has an isomorphism

$$X_1(N)_{\overline{\mathbf{F}}_p} \simeq \operatorname{Proj} \bigoplus_{k\geq 0} H^0(X_1(N)_{\overline{\mathbf{F}}_p}, \underline{\omega}_{\overline{\mathbf{F}}_p}^{\otimes k}),$$

and since $X_1(N)_{\overline{\mathbf{F}}_p}$ is a curve, we see that the graded algebra $M(N) = \bigoplus_{k\geq 0} H^0(X_1(N)_{\overline{\mathbf{F}}_p}, \underline{\omega}_{\overline{\mathbf{F}}_p}^{\otimes k})$ has Krull dimension 2. It is clear that the ideal $(A-1)M(N)$ is in the kernel of the above map. The modular form $\Delta \in M(12,1)_{\overline{\mathbf{F}}_p} \subseteq M(12,N)_{\overline{\mathbf{F}}_p}$ has q-expansion $q + \ldots$ at ∞, so the image of the map (2.5) has dimension at least 1. Since A vanishes to order 1 at the supersingular points, the ideal $(A-1)M(N)$ is prime by Lemma 2.7.4, so for dimension reasons the kernel of (2.5) cannot properly contain it and the proposition follows. For $N \leq 4$, the same proof will work after using the trick of Remark 2.3.3; we omit the details. ■

By using other methods, there is a unique $\overline{\mathbf{F}}_p$-linear derivation

$$\theta : M(N) \to M(N)$$

that increases degrees by $p+1$ and has the effect

$$\begin{aligned} q\frac{d}{dq} : \overline{\mathbf{F}}_p[\![q]\!] &\to \overline{\mathbf{F}}_p[\![q]\!] \\ \sum a_m q^m &\mapsto \sum m a_m q^m \end{aligned}$$

on q-expansions at every cusp [17] (the proof herein carries over to our situation verbatim). Moreover, one checks that θ preserves the sub-algebra $S(N)$ and that for all primes ℓ (including $\ell = p$)

$$T_\ell(\theta f) = \ell\theta(T_\ell f). \tag{2.6}$$

It follows from (2.6) that if f is a normalized eigenform of type (N, k, ε) with eigenvalues a_ℓ (i.e. $T_\ell f = a_\ell f$ for all ℓ) then θf is an eigenform of type $(N, k+p+1, \varepsilon)$ with eigenvalues ℓa_ℓ.

3. Two dimensional Galois representations

In this section, we recall some properties of continuous 2-dimensional $(\bmod\, p)$ Galois representations that will be essential for our later considerations. We fix a prime p and a continuous two-dimensional Galois representation (ρ, V) for the remainder of this section.

3.1. **Artin conductor.** Fix a prime ℓ (not necessarily distinct from p). Since ρ is continuous with target having the discrete topology, we infer that the kernel of ρ is open and hence of finite index in $G_{\mathbf{Q}}$. It follows that the image of ρ is isomorphic to $G := \mathrm{Gal}(F/\mathbf{Q})$ for some finite Galois extension F of $\mathbf{Q}$. Fix a choice of prime $\mathfrak{l}$ of L over ℓ and let $G_\ell \subseteq G$ be the corresponding decomposition group at ℓ:

$$G_\ell := \{\sigma \in G \ : \ \sigma\mathfrak{l} = \mathfrak{l}\}.$$

Note that different choices of $\mathfrak{l}$ yield conjugate decomposition groups (so our abuse of notation G_ℓ is justifiable as we are ultimately only concerned with isomorphism classes of representations). By definition, every $\sigma \in G_\ell$ preserves the valuation on F associated to $\mathfrak{l}$, and so extends uniquely to an automorphism of the $\mathfrak{l}$-adic completion $F_{\mathfrak{l}}$ of F that moreover fixes $\mathbf{Q}_\ell$ (as $\mathbf{Q}$ is dense in $\mathbf{Q}_\ell$). We then easily deduce the identification

$$G_\ell \simeq \mathrm{Gal}(\overline{F}_{\mathfrak{l}}/\mathbf{Q}_\ell),$$

and we may view the restriction of ρ to G_ℓ as a continuous homomorphism

$$\rho_\ell : \mathrm{Gal}(F_{\mathfrak{l}}/\mathbf{Q}_\ell) \to \mathrm{GL}(V) \simeq \mathrm{GL}_2(\overline{\mathbf{F}}_p).$$

Recall [26, IV, §3] that one has a descending chain of subgroups

$$G_\ell = G_{\ell,-1} \supseteq G_{\ell,0} \supseteq G_{\ell,1} \supseteq \cdots \supseteq G_{\ell,i} \cdots,$$

where

$$G_{\ell,i} := \ker\left(\mathrm{Aut}(\mathscr{O}_{F_{\mathfrak{l}}}) \to \mathrm{Aut}(\mathscr{O}_{F_{\mathfrak{l}}}/\mathfrak{l}^{i+1})\right) \tag{3.1}$$

is the i^{th} ramification group of Γ (in the usual lower numbering).

Denote by V_i the subspace of V fixed by $G_{\ell,i}$, and define

$$n(\ell, \rho) := \sum_{i \geq 0} \frac{1}{[G_{\ell,0} : G_{\ell,i}]} \dim(V/V_i). \tag{3.2}$$

Then it can be shown [26, VI,§2] that $n(\ell, \rho) \geq 0$ is an *integer* depending only on ℓ, ρ, V. Moreover, it is easy to see that $n(\ell, \rho) = 0$ if and only if $V_0 = V$ (i.e. ρ is unramified at ℓ) and $n(\ell, \rho) = \dim V/V_0$ if and only if $V_1 = V$ (i.e. ρ is tamely ramified at ℓ). Since ρ is continuous (in particular, unramified outside a finite set of primes) we may make the following definition:

Definition 3.1.1. The *conductor* of ρ is the integer

$$N(\rho) := \prod_{\ell \neq p} \ell^{n(\ell,\rho)}.$$

It is clear from our discussion that, away from p, the representation ρ is ramified at precisely those primes dividing $N(\rho)$. Observe that $N(\rho)$ is the "prime to p" part of the Artin conductor as defined in characteristic zero.

3.2. **Structure of local Galois groups.** As we will make a close study of the local representation $\rho_p : G_p \to \mathrm{GL}(V)$ *at* p we first recall the structure of the group G_p. We proceed (slightly) more generally by recalling the structure of $G_K := \mathrm{Gal}(K^{\mathrm{sep}}/K)$ for field K of characteristic 0, complete with respect to a (normalized) discrete valuation, with residue field k of characteristic $p > 0$. Let $\mathbf{F}_q \subset k^{\mathrm{sep}}$ be the subfield of order q for each $q = p^m$ with $m \geq 1$.

One has the following tower of field extensions and corresponding Galois groups:

$$\begin{tikzcd}
K^{\mathrm{sep}} \arrow[d, dash, "I_p"] \arrow[dd, dash, bend left, "I"] \arrow[ddd, dash, bend right, "G_K"'] \\
K^{\mathrm{t}} \arrow[d, dash, "I_t"] \\
K^{\mathrm{un}} \arrow[d, dash] \\
K
\end{tikzcd}$$

Here I is the *inertia* subgroup of G_K and I_p is the largest pro-p subgroup of I, the so-called *wild inertia* subgroup. One has the identification $G_K/I \simeq \mathrm{Gal}(k^{\mathrm{sep}}/k)$. Notice that $I \lhd G_K$ and $I_p \lhd G_K$ since K^{un}/K and K^{t}/K are Galois extensions, and that $I_t = I/I_p$ is a pro-cyclic "prime to p" group (i.e. every finite discrete quotient of I_t is cyclic with order prime to p). The normality of I and I_p in G_K ensures that G_K acts on I and I_p via conjugation, and that this action descends to the quotient $I_t = I/I_p$. Since I/I_p is abelian, this action descends to an action of $G_K/I \simeq \mathrm{Gal}(k^{\mathrm{sep}}/k)$.

For a fixed choice of uniformizer π of K^{un} we have the explicit description

$$K^{\mathrm{t}} = \varinjlim_{p \nmid n} K^{\mathrm{un}}(\pi^{1/n}). \tag{3.3}$$

If k is finite then

$$K^{\mathrm{un}} = \varinjlim_{p \nmid n} K(\zeta_n).$$

We obtain an inverse system of maps

$$\begin{aligned} \theta_n : \mathrm{Gal}(K^{\mathrm{t}}/K^{\mathrm{un}}) &\to \mu_n(K^{\mathrm{un}}) = \mu_n(k^{\mathrm{sep}}) \\ s &\mapsto \frac{s(\pi^{1/n})}{\pi^{1/n}} \end{aligned} \tag{3.4}$$

which yields the identification

$$I_t = \mathrm{Gal}(K^{\mathrm{t}}/K^{\mathrm{un}}) = \varprojlim_{p \nmid n} \mu_n(K^{\mathrm{un}}) = \varprojlim_{p \nmid n} \mu_n(k^{\mathrm{sep}}); \tag{3.5}$$

moreover, a simple calculation given in [22, 2.2.2] shows this is an identification of $\mathrm{Gal}(k^{\mathrm{sep}}/k)$-modules. For $q = p^m$, the group $\mu_{q-1}(k^{\mathrm{sep}})$ *is* $\mathbf{F}_q^\times$, and as the partially ordered set of integers $\{p^m - 1 | m \geq 1\}$ is cofinal with the set of positive integers prime to p (where both sets are ordered by divisibility), the maps θ_{q-1} give an identification of $\mathrm{Gal}(k^{\mathrm{sep}}/k)$-modules

$$I_t = \varprojlim_{q} \mathbf{F}_q^\times \tag{3.6}$$

with surjective transition maps $\mathbf{F}_{q^m}^\times \to \mathbf{F}_q^\times$ given by

$$\zeta \mapsto \zeta^{(q^m-1)/(q-1)} = \mathrm{Nm}_{\mathbf{F}_{q^m}/\mathbf{F}_q}(\zeta)$$

for $m \geq 1$.

3.3. **The local representation at p.** We now study more closely the local representation ρ_p. As above, we follow [25] and proceed more generally by studying representations $\rho : G_K \to \mathrm{GL}(V)$ of G_K for K as before, with V a 2-dimensional vector space over an algebraically closed field k' of characteristic p.

Proposition 3.3.1. *Let V^{ss} denote the semi-simplification of V as a G_K-module (i.e., the direct sum of the Jordan-Hölder constituents of V). Then I_p acts trivially on V^{ss}.*

Proof. As we need only prove that I_p acts trivially on the direct summands of V^{ss}, we reduce at once to the case that $V = V^{\mathrm{ss}}$ is *simple*. The continuity of ρ ensures that ρ kills an open (hence finite index) subgroup of G_K, so that ρ factors through a finite discrete quotient. As I_p is pro-p, the image $\rho(I_p)$ is a finite p-group. Let $W = V^{I_p}$ be the subspace on which I_p acts trivially. Since W is a p-torsion abelian group on which a finite p-group acts continuously, we have $W \neq 0$ by elementary group theory ($0 \in W$ and the orbits in W have p-power size, so there are at least $p-1$ other singleton orbits). But I_p is a *normal* subgroup of G_K, so W is a nontrivial G_K-stable subspace of V; since V is simple by hypothesis, $W = V$ and I_p acts trivially on V. ■

By Proposition 3.3.1, $I_t = I/I_p$ acts on V^{ss}. The identification (3.5) shows that I_t is *abelian*, and hence (since k' is algebraically closed) that I_t acts on V^{ss} via two (continuous) characters

$$\varphi, \varphi' : I_t \to {k'}^{\times} \tag{3.7}$$

We are thus motivated to understand the group $\mathrm{Hom}_{\mathrm{cont}}\left(I_t, {k'}^{\times}\right)$.

Definition 3.3.2. Let $\phi : I_t \to {k'}^{\times}$ be any continuous character. We say ϕ is of *level m* if m is the smallest integer for which there is a factorization

$$\begin{tikzcd}
I_t \simeq \varprojlim_m \mathbf{F}_{p^m}^{\times} \arrow[rr, "\phi"] \arrow[dr] & & {k'}^{\times} \\
& \mathbf{F}_{p^m}^{\times} \arrow[ur] &
\end{tikzcd}$$

The continuity of ϕ ensures that such an m exists, and clearly the level of ϕ is a factor of any other such m.

There is a convenient set of generators for the group of characters of I_t of level m that we now describe.

Definition 3.3.3. Let k' be an algebraically closed field of characteristic $p > 0$, and let K be as above. Let $q = p^m$. A *fundamental character* of I_t of level m with values in k' is a character that is the composition of

$$\theta_{q-1} : I_t \twoheadrightarrow \mu_{q-1}(K^{\mathrm{un}}) \simeq \mathbf{F}_q^{\times}$$

with an $\mathbf{F}_p$-embedding of fields $\mathbf{F}_q \hookrightarrow k'$. Here, θ_{q-1} is the map defined by (3.4). Clearly there are m fundamental characters of level m with values in ${k'}^{\mathrm{sep}}$.

Example 3.3.4. Recall that the *cyclotomic character* $\chi : G_p \to \mathrm{Aut}(\mu_p) \simeq \mathbf{F}_p^{\times}$ is the character giving the action of G_p on the p^{th} roots of unity; as $\mathbf{Q}_p(\zeta_p)/K$ is tamely ramified, χ gives a character of I_t. We claim χ is the unique fundamental character of level 1 in this case (this is generally false for local fields with absolute ramification degree greater than 1). Following Serre [25], for any $\alpha \in \mathbf{Q}$ we define the one-dimensional $\overline{\mathbf{F}}_p$ vector space

$$V_\alpha = \mathfrak{m}_\alpha / \mathfrak{m}_\alpha^{+},$$

where $\mathfrak{m}_\alpha$ is the $\overline{\mathbf{Z}}_p$-module of $x \in \overline{\mathbf{Q}}_p$ satisfying $v(x) \geq \alpha$ and $\mathfrak{m}_\alpha^{+}$ is the submodule consisting of those $x \in \mathfrak{m}_\alpha$ with $v(x) > \alpha$. The space V_α is equipped with an action of G_p whose restriction to I is *linear* (as I is the kernel of the surjection $G_p \twoheadrightarrow \mathrm{Gal}(\overline{\mathbf{F}}_p/\mathbf{F}_p)$), hence given by a character $\varphi_\alpha : I \to \overline{\mathbf{F}}_p^{\times}$ that moreover kills I_p as $\overline{\mathbf{F}}_p^{\times}$ has trivial p-torsion. Since $p^{1/(p-1)}$ is a basis of $V_{1/(p-1)}$, we find that $\varphi_{1/(p-1)} = \theta_{p-1}$ (as characters of I_t) by the definition of θ_{p-1}. But the homomorphism $\mu_p \to V_{1/(p-1)}$ given by $\zeta \mapsto \zeta - 1$ is an injective morphism of Galois-modules, so the Galois action on μ_p is that of the action on $V_{1/(p-1)}$, whence the claim.

Let us return to our original situation of interest, where $K = \mathbf{Q}_p$, and k' is an algebraic closure of $\mathbf{F}_p$; we set $G_p = \mathrm{Gal}(\overline{\mathbf{Q}}_p/\mathbf{Q}_p)$.

Proposition 3.3.5. *Let φ, φ' be the characters giving the action of I_t on V^{ss} as in* (3.7)*. Then one of the following two possibilities holds:*

(1) *φ, φ are of level one, and $\varphi^p = \varphi$ and $(\varphi')^p = \varphi'$.*
(2) *φ, φ have level two, and $\varphi^p = \varphi'$ and $(\varphi')^p = \varphi$.*

Proof. Because of the identification (3.6) of I_t and $\varprojlim_q \mathbf{F}_q^\times$ as $\mathrm{Gal}(\overline{\mathbf{F}}_p/\mathbf{F}_p)$-modules, for any $\sigma \in G_p$ lifting $\mathrm{Frob}_p \in \mathrm{Gal}(\overline{\mathbf{F}}_p/\mathbf{F}_p)$ the conjugation action of σ on I_t is given by $u \mapsto u^p$. It follows that the set $\{\varphi, \varphi'\}$ is stable under the p-th power map, as claimed. ■

4. Galois representations arising from modular forms $(\bmod\, p)$

4.1. **Some existence results.** In order to motivate the precise form of Serre's conjecture that we will state in Section 5, we examine the properties of 2-dimensional $(\bmod\, p)$ representations arising from modular forms $(\bmod\, p)$. We state several deep theorems due to Deligne, Fontaine, and Carayol without proof. Throughout this section, we fix a cuspidal normalized eigenform f of type (N, k, ε) with $p \nmid N$ and eigenvalues a_ℓ.

Theorem 4.1.1 (Deligne)**.** *There exists a continuous, semi-simple Galois representation*

$$\rho_f : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathrm{GL}_2(\overline{\mathbf{F}}_p)$$

characterized by:

(1) *The representation ρ_f is unramified at all primes $\ell \nmid Np$.*
(2) *The matrix $\rho_f(\mathrm{Frob}_\ell)$ has characteristic polynomial $x^2 - a_\ell x + \varepsilon(\ell)\chi^{k-1}(\ell)$.*

Note in particular that $\det \rho_f = \varepsilon\chi^{k-1}$ by the Cebotarev density theorem, so $(\det \rho_f)(-1) = \varepsilon(-1)\chi(-1)^{k-1} = -1$, where we have used the fact that $\varepsilon(-1) = (-1)^k$ (since $\varepsilon(-1)f = \langle -1 \rangle f = (-1)^k f$ and $f \neq 0$).

We remark that if f has weight one, then Af is a modular form of type (N, p, ε) with the same q-expansion as f, since the Hasse invariant A has level 1 and weight $p-1$. Thus, for the purpose of proving Theorem 4.1.1, it is no loss of generality to suppose that $k \geq 2$, whence there is a lift of f to an eigenform in characteristic 0 by the Deligne–Serre lifting lemma [9, Lemme 6.11].

Proof. See [8] for the case $N = 1$ and [2] in general (using Hilbert modular forms). ■

The *weak form* of Serre's conjecture is a converse to Theorem 4.1.1, accounting for oddness.

Conjecture 4.1.2. *For any continuous odd irreducible representation $\rho : G_{\mathbf{Q}} \to \mathrm{GL}_2(\overline{\mathbf{F}}_p)$, there exists a cuspidal eigenform g such that $\rho_g \simeq \rho$.*

Observe that this conjecture says nothing about the weight, level, or character of g.

4.2. **Some local descriptions.**

Theorem 4.2.1 (Deligne)**.** *Suppose $k \geq 2$ and $a_p \neq 0$. Then $\rho_{f,p}$ is reducible, and up to conjugation in $\mathrm{GL}_2(\overline{\mathbf{F}}_p)$, we have*

$$\rho_{f,p} = \begin{pmatrix} \chi^{k-1}\lambda(\epsilon(p)/a_p) & * \\ 0 & \lambda(a_p) \end{pmatrix},$$

where $\lambda(a)$ is the unramified character of G_p taking $\mathrm{Frob}_p \in G_p/I$ to a, for any $a \in \overline{\mathbf{F}}_p^\times$.

Proof. See [14, §12] for a proof when $p \geq k$. The general case is treated in an unpublished letter from Deligne to Serre. ■

Theorem 4.2.2 (Fontaine)**.** *Suppose $k \geq 2$ and $a_p = 0$. Then $\rho_{f,p}$ is irreducible, and up to conjugation*

$$\rho_f\big|_I = \begin{pmatrix} {\psi'}^{k-1} & 0 \\ 0 & \psi^{k-1} \end{pmatrix},$$

where $\psi, \psi' : I_t \to \overline{\mathbf{F}}_p^\times$ are the two fundamental characters of level 2 *(viewed as characters of I via the natural surjection $I \to I/I_p = I_t$).*

Proof. See [10, §6]. ■

Theorem 4.2.3 (Carayol)**.** *Let $N(\rho)$ be as in Definition 3.1.1. Then $N(\rho_f)|N$.*

Proof. See [3]. ∎

It follows from (2.6) and our discussion of the derivation $\theta : M(N) \to M(N)$ that θf has type $(N, k+p+1, \varepsilon)$ and eigenvalues ℓa_ℓ. Since the cyclotomic character χ satisfies $\chi(\mathrm{Frob}_\ell) \equiv \ell (\bmod\, p)$ for all $\ell \neq p$, we see by the Brauer-Nesbitt Theorem and the identity $\det \rho_f = \chi^{k-1}\varepsilon$ that

$$\rho_{\theta f} = \rho_f \otimes \chi.$$

Concerning these "twists by χ," one has the following theorem:

Theorem 4.2.4. *There exist integers i, k' with $0 \leq i \leq p-1$ and $k' \leq p+1$ and an eigenform g of type (N, k', ε) such that*

$$\rho_f \simeq \rho_{\theta^i g} \simeq \rho_g \otimes \chi^i.$$

Proof. See [10, Theorem 3.4]. ∎

This last theorem is very important: up to twists by χ, we "only" need to consider modular forms $(\bmod\, p)$ in weight at most $p+1$.

5. Serre's recipe

In this section, we fix an odd irreducible continuous 2-dimensional $(\bmod\, p)$ Galois representation $\rho : G_{\mathbf{Q}} \to \mathrm{GL}(V) \simeq \mathrm{GL}(\overline{\mathbf{F}}_p)$.

5.1. Some definitions.

Definition 5.1.1. Let ρ be as above. We say that ρ is *modular* if there exists a cuspidal eigenform f with $\rho \simeq \rho_f$. If f has level N, weight k, and character ε, we will say that ρ has *type* (N, k, ε).

Definition 5.1.2. If ρ is modular, then we say ρ has *minimal type* (N, k, ε) if ρ is modular of type (N, k, ε) and whenever ρ is modular of type (N', k', ε') we have $N' \geq N$ and $k' \geq k$.

Let ρ be as above. Serre's conjecture asserts that ρ is modular, and gives a recipe for determining a minimal type (N, k, ε) or ρ. It is *not a priori* evident that a modular representation ρ has a minimal type. In this section, we carefully state and try to motivate Serre's formulae prescribing the minimal type (N, k, ε) of ρ. We follow [11], and note that our definition of the minimal weight $k(\rho)$ differs from Serre's [24]; this amounts to the fact that we deal with modular forms in the sense of Katz, as explained in Section 2, and not with the forms Serre considers, which are by definition those forms obtained by reduction $(\bmod\, p)$ (i.e. forms in the space $M(k, N)_{\overline{\mathbf{Z}}} \otimes_{\overline{\mathbf{Z}}} \overline{\mathbf{F}}_p$).

5.2. The level. Let ρ be as above, and let $N(\rho)$ be as in Definition 3.1.1. By Theorem 4.2.3, if ρ is modular of type (N, k, ε), then $N(\rho)|N$. If one were to be optimistic, then one would conjecture that the minimal level of ρ is *exactly* $N(\rho)$, and this is what Serre conjectures.

5.3. The character and $k(\bmod\, p-1)$. Associated to ρ we have the character

$$\det \rho : G_{\mathbf{Q}} \to \overline{\mathbf{F}}_p^\times.$$

Since ρ is continuous, the image of $\det \rho$ is a finite subgroup of $\overline{\mathbf{F}}_p^\times$. One can show [11, §1] that the character $\det \rho$ has conductor dividing $pN(\rho)$, and therefore may be interpreted as a character

$$(\mathbf{Z}/pN(\rho)\mathbf{Z})^\times \to \overline{\mathbf{F}}_p^\times.$$

Since $p \nmid N(\rho)$, there is a canonical isomorphism

$$(\mathbf{Z}/pN(\rho)\mathbf{Z})^\times \simeq (\mathbf{Z}/N(\rho)\mathbf{Z})^\times \times (\mathbf{Z}/p\mathbf{Z})^\times, \tag{5.1}$$

and we define the character $\varepsilon(\rho)$ to be the restriction of $\det \rho$ to $(\mathbf{Z}/N(\rho)\mathbf{Z})^\times$. Moreover, since the character group $\mathrm{Hom}((\mathbf{Z}/p\mathbf{Z})^\times, \mathbf{F}_p^\times)$ is cyclic of order $p-1$, generated by the cyclotomic character χ, the restriction of $\det \rho$ to $(\mathbf{Z}/p\mathbf{Z})^\times$ is of the form χ^h for some $h \in \mathbf{Z}/(p-1)\mathbf{Z}$. We define $k(\rho)(\bmod\, p-1)$ to be $h+1$.

These definitions are of course motivated by Theorem 4.1.1. When ρ is modular of type (N, k, ε), we have $\det \rho = \varepsilon\chi^{k-1}$, and the conductor of ρ divides pN. We interpret $\det \rho$ as a character $(\mathbf{Z}/pN\mathbf{Z})^\times$, and we see easily that ε *is* the restriction of $\det \rho$ to $(\mathbf{Z}/N\mathbf{Z})^\times$ and χ^{k-1} is the restriction to $(\mathbf{Z}/p\mathbf{Z})^\times$ under the canonical isomorphism, so $k \equiv k(\rho) (\operatorname{mod} p-1)$

5.4. **The weight.** In this section, we the recipe for the minimal weight $k(\rho)$ of ρ.

Let ρ, V be as above, and let ρ_p, I, I_p, I_t be as in Section 3.2. We saw in 3.3 that I_t acts on V^{ss} via two characters φ, φ' that by Proposition 3.3.5 have level 1 or 2. We let ψ, ψ' denote the two fundamental characters of level 2, as in Definition 3.3.3, and as usual χ is the cyclotomic character (i.e. the unique fundamental character of level 1).

Before we can define the integer $k(\rho)$, we need to recall the notion of "finite at p".

Definition 5.4.1. With ρ, V as above, we say that ρ is *finite at* p if there exists a finite flat group scheme $\mathscr{G}$ over $\mathbf{Z}_p$ equipped with an action by a finite field $\kappa \subseteq \overline{\mathbf{F}}_p$ such that $V \simeq \overline{\mathbf{F}}_p \otimes_\kappa \mathscr{G}(\overline{\mathbf{Q}}_p)$. By Raynaud's work [30], it is equivalent to pick *any* descent of (ρ, V) to a representation space over a finite field (which we may do by continuity) and to demand that the underlying finite Galois-module is the $\mathbf{Q}_p$-fiber of a finite flat $\mathbf{Z}_p$-group.

Define the integer $k(\rho)$ as follows:

(1) Suppose φ, φ' have level 2. We claim that ρ_p is automatically irreducible. If this were not the case, V would have a stable one-dimensional subspace, and the action on this subspace would be given by one of the characters φ, φ', which would therefore extend to a tame character of G_p. But the restriction of any tame character of G_p to I takes values in $\mathbf{F}_p^\times$ because any lift $\sigma \in G_p$ of $\mathrm{Frob}_p \in \mathrm{Gal}(\overline{\mathbf{F}}_p/\mathbf{F}_p) \simeq G_p/I$ acts via conjugation on I_t as the p^{th}-power map. This contradicts the hypothesis that φ, φ' have level 2. It follows that ρ is simple, so I_p acts trivially by Proposition 3.3.1. By normality, $\rho\big|_I$ is semisimple and we have
$$\rho_p\big|_I = \rho\big|_{I_t} = \begin{pmatrix} \varphi & 0 \\ 0 & \varphi' \end{pmatrix}.$$
We may uniquely write $\varphi = \psi^a \psi'^b$ and $\varphi' = \varphi^p = \psi'^a \psi^b$ for $0 \le a, b \le p-1$. Observe that we cannot have $a = b$, for in this case $\varphi = (\psi\psi')^a = \chi^a$ has level 1, contrary to our hypothesis. Thus, after exchanging φ, φ' if necessary, we can arrange that $0 \le a < b \le p-1$, and we define $k(\rho) = 1 + pa + b$.

(2) Suppose that φ, φ' are of level 1 and I_p acts trivially. Then
$$\rho_p\big|_I = \rho\big|_{I_t} = \begin{pmatrix} \chi^b & 0 \\ 0 & \chi^a \end{pmatrix}$$
for unique a, b with $0 \le a, b \le p-2$. We may interchange a, b to suppose $0 \le a \le b \le p-2$ and we define $k(\rho) = 1 + pa + b$.

(3) Suppose φ, φ' have level 1 and I_p does not act trivially. Then the proof of Proposition 3.3.1 shows that V^{I_p} is a nontrivial, one-dimensional stable subspace of V. The action of G_p on V^{I_p} and V/V^{I_p} is then via two characters ϕ_2, ϕ_1, and we have:
$$\rho_p = \begin{pmatrix} \phi_2 & * \\ 0 & \phi_1 \end{pmatrix}.$$
We may write $\phi_1 = \chi^\alpha \varepsilon_1$ and $\phi_2 = \chi^\beta \varepsilon_2$ for unique $0 \le \alpha \le p-2$ and $1 \le \beta \le p-1$, and unramified characters $\varepsilon_1, \varepsilon_2$. We then have
$$\rho_p\big|_I = \begin{pmatrix} \chi^\beta & * \\ 0 & \chi^\alpha \end{pmatrix}.$$
Set $a = \min(\alpha, \beta)$ and $b = \max(\alpha, \beta)$.
   (a) If $\beta = \alpha + 1$ (equivalently $\chi^{\beta-\alpha} = \chi$) and $\rho_p \otimes \chi^{-\alpha}$ is not finite at p then set $k(\rho) = 1 + pa + b + p - 1$.
   (b) Otherwise, set $k(\rho) = 1 + pa + b$.

Remarks 5.4.2.

(1) Observe that in any case, we have $k(\rho) - 1 \equiv a + b (\operatorname{mod} p-1)$, and $\det \rho_p = \chi^{a+b}$, so this agrees with the results of 5.3.

(2) We can motivate the definition of $k(\rho)$ in the situation of (1) above by using Theorem 4.2.2 and Theorem 4.2.4. Supposing that we are in this situation, we have
$$\rho_p\big|_I = \begin{pmatrix} \psi^a \psi'^b & 0 \\ 0 & \psi^b \psi'^a \end{pmatrix} = \chi^a \begin{pmatrix} \psi'^{b-a} & 0 \\ 0 & \psi^{b-a} \end{pmatrix},$$

so this looks just like the twist by the cyclotomic character (as in Theorem 4.2.4) of a representation whose restriction to I is of the form

$$\begin{pmatrix} \psi'^{k-1} & 0 \\ 0 & \psi^{k-1} \end{pmatrix},$$

with $2 \leq b-a+1 = k \leq p$. Theorems 4.2.2 and 4.2.4 suggest that the weight of the untwisted representation should be $k = b-a+1$, and therefore, by our discussion of the effect of θ on the weight, we should define $k(\rho) = b-a+1+a(p+1) = 1+pa+b$, as we have done.

(3) Similarly, in the situation of (2) above, we realize that $\rho_p\big|_I$ as a twist by χ^a of a representation whose restriction to I has the form

$$\begin{pmatrix} \chi^{k-1} & 0 \\ 0 & 1 \end{pmatrix},$$

where $1 \leq k = b-a+1 \leq p-1$. Theorems 4.2.1 and 4.2.4 then suggests that the weight of the untwisted representation should be k, and hence (as above) we should define $k(\rho) = b-a+1+a(p+1) = 1+pa+b$.

5.5. **The condition of "finite at p".** We would like to give a purely Galois-theoretic interpretation of the condition "finite at p." To do this, we suppose we are in the situation of (3a). As ρ_p is continuous, the group $\rho_p(I)$ is the Galois group of a totally ramified finite extension $K/\mathbf{Q}_p^{\mathrm{un}}$, and the group $\rho_p(I_p)$ is the Galois group of K/K_t, where $K_t/\mathbf{Q}_p^{\mathrm{un}}$ is the maximal tamely ramified subextension of K. The finite abelian group $\rho_p(I)/\rho_p(I_p) = \mathrm{Gal}(K_t/\mathbf{Q}_p^{\mathrm{un}})$, has a faithful representation

$$\begin{pmatrix} \chi^{\alpha+1} & 0 \\ 0 & \chi^{\alpha} \end{pmatrix},$$

so it has order $p-1$. Since $K_t \supseteq \mathbf{Q}_p^{\mathrm{un}}(\zeta_p)$, we conclude that $K_t = \mathbf{Q}_p^{\mathrm{un}}(\zeta_p)$ and $\mathrm{Gal}(K_t/\mathbf{Q}_p^{\mathrm{un}}) \simeq (\mathbf{Z}/p\mathbf{Z})^\times$. We have seen before that $\rho_p(I_p)$ is an abelian p-group. Since χ is trivial on I_p, we see that $\rho_p(I_p)$ is of the form

$$\begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix},$$

and is therefore killed by p. Thus, $\rho_p(I_p)$ is an abelian group of type $(p, p, \ldots, p)$. One easily computes that the conjugation action of $\mathrm{Gal}(K_t/\mathbf{Q}_p^{\mathrm{un}}) = \rho_p(I)/\rho_p(I_p)$ on $\mathrm{Gal}(K/K_t) = \rho_p(I)$ is through the character $\chi^{\beta-\alpha} = \chi$. Kummer theory permits us to conclude that

$$K = K_t(x_1^{1/p}, x_2^{1/p}, \ldots, x_m^{1/p}), \qquad \text{where } p^m = [K : K_t],$$

and $x_i \in (\mathbf{Q}_p^{\mathrm{un}})^\times/(\mathbf{Q}_p^{\mathrm{un}})^{\times p}$.

Definition 5.5.1. In the above situation, we say that ρ_p is *peu ramifié* if each x_i can be taken to have valuation 0 (i.e. a unit in $\mathbf{Z}_p^{\mathrm{un}}$). Otherwise, we say that ρ_p is *très ramifié*.

By [10, Proposition 8.2], the representation ρ_p is *peu ramifié* if and only if ρ is finite at p.

We may now state the precise form of Serre's conjecture:

Conjecture 5.5.2 (Serre)**.** *Let p be a prime and $\rho : G_{\mathbf{Q}} \to \mathrm{GL}_2(\overline{\mathbf{F}}_p)$ a continuous, irreducible odd representation. Then there exists an eigenform f of type $(N(\rho), k(\rho), \varepsilon(\rho))$ such that ρ is isomorphic to ρ_f.*

6. Examples

In this section we would like to give evidence for Serre's conjecture.

6.1. **Theoretical evidence.** In this section, we will show how the following deep theorem of Langlands–Tunnel can be used to prove Serre's conjecture in some cases.

Theorem 6.1.1 (Langlands–Tunnel)**.** *Let $\rho : G_{\mathbf{Q}} \to \mathrm{GL}_2(\mathbf{C})$ be a continuous irreducible odd representation with solvable image. Then ρ is equivalent to ρ_g for some eigenform g of weight one.*

For a proof of this theorem, consult [19], [31], and [12].

Example 6.1.2 (Dihedral representations). When the image of ρ is a dihedral group D_{2n} with $p \nmid n$, Conjecture 5.5.2 is known to be true [32]. The weak form of Serre's conjecture (Conjecture 4.1.2) follows from Theorem 6.1.1, but we will give the indications of a proof due to Hecke.

For any n, the group D_{2n} can be embedded into $\mathrm{GL}_2(\mathbf{C})$, so ρ gives rise to an odd Artin representation $\widetilde{\rho} : G_{\mathbf{Q}} \to \mathrm{GL}_2(\mathbf{C})$. We claim that $\widetilde{\rho}$ is induced from a character of $\mathbf{Z}/n\mathbf{Z}$. Indeed, view $\widetilde{\rho}$ with a representation of D_{2n}. Under the identification of D_{2n} with $\mathbf{Z}/n\mathbf{Z} \rtimes \mathbf{Z}/2\mathbf{Z}$ the restriction of $\widetilde{\rho}$ to $\mathbf{Z}/n\mathbf{Z}$ is given by two characters, φ, φ', so after a suitable conjugation we have

$$\widetilde{\rho}|_{\mathbf{Z}/n\mathbf{Z}} = \begin{pmatrix} \varphi & 0 \\ 0 & \varphi' \end{pmatrix}.$$

Since the action of $\mathbf{Z}/2\mathbf{Z}$ on $\mathbf{Z}/n\mathbf{Z}$ by conjugation is inversion, we find after an easy matrix calculation that $\varphi' = \varphi^{-1}$ and that $\widetilde{\rho}(\mathbf{Z}/2\mathbf{Z})$ is generated by a matrix of the form

$$\begin{pmatrix} 0 & u \\ v & 0 \end{pmatrix};$$

we may therefore scale basis vectors to achieve $u = v = 1$. A simple calculation with the definition of the induced representation $\mathrm{Ind}_{\mathbf{Z}/n\mathbf{Z}}^{D_{2n}} \varphi$ shows that we have an isomorphism

$$\mathrm{Ind}_{\mathbf{Z}/n\mathbf{Z}}^{D_{2n}} \varphi \simeq \widetilde{\rho}$$

as claimed, and one checks easily that $\widetilde{\rho}$ is irreducible if and only if φ is nontrivial.

Since the image of ρ is dihedral, it corresponds to a Galois extension $L/\mathbf{Q}$ with L a $\mathbf{Z}/n\mathbf{Z}$-extension of a quadratic field $K/\mathbf{Q}$. The character φ of $\mathrm{Gal}(L/K) \simeq \mathbf{Z}/n\mathbf{Z}$ associated to $\widetilde{\rho}$ as above can be viewed as a character of $\mathscr{O}_K$-ideals via the Artin map. The theta function

$$g = \sum_I \varphi(I) q^{\mathrm{Nm}\, I}$$

is a cusp form of weight 1 (for φ nontrivial) and level $|\,\mathrm{Disc}(L^{\mathrm{Gal}(K/\mathbf{Q})})|$. One multiplies g by a suitable Eisenstein series of weight 1 and level p to obtain a form f which, modulo p, is an eigenform and gives rise to ρ (*cf.* [6, 3.2.1]).

To obtain the full strength of Conjecture 5.5.2, one uses the weight and level-lowering techniques of Ribet, Edixhoven, Diamond, Buzzard, etc. as in [32].

Example 6.1.3 (The case $\mathrm{GL}_2(\mathbf{F}_3)$). Suppose that ρ has image $\mathrm{GL}_2(\mathbf{F}_3)$. Because of the existence of a section to the natural surjection $\mathrm{GL}_2(\mathbf{Z}[\sqrt{2}]) \twoheadrightarrow \mathrm{GL}_2(\mathbf{F}_3)$ given by reduction modulo the prime above 3, one can lift ρ to an odd Artin representation $\widetilde{\rho} : G_{\mathbf{Q}} \to \mathrm{GL}_2(\mathbf{C})$ with solvable image, as above. By Theorem 6.1.1, we can find an eigenform f of weight one giving rise to $\widetilde{\rho}$. By multiplying f by the Eisenstein series $6E_{1,\chi}$, where χ is the quadratic Dirichlet character $(\mathrm{mod}\, 3)$, we obtain a weight two form $g \equiv f (\mathrm{mod}\, 3)$. By [9, Lemma 6.11], there exists an *eigenform* g' of weight 2 whose eigenvalues are congruent to those of f modulo $(1 + \sqrt{-2})$. One then uses the same weight and level lowering theorems alluded to above to prove Conjecture 5.5.2 (at least when ρ is not exceptional, cf. [6]).

6.2. **Computational evidence.**

6.2.1. *Representations associated to semi-stable elliptic curves over* $\mathbf{Q}$. Fix a prime p and let $E/\mathbf{Q}$ be a semi-stable elliptic curve; that is, an elliptic curve having either good or multiplicative reduction everywhere. In this case, we can determine explicitly the invariants $N(\rho), k(\rho), \varepsilon(\rho)$ attached to the Galois representation $\rho : G_{\mathbf{Q}} \to \mathrm{GL}(V)$, where V is the two dimensional $\mathbf{F}_p$-vector space $E[p](\overline{\mathbf{Q}})$.

Theorem 6.2.1. *Let $E/\mathbf{Q}$ and ρ be as above, and let Δ_E be the minimal discriminant of E. Then*

$$N(\rho) = \prod_{\substack{\ell \neq p \\ p \nmid \mathrm{ord}_\ell(\Delta_E)}} \ell \qquad k(\rho) = \begin{cases} 2 & \text{if } p | \,\mathrm{ord}_p(\Delta_E) \\ p+1 & \text{otherwise} \end{cases} \qquad \varepsilon(\rho) = 1.$$

Proof. To handle $N(\rho)$, we distinguish two cases: that of good reduction at ℓ (i.e. $\mathrm{ord}_\ell(\Delta_E) = 0$), and that of multiplicative reduction at ℓ. In the first case, ρ is unramified at ℓ (this is the "easy" direction of NOS cf. [28, VII, Proposition 4.1]). In the second case, there is an unramified extension K of $\mathbf{Q}_\ell$ such that E/K has *split* multiplicative reduction. One then has an isomorphism of $\mathrm{Gal}(\overline{\mathbf{Q}}_\ell/K)$-modules

$$\overline{\mathbf{Q}}_\ell^\times/q^{\mathbf{Z}} \simeq E(\overline{\mathbf{Q}}_\ell)$$

for some $q \in K^\times$ with $v_\ell(q) > 0$. Under this isomorphism, $E[p]$ corresponds to the subgroup $\langle \zeta_p, q^{1/p}\rangle$. Since $\ell \neq p$, we conclude that the extension $K(\zeta_{\mathfrak{p}}, q^{1/p})/K$ is tamely ramified, and unramified if and only if $p|v_\ell(\Delta_E) = v_\ell(q)$. Since $K/\mathbf{Q}_\ell$ is unramified, our claim for $N(\rho)$ follows.

To determine $k(\rho)$, we analyze the local representation ρ_p. If ρ has good reduction at p, then the p-torsion in the Néron model shows that ρ_p is finite at p, so $k(\rho) = 2$. Observe also that in this case $\mathrm{ord}_p(\Delta_E) = 0$, so in particular $p \nmid \mathrm{ord}_p(\Delta_E)$. If ρ does not have good reduction at p, then by assumption it has multiplicative reduction at p, so over an unramified extension K of $\mathbf{Q}_p$ we have the exact sequence of Galois modules over K as above (using the Tate curve):

$$0 \to \mu_p \to E[p] \to \mathbf{Z}/p\mathbf{Z} \to 0,$$

so

$$\rho_p\big|_I \simeq \begin{pmatrix} \chi & * \\ 0 & 1 \end{pmatrix}.$$

As before, we have an isomorphism of $\mathrm{Gal}(\overline{\mathbf{Q}}_p/K)$-modules

$$E[p](\overline{\mathbf{Q}}_p) \simeq K(\zeta_p, q^{1/p}),$$

so by our considerations in 5.5, ρ_p is "*peu ramifié*" (hence finite at p) if and only if $p|v_p(q) = \mathrm{ord}_p(\Delta_E)$. Appealing to (3) of the definition of $k(\rho)$, we see that that $k(\rho) = 2$ if $p|\,\mathrm{ord}_p(\Delta_E)$ and is $p+1$ otherwise.

To determine $\varepsilon(\rho)$, we simply recall that $\det\rho = \chi$, since the Weil self pairing gives an isomorphism of Galois modules

$$\wedge^2 E[p] \simeq \mu_p.$$

■

Remark 6.2.2. We could generalize Theorem 6.2.1 as follows. For any elliptic curve $E/\mathbf{Q}$, Ogg [21] (or see the more general results of Saito [23]) gave a formula for the *conductor* of E (whose prime-to-p part is, in particular, equal to the Artin conductor of the Galois representation on $E[p]$ for any prime p). Let m_ℓ be the number of geometric irreducible components (not counting multiplicities) of the reduction of the minimal Néron model of E at ℓ. Then Ogg showed that

$$n(\ell, \rho) = \mathrm{ord}_\ell(\Delta_E) + 1 - m_\ell,$$

where $n(\ell, \rho)$ is as in Definition 3.1.1. This enables us to compute $N(\rho)$ for any elliptic curve $E/\mathbf{Q}$. If we require that E have multiplicative reduction at p, then we can use our methods above to compute $k(\rho)$ as well.

Let us use Theorem 6.2.1 and Remark 6.2.2 to illustrate Serre's conjecture in some concrete cases.

Example 6.2.3. Consider the elliptic curve $E/\mathbf{Q}$ with Weierstrass equation

$$y^2 + xy + y = x^3 + 1.$$

We compute that this model of E has discriminant $\Delta = -3^2 \cdot 71$, and that E has split multiplicative reduction at 3 and nonsplit multiplicative reduction at 71. Let us consider the Galois representation ρ on $E[3]$. By Theorem 6.2.1, we have $N(\rho) = 71$, $k(\rho) = 4$, and $\varepsilon(\rho) = 1$. Using MAGMA, we find a cuspidal eigenform of $f = \sum b_n q^n$ level 71, weight 4 and trivial character, and we compare the q-coefficients of f to the traces of Frobenius elements a_ℓ on $E[3]$:

ℓ	2	3	5	6	11	13	17	19	23	29	31	37	41	43
b_ℓ	1	1	-16	-1	24	7	72	-153	-213	232	149	-203	-432	71
a_ℓ	1	1	2	2	0	-2	0	0	0	-2	-10	-6	0	-4

Observe that in all cases computed $a_\ell \equiv b_\ell (\mathrm{mod}\, 3)$ (note that we do not expect this for $\ell = 3$).

Remark 6.2.4. In fact, one can prove that the representations ρ and ρ_f are isomorphic by verifying that $a_\ell \equiv b_\ell (\operatorname{mod} 3)$ for *finitely* many ℓ. Indeed, an effective version of the Chebotarev density theorem shows that for any finite Galois extension $K/\mathbf{Q}$, ramified at a finite set of primes S, the group $\operatorname{Gal}(K/\mathbf{Q})$ is generated by the conjugacy classes of Frob_ℓ for *finitely* many $\ell \notin S$. Under GRH, there exists an explicitly computable bound B, depending only on $[K : \mathbf{Q}]$ and the primes in S, such that $\operatorname{Gal}(K/\mathbf{Q})$ is generated by the conjugacy classes of Frob_ℓ for $\ell < B$ not in S [27, §2.5]. As a consequence, one can prove that two continuous $(\operatorname{mod} p)$ Galois representations are isomorphic by verifying a finite number of equalities (of traces of Frob_ℓ's for ℓ as above). One has the following theorem of Serre [27, §2.5 Théorèm 6]:

Theorem 6.2.5. *Let $K/\mathbf{Q}$ be a finite Galois extension of degree n, unramified outside a finite set of primes S. Under GRH, every conjugacy class of* $\operatorname{Gal}(K/\mathbf{Q})$ *contains some* Frob_ℓ *for*

$$\ell \leq 280 n^2 (\log n + \sum_{q \in S} \log q)^2.$$

In the situation above, we may take $n = \#GL_2(\mathbf{F}_3) = 48$ and $S = \{3, 71\}$ to obtain the bound $B = 54989339$. It is likely that we could explicitly determine a much smaller bound, by analyzing the orders of various Frob_ℓ's and using the structure of $\operatorname{GL}_2(\mathbf{F}_3)$, but we have not carried this out.

Example 6.2.6. Consider the elliptic curve $E/\mathbf{Q}$ with Weirstrass model

$$y^2 + xy = x^3 - x^2 - 37x - 78.$$

Then E has discriminant $\Delta = 7^3$ and has additive reduction at 7. It follows from Remark 6.2.2 that E has conductor $N = 7^2$. We consider the Galois representation ρ on $E[2]$. Theorem 6.2.1 gives $N(\rho) = 7^2$ and $k(\rho) = 2$. The space of cuspforms of weight 2 for $\Gamma_0(49)$ is one-dimensional, so the modular curve $X_0(49)$ is an elliptic curve and the unique cuspform $f = \sum b_n q^n$ must be an eigenform. One can determine a Weirstrass model for $X_0(49)$ using [13]

$$y^2 - 2xy = x^3 + 20x^2 + 112x,$$

and we find a degree 2 isogeny $X_0(49) \to E$ given explicitly by

$$(x, y) \mapsto \left(\frac{x}{4} + 2 + \frac{28}{x}, -\frac{x}{4} + \frac{y}{8} - 1 - 14\frac{y}{x^2} \right).$$

It follows that the traces a_ℓ *are* the Fourier coefficients b_ℓ.

Example 6.2.7. In this example, we make a detailed study of *icosahedral* mod 2 representations. To be precise, the group $\operatorname{PSL}_2(\mathbf{F}_4) = \operatorname{SL}_2(\mathbf{F}_4)$ acts on the 5 lines in $\mathbf{F}_4^2$, giving the identification

$$A_5 \simeq \operatorname{SL}_2(\mathbf{F}_4) \subseteq \operatorname{GL}_2(\mathbf{F}_4),$$

and we consider Galois extensions $K/\mathbf{Q}$ that are the splitting fields of irreducible quintic polynomials, with Galois group A_5. Although we prefer to provide our own examples, we follow Mestre [20, §4] in spirit.

First we prove a lemma giving a characterization of those quintic polynomials having Galois group A_5 over number fields.

Lemma 6.2.8. *Let $f \in \mathscr{O}_F[x]$ be a monic quintic polynomial over a number field F. Then the splitting field of f over F has Galois group A_5 if and only if the following three conditions are verified:*

(1) *The polynomial f is irreducible over F,*
(2) *there exists a prime $\mathfrak{p}$ of F prime to* $\operatorname{Disc}(f)$ *such that $f (\operatorname{mod} \mathfrak{p})$ has exactly two roots in $\kappa(\mathfrak{p})$,*
(3) *the discriminant of f is a square in $F^\times$*

Proof. Let G be the Galois group of f and identify G with a subgroup of S_5. The first condition ensures that G contains a 5-cycle and the second condition ensures that G contains a 3-cycle. Thus, G contains A_5. The condition on $\operatorname{Disc}(f)$ guarantees that G contains no 2-cycles, and hence must be A_5. It is not hard to see that these conditions are also necessary (using the Chebotarev Density Theorem to handle condition (2)). ■

Now fix a monic $f \in \mathbf{Z}[x]$ with splitting field $K/\mathbf{Q}$ having Galois group $G \simeq A_5$, and let

$$\rho : G \to \operatorname{GL}_2(\mathbf{F}_4)$$

be the associated Galois representation. We let L be any fixed subfield of K of degree 5 over $\mathbf{Q}$ generated by a root of f. Set $\mathrm{Gal}(K/L) = H \subseteq G$; it is of index 5 and isomorphic to A_4. We would like to determine the invariants $N(\rho), k(\rho), \varepsilon(\rho)$. To do this, we need to determine the ramification groups attached to the prime 2 and those primes that ramify in K. Explicitly carrying this out may at first appear to be a daunting task: in theory we must determine the splitting behavior of these primes in a degree 60 extension of $\mathbf{Q}$—a formidable task, even for advanced computer-algebra systems like MAGMA. It turns out, however, that we can identify all higher ramification groups at any given prime ℓ (starting with the inertia subgroup) from two pieces of information: the splitting behavior of ℓ in L and the exponent of ℓ in the discriminant of L. This follows from the following Proposition, due to Buhler [1].

Proposition 6.2.9 (Buhler)**.** *There are precisely 19 possibilities for the sequence of higher ramification groups of G at any prime ℓ with nontrivial decomposition group, as given in the table below.*

Type	*Nontrivial $G_{\ell,i}$ for $i \geq -1$*	*Splitting type of ℓ*	$\mathrm{ord}_\ell(\mathrm{Disc}(L))$	*Condition on ℓ*
1	C_5, C_5	1^5	4	$\ell \equiv 1 (\mathrm{mod}\, 5)$
2	C_3, C_3	$1^3 \cdot 1 \cdot 1$	2	$\ell \equiv 1 (\mathrm{mod}\, 3)$
3	C_2, C_2	$1^2 \cdot 1^2 \cdot 1$	2	$\ell \neq 2$
4	D_5, C_5	1^5	4	$\ell \equiv -1 (\mathrm{mod}\, 5)$
5	D_3, C_3	$1^3 \cdot 2$	2	$\ell \equiv -1 (\mathrm{mod}\, 3)$
6	D_2, C_2	$2^2 \cdot 1$	2	$\ell \neq 2$
7	C_5, C_5, C_5	1^5	8	$\ell = 5$
8	D_5, D_5, C_5	1^5	6	$\ell = 5$
9	D_5, C_5, C_5	1^5	8	$\ell = 5$
10	C_3, C_3, C_3	$1^3 \cdot 1 \cdot 1$	4	$\ell = 3$
11	D_3, D_3, C_3	$1^3 \cdot 1^2$	4	$\ell = 3$
12	D_3, C_3, C_3	$1^3 \cdot 2$	4	$\ell = 3$
13	D_3, D_3, C_3, C_3, C_3	$1^3 \cdot 1^2$	6	$\ell = 3$
14	C_2, C_2, C_2	$1^2 \cdot 1^2 \cdot 1$	4	$\ell = 2$
15	C_2, C_2, C_2, C_2	$1^2 \cdot 1^2 \cdot 1$	6	$\ell = 2$
16	D_2, C_2, C_2	$2^2 \cdot 1$	4	$\ell = 2$
17	A_4, D_2, D_2	$1^4 \cdot 1$	6	$\ell = 2$
18	D_2, C_2, C_2, C_2	$2^2 \cdot 1$	6	$\ell = 2$
19	D_2, D_2, D_2, C_2, C_2	$1^4 \cdot 1$	8	$\ell = 2$

Here, a splitting type of $f_1^{e_1} \cdot f_2^{e_2} \cdot f_3^{e_3}$ indicates that ℓ splits as a product $\mathfrak{l}_1^{e_1}\mathfrak{l}_2^{e_2}\mathfrak{l}_3^{e_3}$ in L, with primes $\mathfrak{l}_i$ having inertial degrees f_i. The condition on ℓ is necessary for the given type to occur.

Proof. See [1, Chapter 3]. ■

Note that the splitting type of ℓ together with the $\mathrm{ord}_\ell(\mathrm{Disc}(L))$ suffice to determine which of the 19 possible types occurs with the single ambiguity of distinguishing between types 7 and 9. Although we can differentiate between types 7 and 9 via [1, Appendix 2], for our purposes we do not need to: the two ramification filtrations agree from the inertia group $G_{5,0}$ onwards, and the formula for the Artin conductor 3.2 only depends on the ramification groups $G_{\ell,i}$ for $i \geq 0$.

Propostion 6.2.9 enables us to easily compute $N(\rho)$. Indeed, we need only know the order of $G_{\ell,i}$ and the number $\dim V/V^{G_{\ell,i}}$. The former is immediate from the table given in Proposition 6.2.9, while for the latter we observe that $\dim V^{G_{\ell,i}} = 0$ whenever $\rho(G_{\ell,i})$ contains an element of order greater than 2 since such elements never have 1 as an eigenvalue. Since we are only interested in $\ell > 2$, considerations of the possibilities for the $G_{\ell,i}$ as given by Proposition 6.2.9 yield

$$\dim V/V^{G_{\ell,i}} = \begin{cases} 0 & \text{if } \#G_{\ell,i} = 1 \\ 1 & \text{if } \#G_{\ell,i} = 2 \\ 2 & \text{otherwise} \end{cases}.$$

To determine $k(\rho)$, we study the local representation ρ_2 at 2. If 2 is unramified, then $e = 1$ and $k(\rho) = 1$. If 2 is tamely ramified, then by the table of Proposition 6.2.9 we must have $e = 3$ and it is not hard to see that the characters giving the action of the tame quotient have level 2, and our normalizations of a, b in that case force $k(\rho) = 2$. Finally, if 2 is wildly ramified, then $e = 2$ or 4, and we are in case (3) of the definition of $k(\rho)$. To ascertain whether ρ_2 is finite at 2 or not (corresponding to $k(\rho) = 2$ or $k(\rho) = 3$), we proceed via a case-by-case analysis of types 14–19 in the table of Proposition 6.2.9.

Recall that there are exactly 7 distinct quadratic extensions of $\mathbf{Q}_2$, given by adjoining to $\mathbf{Q}_2$ a square root of $b \in \mathbf{Q}_2$, where b is one of $-1, 2, -2, 5, -5, 10, -10$. Of these, all are ramified except for the extension $\mathbf{Q}_2(\sqrt{5})$. One easily sees from the definition (3.1) of the $G_{2,i}$ that $\mathbf{Q}_2(\sqrt{b})$ is of type 14 if and only if $b = -1, -5$ and is of type 15 if and only if $b = \pm 2, \pm 10$. Thus, by Definition 5.5.1, we see that if ρ_2 is of type 14 then it is peu ramifié, and if it is of type 15 then it is très ramifié. Now any D_2-extension of $\mathbf{Q}_2$ is realized as $\mathbf{Q}_2(\sqrt{a}, \sqrt{b})$ for some $a, b \in \{-1, \pm 2, \pm 5, \pm 10\}$, and such an extension is of type 16 or 18 if and only if it has an unramified quadratic sub-extension, i.e. if and only if a can be taken to be 5. By a similar analysis as in the case of a degree two extension, or by looking at discriminants, we see that type 16 occurs if and only if we may take $b = -1, -5$. Thus, if ρ_2 is of type 16 (respectively 18) then it is peu (respecvitely très) ramifié. Type 19 corresponds to the case of a, b with $\mathbf{Q}_2(\sqrt{a}, \sqrt{b})$ having no unramified quadratic sub-extension; i.e. one of a, b must have positive 2-adic valuation and any ρ_2 of type 19 is très ramifié. Finally, to analyze type 17, we observe that there is a unique A_4-extension of $\mathbf{Q}_2$ given explicitly as the splitting field F of $x^4 + 2x^3 + 2x^2 + 2$ [1, Chap. 3, Table 3.2]. Since the sylow-2 subgroup of A_4 is normal, there is a unique subfield F' of F of degree 3 over $\mathbf{Q}_3$. Elementary calculations show that $F' = \mathbf{Q}_2(r)$ where r is a root of $x^3 - 5x^2 + 6x - 1$, and that $F = F'(\sqrt{a}, \sqrt{b})$, where we may take

$$a = r^2 - 2r, \qquad b = -2r^2 + 7r - 2.$$

As both a and b are obviously 2-adic units, we conclude that if ρ_2 is of type 17, then it is peu ramifié.

Summarizing this discussion, we have

$$k(\rho) = \begin{cases} 1 & \text{if } \rho \text{ is unramified at 2} \\ 2 & \text{if } \rho_2 \text{ is of type 5 (tame ramification)} \\ 2 & \text{if } \rho_2 \text{ is of type 14, 16, 17 (wild ramification, peu)} \\ 3 & \text{if } \rho_2 \text{ is of type 15, 18, 19 (wild ramification, très)} \end{cases}$$

As for $\varepsilon(\rho)$, we know by construction that ρ has image in $\mathrm{SL}_2(\mathbf{F}_4)$, so $\det \circ \rho = 1$ whence $\varepsilon = 1$.

Once we have computed $N(\rho), k(\rho)$, we need to compute the $a_\ell := \mathrm{Tr}(\rho(\mathrm{Frob}_\ell))$. In order to do this, we observe that the trace of an element of $\mathrm{SL}_2(\mathbf{F}_4)$ up to automorphisms of $\mathbf{F}_4/\mathbf{F}_2$ depends only on its *order*, and hence only on the corresponding f (the inertial degree of ℓ in K). Indeed, the possible orders of elements in $\mathrm{SL}_2(\mathbf{F}_4)$ are $2, 3, 5$. If an element has order 2, it must have characteristic polynomial $x^2 - 1 = (x-1)^2$ and so has trace 0. Similarly, every nontrivial element of order 3 has characteristic polynomial $x^2 + x + 1$ and so has trace 1. Finally, the nontrivial elements of order 5 have characteristic polynomial a degree 2 monic polynomial over $\mathbf{F}_4$ dividing $x^4 + x^3 + x^2 + x + 1$, and the unique two such polynomials are $\mathrm{Gal}(\mathbf{F}_4/\mathbf{F}_2)$-conjuagte as claimed. Therefore,

$$a_\ell = \begin{cases} 0 & \text{if } \mathrm{ord}(\mathrm{Frob}_\ell) = 1 \text{ or } 2 \\ 1 & \text{if } \mathrm{ord}(\mathrm{Frob}_\ell) = 3 \\ \omega \text{ or } \omega^2 & \text{if } \mathrm{ord}(\mathrm{Frob}_\ell) = 5 \end{cases},$$

where ω, ω^2 are the distinct roots of $x^2 + x + 1$ in $\mathbf{F}_4$. In practice, we invoke the Chebotarev density theorem and compute enough a_ℓ that are either 1 or 0 to single out a unique cuspidal eigenform of the prescribed level and weight with the given Hecke eigenvalues. It is likely that one could gain a refined understanding of the relationships between the various Frob_ℓ's of order 5 to determine exactly when the corresponding a_ℓ's are *nontrivially* $\mathrm{Gal}(\mathbf{F}_4/\mathbf{F}_2)$-conjugate.

In order to efficiently compute the order of $\rho(\mathrm{Frob}_\ell)$ for unramified ℓ, (i.e. the inertial degree of ℓ in K), we use the following lemma to reduce to calculations in the degree 5 extension $L/\mathbf{Q}$, which are invariably easier:

Lemma 6.2.10. *Let K/F be an A_5-extension of number fields, ℓ a prime of F that is unramified in K and let f be the inertia degree of any prime in K over ℓ. Let $\{f_i\}$ be the corresponding degrees for the primes $\mathfrak{l}_i$ over ℓ in a subfield L of K of degree 5 over F. Then $f = f_i$ for some i, so in particular*

$$f = \mathrm{lcm}_i\, f_i.$$

Proof. Let D be any decomposition subgroup of a prime of K over ℓ. Since D is abelian (in view of the triviality of the inertia group at ℓ) it must be isomorphic to C_2, C_3, C_5, or D_2 (by the well-known classification of subgroups of A_5). We claim there exists a conjugation of D having trivial intersection with $H := \mathrm{Gal}(K/L)$. Indeed, either $D \simeq C_5$, in which case our claim is trivial as H has order prime to 5, or D is isomorphic to one of C_2, C_3, or D_2. In this case, viewing A_5 as the group of permutations of a 5-element set, we see that D fixes at least one element and at most 2 elements. As the same is true for H, we may choose a conjugation D' of D which fixes different elements from that of H, and this ensures that $H \cap D' = \{1\}$. It follows that there is a prime $\mathfrak{l}'$ of K over ℓ with decomposition group D' such that

$$f(\mathfrak{l}'|\mathfrak{l}' \cap L) = \#H \cap D' = 1,$$

and since K/L is Galois, we conclude that $\mathfrak{l}' \cap L$ splits completely in K. Thus, $\mathfrak{l}' \cap L$ is a prime of L over ℓ with inertial degree f, and this obviously implies the lemma. ■

Remark 6.2.11. We remark that if the condition that ℓ be unramified in K is removed from the statement of Lemma 6.2.10, then the conclusion is false. The proof breaks down because D can then be isomorphic to D_5, and every copy of D_5 inside A_5 has nontrivial intersection with every copy of A_4.

We now give an explicit example. Let

$$f = x^5 + 2x^3 - 4x^2 - 2x + 4.$$

Then f is irreducible, $d := \mathrm{Disc}(f) = (2^4 \cdot 73)^2$, and $f (\mathrm{mod}\, 7)$ has exactly two roots in $\mathbf{F}_7$, so if K denotes the splitting field of f then Lemma 6.2.8 shows that $G := \mathrm{Gal}(K/\mathbf{Q}) \simeq A_5$. Letting L be the subfield of K given by adjoining a root of f to $\mathbf{Q}$, we readily compute the following factorizations:

$$(2) = \mathfrak{l}_1\mathfrak{l}_2^4 \qquad (73) = \mathfrak{l}_1\mathfrak{l}_2^2\mathfrak{l}_3^2,$$

so ρ_{73} must be of type 3 and ρ_2 is of type 17 or 19; since $\mathrm{ord}_2(\mathrm{Disc}(L)) = 6$, we see that ρ_2 is of type 17 so by our considerations we have

$$N(\rho) = 73 \qquad k(\rho) = 2.$$

We compute the a_ℓ for $\ell \neq 2, 73$ up to $\mathrm{Gal}(\mathbf{F}_4/\mathbf{F}_2)$-conjugacy as indicated above in the following table:

ℓ	3	5	7	11	13	17	19	23	29	31	37	41	43	47	53	59	61	67	71
a_ℓ	ω, ω^2	ω, ω^2	1	ω, ω^2	ω, ω^2	1	1	ω, ω^2	1	0	1	0	1	1	1	0	ω, ω^2	1	ω, ω^2

We now appeal to the MAGMA to find a cuspidal eigenform of level 73 and weight 2 with matching eigenvalues. Using the code

```
S:=CuspForms(Gamma1(73),2);
f:=Newform(S,2);
Parent(f);
R:=Reductions(f,2);
f2:=R[1][1];
PowerSeries(f2,72);
```

we find that there is a single Galois conjugacy class of newforms of weight 2 on $\Gamma_1(73)$ defined over the extension of $\mathbf{Q}$ given by adjoining a root of $x^2 + 3x + 1$, and that the reduction modulo 2 of one of the two elements of this conjugacy class is the form

$$\begin{aligned} f = q + \omega q^2 + \omega^2 q^3 + \omega^2 q^4 + \omega q^5 + q^6 + q^7 + q^8 + \omega^2 q^9 + \omega^2 q^{10} + \omega^2 q^{11} + \omega q^{12} + \omega^2 q^{13} + \omega q^{14} + q^{15} \\ + \omega q^{16} + q^{17} + q^{18} + q^{19} + q^{20} + \omega^2 q^{21} + q^{22} + \omega q^{23} + \omega^2 q^{24} + \omega q^{25} + q^{26} + q^{27} + \omega^2 q^{28} + q^{29} \\ + \omega q^{30} + \omega^2 q^{32} + \omega q^{33} + \omega q^{34} + \omega q^{35} + \omega q^{36} + q^{37} + \omega q^{38} + \omega q^{39} + \omega q^{40} + q^{42} + q^{43} + \omega q^{44} + q^{45} \\ + \omega^2 q^{46} + q^{47} + q^{48} + \omega^2 q^{50} + \omega^2 q^{51} + \omega q^{52} + q^{53} + \omega q^{54} + q^{55} + q^{56} + \omega^2 q^{57} + \omega q^{58} + \omega^2 q^{60} \\ + \omega q^{61} + \omega^2 q^{63} + q^{64} + q^{65} + \omega^2 q^{66} + q^{67} + \omega^2 q^{68} + q^{69} + \omega^2 q^{70} + \omega^2 q^{71} + \cdots \end{aligned}$$

Observe that the Hecke eigenvalues are the a_ℓ up to $\mathrm{Gal}(\mathbf{F}_4/\mathbf{F}_2)$-conjugacy, at least in the range we have considered.

Let us conclude this example by giving a table of polynomials having Galois group A_5 and the corresponding values of $N(\rho), k(\rho)$.

	$N(\rho)$	$k(\rho)$
$x^5 - 10x^3 - 4x^2 + 13x - 12$	193	2
$x^5 - 6x^3 - 12x^2 - 10x - 4$	17^2	2
$x^5 - 2x^3 - 2x^2 + 3x + 2$	29^2	2
$x^5 + x^3 - 5x^2 - 4x - 7$	353	2
$x^5 + 2x^3 - 4x^2 + 6x - 4$	67	2
$x^5 + 2x^3 - 2x^2 - x + 2$	$5^2 \cdot 11$	2
$x^5 + 3x^3 + 6x^2 + 2x + 1$	653	1
$x^5 + 6x^3 - 12x^2 + 2x - 4$	$5 \cdot 149$	2
$x^5 + 6x^3 - 7x - 8$	29^2	2
$x^5 - 4x^2 + x + 4$	61^2	3

We leave it to the interested reader to compute the a_ℓ in each case and find a normalized cuspidal eigenform of the prescribed weight and level with the same Hecke eigenvalues.

References

[1] J. Buhler, *Icosahedral Galois representations*, Lecture Notes in Math. **654** (1978).

[2] H. Carayol, *Sur les répresentations ℓ-adiques associées aux formes modulaires de Hilbert*, Ann. Sci. Ecole Norm. Sup. (4) **19** (1986), 409–468.

[3] H. Carayol, *Sur les répresentations galoisiennes modulo ℓ attachées aux formes modulaires*, Duke Math. J. **59** (1989), 785–801.

[4] B. Conrad, *Arithmetic moduli of generalized elliptic curves*, to appear.

[5] B. Conrad, *Grothendieck duality and base change*, Lecture Notes in Math. **1750** (2000).

[6] H. Darmon, *Serre's Conjectures*, Seminar on Fermat's last theorem (Toronto, ON., 1993-1994), Amer. Math. Soc., Providence, RI., (1995), 135–153.

[7] P. Deligne and M. Rapoport, *Schémas de modules de courbes elliptiques*, Lecture Notes in Math. **349** (1973), 143–316.

[8] P. Deligne, *Formes modulaires et représentations ℓ-adiques*, Sém. Bourbaki **355**, Lecture Notes in Math. **179** (1971), 136–172.

[9] P. Deligne and J-P. Serre, *Formes modulaires de poids 1*, Ann. Sci. E.N.S. **7** (1974), 507–530.

[10] B. Edixhoven, *The weight in Serre's conjectures on modular forms*, Invent. Math. **109** (1992), 563–594.

[11] B. Edixhoven, *Serre's conjecture*, Modular forms and Fermat's last theorem (Boston, MA., 1995), Springer-Verlag, N.Y. (1997), 209–242.

[12] S. Gelbart, *Three lectures on the modularity of $\overline{\rho}_{E,3}$ and the Langlands reciprocity conjecture*, Modular forms and Fermat's last theorem (Boston, MA., 1995), Springer-Verlag, N.Y. (1997), 155–209.

[13] J.G. Rovira, *Equations of hyperelliptic modular curves*, Annales de l'institute Fourier **41** No. 4 (1991), 779–795.

[14] B. Gross, *A tameness criterion for Galois representations associated to modular forms* $(\bmod\, p)$, Duke Math. J. **61** No. 2 (1990), 445–517.

[15] R. Hartshorne, *Algebraic geometry*, Springer GTM **52**, Springer-Verlag, N.Y. (1977).

[16] N. Katz, *p-adic properties of modular schemes and modular forms*, Lecture Notes in Math. **350** (1973), 69–170.

[17] N. Katz, *A result on modular forms in characteristic p*, Lecture notes in Math. **601** (1976), 53–61.

[18] N. Katz and B. Mazur, *Arithmetic moduli of elliptic curves*, Annals of Math. Stud. **108**, Princeton University (1985).

[19] R. Langlands, *Base change for* GL(2), Ann. of Math. Stud **96**, Princeton University Press (1980).

[20] J-F. Mestre, *La méthode des graphes. Exemples et applications,* Taniguchi Symp., Kyoto (1986), 217–242.

[21] A.P. Ogg, *Elliptic curves and wild ramification*, Amer. J. of Math. **89** No. 1 (1967), 1–21.

[22] K. Ribet and W. Stein, *Lectures on Serre's conjectures*, Arithmetic algebraic geometry, IAS/Park City Math. Ser. **9** (2001).

[23] T. Saito, *Conductor, discriminant, and the Noether formula of arithmetic surfaces*, Duke Math. J. **57** No. 1 (1988) 151–173.

[24] J-P. Serre, *Sur les représentations modulaires de degré 2 de* Gal$(\overline{\mathbf{Q}}/\mathbf{Q})$, Duke Math. J. **54** No. 1 (1987), 179–230.

[25] J-P. Serre, *Propriétés galoisienne des points d'ordre fini des courbes elliptiques*, Invent. Math. **15** (1972), 259–331.

[26] J-P. Serre, *Local fields*, Springer GTM **67**, Springer-Verlag, N.Y. (1979).

[27] J-P. Serre, *Quelques applications du théorème de densité de Chebotarev*, Publ. Math. IHES **54** (1981), 123–202.

[28] J. Silverman, *The arithmetic of elliptic curves*, Springer GTM **106**, Springer-Verlag, N.Y. (1986).

[29] W. Stein, *The modular forms database*, `http://modular.ucsd.edu/mfd`

[30] J. Tate, *Finite flat group schemes*, Modular forms and Fermat's last theorem (Boston, MA., 1995), Springer-Verlag, N.Y. (1997),

[31] J. Tunnel, *Artin's conjecture for representations of octahedral type*, Bull. A.M.S. (1981), 173–175.

[32] G. Wiese, *Dihedral Galois representations and Katz modular forms*, Documenta Math. **9** (2004), 123–133. 209–242.