Serre's conjecture

Alex J. Best

Contents

1 Introduction

In 1987 Jean-Pierre Serre published a paper [Ser87], "Sur les représentations modulaires de degré 2 de $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$", in the Duke Mathematical Journal. In this paper Serre outlined a conjecture detailing a precise relationship between certain mod p Galois representations and specific mod p modular forms. This conjecture and its variants have become known as Serre's conjecture, or sometimes *Serre's modularity conjecture* in order to distinguish it from the many other conjectures Serre has made. The conjecture has since been proven correct by the work of numerous people, culminating with that of Khare–Wintenberger and Kisin, published in 2009 [KW09a, KW09b, Kis09].

Here we provide a motivated account of the original form of the conjecture before going on to compute some explicit examples and examining some interesting consequences.

Beyond the original paper there are many very good accounts of Serre's statement, including Cais [Cai09], Edixhoven [Edi97] (both of which use Katz's more general definition of mod p modular forms), and Darmon [Dar95] (which stays closer to the original article). There is also a chapter by Ribet–Stein [RS99]. Alex Ghitza has prepared a translation of part of Serre's paper [Ghi] which has been helpful. Article by Edixhoven [Edi92].

2 Background

Here we fix several definitions and key results that will be relevant when discussing Serre's conjecture.

2.1 Modular forms

We assume material relating to classical modular forms, and here only look at the passage to *mod p modular forms* as these are a key part of Serre's conjecture and as there is some amount of choice in how these forms are defined.

Definition 2.1. Given a subring R of $\mathbf{C}$ we let $S_k(N, \varepsilon; R)$ be the space of cusp forms of level k, weight N and character $\varepsilon\colon (\mathbf{Z}/N\mathbf{Z})^* \to R$, whose q-expansion coefficients lie in R.

Given a mod p character

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

we may lift to a character

$$\hat{\varepsilon}\colon (\mathbf{Z}/N\mathbf{Z})^* \to \overline{\mathbf{Z}}^*,$$

with values in the prime to p roots of unity.

We can now let the space of *cuspidal mod p modular forms* of weight k, level N and character $\varepsilon\colon (\mathbf{Z}/N\mathbf{Z})^* \to \overline{\mathbf{F}}_p^*$ be the subspace of $\overline{\mathbf{F}}_p[[q]]$ obtained by reducing mod p the q-expansions of forms in $S_k(N, \hat{\varepsilon}; \overline{\mathbf{Z}})$. We denote this space by

$$S_k(N, \varepsilon; \overline{\mathbf{F}}_p).$$

Taking the union over all characters ε gives us the space of mod p cusp forms of weight k and level N

$$S_k(N; \overline{\mathbf{F}}_p).$$

We can in the same way define the full (non-cuspidal) space of mod p modular forms, along with mod p modular forms for more general congruence subgroups. But we don't need to consider such forms in this essay so we restrict to cusp forms for Γ_1 to keep things simple.

Many notions defined for normal modular forms descend to mod p modular forms in the natural way.

Definition 2.2. The Hecke operators have an action on q-expansions that preserves each space $S_k(N, \varepsilon; \overline{\mathbf{Z}})$ (see the proof of Proposition 4.1). So we may define the action of the Hecke operators on mod p modular forms by letting them act on a lifts of the mod p q-expansions and then reducing the expansion again.

Definition 2.3. As for standard modular forms, we say a mod p cusp form $f = \sum_{n\geq 1} a_n q^n$ is *normalised* if $a_1 = 1$.

Proposition 2.1. *If f and g are two non-zero mod p modular forms of weights k and k' respectively, whose q-expansions are equal, then*

$$k \equiv k' \pmod{p-1}.$$

Proof. See [Ser73a]. □

Example 2.1. Using Sage [S+15] we find the following example, let

$$f = q - q^2 - 2q^3 - 7q^4 + 16q^5 + 2q^6 - 7q^7 + O(q^8) \in S_4(7, \mathrm{Id}; \mathbf{Z}),$$

$$g = q - 6q^2 - 42q^3 - 92q^4 - 84q^5 + 252q^6 + 343q^7 + O(q^8) \in S_8(7, \mathrm{Id}; \mathbf{Z}),$$

then if we reduce mod 5 we see that

$$\begin{aligned}\overline{f} &= q + 4q^2 + 3q^3 + 3q^4 + q^5 + 2q^6 + 3q^7 + O(q^9) \in S_4(7, \mathrm{Id}; \overline{\mathbf{F}}_5),\\ \overline{g} &= q + 4q^2 + 3q^3 + 3q^4 + q^5 + 2q^6 + 3q^7 + O(q^9) \in S_8(7, \mathrm{Id}; \overline{\mathbf{F}}_5),\end{aligned}$$

which are indeed equal up to this precision.

In fact for $p \geq 5$ it is always the case that $S_k(N; \overline{\mathbf{F}}_p) \subset S_{k+p-1}(N; \overline{\mathbf{F}}_p)$ [Ser73b]. Due to this behaviour the concept of weight is not particularly well defined for mod p modular forms, so we introduce the notion of a *filtration*.

Definition 2.4. The *filtration* of a mod p cusp form f of level N is the minimal k for which $f \in S_k(N; \overline{\mathbf{F}}_p)$. We denote this by $w(f)$.

Now we look at an important operator on the space of mod p modular forms, which we shall study more in Section 4.3.

Definition 2.5. The Θ operator is defined on (cuspidal) mod p modular forms via its action on q-expansions by

$$\Theta\left(\sum_{n\geq 0} a_n q^n\right) = q\frac{\mathrm{d}}{\mathrm{d}q}\left(\sum_{n\geq 0} a_n q^n\right) = \sum_{n\geq 0} n a_n q^n.$$

Proposition 2.2. *If f is a mod p cusp form of filtration $w(f) = k$, then $\Theta(f)$ is also a mod p cusp form of the same level and character and has filtration*

$$w(\Theta(f)) = \begin{cases} k + p + 1 & \text{if } p \nmid k,\\ k + p + 1 - n(p-1),\ n \geq 1 & \text{if } p \mid k.\end{cases}$$

Proof. See [Ser73a] and also [Joc82] for more detail about how the filtration lowers in the $p \mid k$ case. □

It is clear from the definition of the action that Θ preserves the set of normalised forms.

Proposition 2.3. *Θ semicommutes with the Hecke operators T_ℓ (specifically we have $T_\ell \Theta = \ell \Theta T_\ell$), and hence Θ preserves eigenforms.*

Proof. The Hecke operators T_ℓ on $S_k(N, \varepsilon; \overline{\mathbf{F}}_p)$ act on q-expansions by

$$T_\ell\left(\sum_{n\geq 1} a_n q^n\right) = \begin{cases} \sum_{n\geq 1} a_{\ell n} q^n + \ell^{k-1}\varepsilon(\ell)\sum_{n\geq 1} a_n q^{\ell n} & \text{if } \ell \nmid N, \\ \sum_{n\geq 1} a_{\ell n} q^n & \text{if } \ell \mid N. \end{cases}$$

We let $f = \sum_{n\geq 1} a_n q^n \in S_k(N, \varepsilon; \overline{\mathbf{F}}_p)$ and calculate

$$\Theta T_\ell f = \begin{cases} \sum_{n\geq 1} n a_{\ell n} q^n + \ell^{k-1}\varepsilon(\ell)\sum_{n\geq 1} \ell n a_n q^{\ell n} & \text{if } \ell \nmid N, \\ \sum_{n\geq 1} n a_{\ell n} q^n & \text{if } \ell \mid N, \end{cases}$$

and

$$T_\ell \Theta f = \begin{cases} \sum_{n\geq 1} \ell n a_{\ell n} q^n + \ell^{k+p+1-1}\varepsilon(\ell)\sum_{n\geq 1} n a_n q^{\ell n} & \text{if } \ell \nmid N, \\ \sum_{n\geq 1} \ell n a_{\ell n} q^n & \text{if } \ell \mid N. \end{cases}$$

As we are in characteristic p here $\ell^{k+p} = \ell^{k+1}$, so

$$T_\ell \Theta = \ell \Theta T_\ell,$$

thus if f is an eigenform for the T_ℓ then Θf is an eigenform too. However the eigenvalue for each T_ℓ is ℓ times the original. $\square$

2.2 Galois representations

Here we mostly concern ourselves with fixing definitions and recalling important results that shall be needed later. There are many good references for this type of material, for example [Wie12].

Definition 2.6. An *n-dimensional mod p Galois representation* is a homomorphism

$$\rho\colon \operatorname{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \operatorname{GL}_n(\overline{\mathbf{F}}_p).$$

Similarly, an *n-dimensional p-adic Galois representation* is a homomorphism

$$\rho\colon \operatorname{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \operatorname{GL}_n(\mathbf{Q}_p).$$

Unless stated otherwise the term Galois representation will refer to a mod p Galois representation.

Recall that $\operatorname{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ is defined as the inverse limit of $\operatorname{Gal}(K/\mathbf{Q})$ as K ranges over all number fields. So the group $\operatorname{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ naturally has the profinite topology, where the open subgroups are the subgroups of finite index. We demand that all of our mod p representations be continuous with respect to this topology and the discrete topology on $\operatorname{GL}_n(\overline{\mathbf{F}}_p)$.

Remark 2.1. The continuity condition for mod p Galois representations reduces to having an open kernel, so continuous mod p Galois representations always have finite image.

We deal mostly with 1 and 2 dimensional mod p Galois representations. Those of dimension 1 (i.e. maps $\phi\colon \operatorname{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \overline{\mathbf{F}}_p^*$) are called *characters*.

Given a 2-dimensional mod p representation $\rho\colon G \to \mathrm{GL}_2(\overline{\mathbf{F}}_p)$ we often use the notation

$$\rho \sim \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix},$$

where α, β, γ and δ are characters, to indicate that there is some $A \in \mathrm{GL}_2(\overline{\mathbf{F}}_p)$ such that for every $\sigma \in G$

$$\rho(\sigma) = A \begin{pmatrix} \alpha(\sigma) & \beta(\sigma) \\ \gamma(\sigma) & \delta(\sigma) \end{pmatrix} A^{-1}.$$

Definition 2.7. Let ρ be a mod p Galois representation and ϕ be a mod p Galois character. We can form a new mod p Galois representation of the same dimension as ρ by taking the product of the images for each element of $\operatorname{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$. This is called the *twist* of ρ by ϕ, and is denoted $\phi \otimes \rho$.

Although our main object of study is $\operatorname{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ it will be very useful for us to take a prime ℓ and also consider representations of

$$\mathrm{G}_\ell = \operatorname{Gal}(\overline{\mathbf{Q}}_\ell/\mathbf{Q}_\ell).$$

Indeed such representations can be obtained from those of $\operatorname{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ using an inclusion

$$\overline{\mathbf{Q}} \hookrightarrow \overline{\mathbf{Q}}_\ell$$

to define a restriction map

$$\mathrm{G}_\ell \to \operatorname{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}).$$

In fact due to Krasner's lemma [Coh08, p. 238] the map $\mathrm{G}_\ell \to \operatorname{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ is injective and so we may view G_ℓ as a subgroup of $\operatorname{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$. The way this subgroup sits inside $\operatorname{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ depends on the choice of embedding $\overline{\mathbf{Q}} \hookrightarrow \overline{\mathbf{Q}}_\ell$ and varies by conjugation as this embedding changes.

The group G_ℓ has several important subquotients which will be helpful for us to study restrictions of representations to.

Definition 2.8. The ring of integers of $\overline{\mathbf{Q}}_\ell$ is stable under the action of G_ℓ, as is the maximal ideal of the local ring $\overline{\mathbf{Q}}_\ell$. So we get an action of G_ℓ on the residue field, this field may be identified with $\overline{\mathbf{F}}_p$. We therefore obtain a map

$$G_\ell \twoheadrightarrow \mathrm{Gal}(\overline{\mathbf{F}}_\ell/\mathbf{F}_\ell).$$

The *inertia subgroup* I_ℓ is defined to be the kernel of this map. The group $\mathrm{Gal}(\overline{\mathbf{F}}_\ell/\mathbf{F}_\ell)$ is topologically cyclic, generated by the Frobenius morphism $x \mapsto x^\ell$. We let $\mathrm{Frob}_\ell \in G_\ell$ be a preimage of this morphism under the restriction map, this is only defined up to conjugation.

Next the *wild* inertia group $I_{\ell,w}$ is the maximal pro-ℓ-subgroup of I_ℓ and the *tame* inertia group is the quotient

$$I_{\ell,t} = I_\ell / I_{\ell,w}.$$

This is canonically isomorphic to

$$\prod_{p \neq \ell} \mathbf{Z}_p$$

Finally we may define a series of subgroups of G_ℓ that study the higher ramification. Let ν_l be the extension of the ℓ-adic valuation to $\overline{\mathbf{Q}}_\ell$ and define

$$G_{\ell,u} = \{\sigma \in G_\ell : \nu_l(\sigma(x) - x) \geq u + 1 \; \forall x \in \mathcal{O}_{\overline{\mathbf{Q}}_\ell}\}.$$

The $G_{\ell,u}$ form a descending chain as u ranges over the integers that includes several groups we have already mentioned

$$G_\ell = G_{\ell,-1} \supseteq I_\ell = G_{\ell,0} \supseteq I_{\ell,w} = G_{\ell,1} \supseteq G_{\ell,2} \supseteq \cdots.$$

The groups we have been looking at correspond to important extensions on the Galois side. Let $\mathbf{Q}_p^{\mathrm{nr}}$ denote the maximal non-ramified extension of $\mathbf{Q}_p$ and $\mathbf{Q}_p^{\mathrm{tr}}$ denote the maximal tamely-ramified extension of $\mathbf{Q}_p$.

$$\begin{tikzcd}
\overline{\mathbf{Q}}_\ell \arrow[d, dash, "I_{\ell,w}"] \arrow[dd, dash, bend left=60, "I_\ell"] \arrow[ddd, dash, bend right=60, "G_\ell"'] \\
\mathbf{Q}_\ell^{\mathrm{tr}} \arrow[d, dash, "I_{\ell,t}"] \\
\mathbf{Q}_\ell^{\mathrm{nr}} \arrow[d, dash] \\
\mathbf{Q}_\ell
\end{tikzcd}$$

The tame inertia $I_{\ell,t}$ may be identified with

$$\varprojlim \mathbf{F}_{\ell^n}^*.$$

Definition 2.9. We say a Galois representation ρ is *unramified* at ℓ if $\rho|_{I_\ell}$ is trivial. Otherwise, we say ρ is *ramified* at ℓ.

Similarly we say ρ is *tamely ramified* at ℓ if $\rho|_{I_{\ell,w}}$ is trivial.

The usefulness of the Frobenius elements stems in part from the following theorem.

Theorem 2.1 (Chebotarev's density theorem). *Galois representations are determined completely by the images of Frobenius elements.*

Definition 2.10. Let $\phi\colon \operatorname{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to K^*$ be a character for some field K and fix an embedding $\overline{\mathbf{Q}} \hookrightarrow \mathbf{C}$. We may then view complex conjugation as an element $c \in \operatorname{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$, looking at its image $\phi(c)$ we see it is an element of order 2 in K^*, so $\phi(c)$ must be ± 1. If $\phi(c) = -1$ we say ϕ is *odd*, otherwise we say ϕ is *even* (though we shall mostly be concerned with distinguishing odd representations here).

Now given any Galois representation

$$\rho\colon \operatorname{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathrm{GL}_n(K),$$

we define the parity of ρ to be that of the character $\det \rho$.

Definition 2.11. Each character

$$\phi\colon \operatorname{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \overline{\mathbf{F}}_p^*$$

has finite image and so factors through some $\mathbf{F}_{p^n}$, the smallest n for which this can happen is called the *level* of the character.

As any character $\phi\colon \operatorname{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \overline{\mathbf{F}}_p^*$ factors through an abelian subgroup, the Kronecker–Weber theorem tells us that any such character factors as

$$\phi\colon \operatorname{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \operatorname{Gal}(\mathbf{Q}(\zeta_N)/\mathbf{Q}) \cong (\mathbf{Z}/N\mathbf{Z})^* \xrightarrow{\phi_N} \overline{\mathbf{F}}_p^*,$$

where ζ_N is a primitive Nth root of unity. We can also use this factorisation to extend any Dirichlet character to a character of the absolute Galois group. Thus characters of the Galois group are in bijection with Dirichlet characters

$$(\mathbf{Z}/N\mathbf{Z})^* \xrightarrow{\phi_N} \overline{\mathbf{F}}_p^*.$$

Definition 2.12. The identity map

$$(\mathbf{Z}/p\mathbf{Z})^* \to \mathbf{F}_p^* \hookrightarrow \overline{\mathbf{F}}_p^*$$

is a Dirichlet character and thus gives us a character of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$. This character is called the mod p cyclotomic character, denoted χ_p.

Remark 2.2. We note some important properties of the mod p cyclotomic character.

Taking any $\sigma \in \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ the definition above is saying that σ sends

$$\zeta_p \mapsto \zeta_p^{\chi_p(\sigma)},$$

where ζ_p is a primitive pth root of unity. Assume $\ell \neq p$ and denote reduction mod ℓ by $\overline{\cdot}$. We see that

$$\overline{\mathrm{Frob}_\ell(\zeta_p)} = \overline{\zeta_p}^{\ell},$$

but the only possibility is that $\mathrm{Frob}_\ell(\zeta_p) = \zeta_p^\ell$ and so

$$\chi_p(\mathrm{Frob}_\ell) = \ell.$$

Now if we fix an embedding $\overline{\mathbf{Q}} \hookrightarrow \mathbf{C}$ and considering complex conjugation $c \in \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ we see that it takes $\zeta_p \mapsto \zeta_p^{-1}$ and hence

$$\chi_p(c) = -1,$$

so χ_p is an example of an odd character.

Finally, straight from the definition we see that χ_p is of level 1.

For each $n \geq 1$ we now distinguish n special mod p characters of $I_{p,t}$ of level n, these will allow us to describe all such characters of a particular level.

Definition 2.13. The identification

$$I_{p,t} = \varprojlim \mathbf{F}_{p^n}^*$$

gives us a natural map

$$\psi \colon I_{p,t} \to \mathbf{F}_{p^n}^*$$

for each n. The *fundamental characters* of level n are defined by extending ψ to an $\overline{\mathbf{F}}_p$-character via the n embeddings $\mathbf{F}_{p^n}^* \hookrightarrow \overline{\mathbf{F}}_p^*$.

While any individual fundamental character is not canonical, the set of all of them of a particular level is.

Remark 2.3. The embeddings are all obtained from any chosen one by applying Frobenius and as such the product of all fundamental characters of level n is the same as the composition of the norm map $\mathbf{F}_{p^n}^* \to \mathbf{F}_p^*$ with any one. So this product will always be the unique fundamental character of level 1.

Definition 2.14. The *semisimplification* of a 2-dimensional representation ρ is another representation, denoted ρ^{ss}, that is obtained as follows. If ρ is irreducible (and hence semisimple) we leave it as it is and set $\rho^{\mathrm{ss}} = \rho$. Otherwise if ρ is reducible we know that

$$\rho \sim \begin{pmatrix} \phi_1 & * \\ 0 & \phi_2 \end{pmatrix}.$$

The semisimplification ρ^{ss} is then the representation given by

$$\begin{pmatrix} \phi_1 & 0 \\ 0 & \phi_2 \end{pmatrix},$$

conjugated in the same way ρ was. Which is indeed semisimple, as you would hope.

In the general case the process of semisimplification is analogous, it is obtained by taking the direct sum of the Jordan–Hölder constituents of a representation, though for us the above description suffices.

Definition 2.15. We now classify Galois representations $\rho_p \colon \mathrm{G}_p \to \mathrm{GL}_2(\overline{\mathbf{F}}_p)$ that satisfy

$$\rho_p \sim \begin{pmatrix} \chi_p \varepsilon_1 & * \\ 0 & \varepsilon_2 \end{pmatrix}.$$

There is a unique maximal tamely ramified extension of $\mathbf{Q}_p^{\mathrm{nr}}$ that is contained inside of K, we write K_t for this extension, and we have the following setup

$$\begin{tikzcd}
\overline{\mathbf{Q}}_p \arrow[d, no head] \arrow[ddd, bend left, no head, "I_p"] \\
K \arrow[d, no head, "\rho_p(I_{p,w})"] \arrow[dd, bend right, no head, "\rho_p(I_p)"'] \\
K_t \arrow[d, no head] \\
\mathbf{Q}_p^{\mathrm{nr}} \arrow[d, no head] \\
\mathbf{Q}_p
\end{tikzcd}$$

As

$$\mathrm{Gal}(K_t/\mathbf{Q}_p^{\mathrm{nr}}) = (\mathbf{Z}/p\mathbf{Z})^*$$

we may write

$$K_t = \mathbf{Q}_p^{\mathrm{nr}}(z),$$

where z is a primitive pth root of unity. If we look at $\mathrm{Gal}(K/K_t)$ we see that

$$\mathrm{Gal}(K/K_t) = \rho_p(I_{p,w})$$

consists of elements of the form

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

So this is a finite elementary abelian p-group and hence isomorphic to $(\mathbf{Z}/p\mathbf{Z})^m$ for some m.

Now we see that K is in fact

$$K = K_t(x_1^{1/p}, \ldots, x_m^{1/p}).$$

The valuations of these x_i will determine which case we are in. If

$$\nu_p(x_i) \equiv 0 \pmod{p}$$

for all i then we say that ρ_p is *peu ramifé*, otherwise if any $\nu_p(x_i)$ is coprime to p then we say it is *très ramifé*.

3 Obtaining Galois representations from modular forms

The two concepts just introduced, modular forms and Galois representation, appear at first glance not to be particularly related to each other. However in reality they are inextricably linked, and exploring the links between them will be the goal of the rest of this essay.

We will start with a historically important example that provides the first glimpse of the behaviour we will be looking at.

Example 3.1. Let

$$\Delta = \sum_{n \geq 1} \tau(n) q^n$$

be the unique normalised cusp form of weight 12 for $\Gamma_1(1) = \mathrm{SL}_2(\mathbf{Z})$. The coefficients of this q-expansion were studied in detail by Ramanujan who made many influential conjectures concerning them, and they are now known as the Ramanujan τ function. The properties of this function provide the first glimpses of behaviours that extend to more general systems of Hecke eigenvalues.

Various people, including Ramanujan (in the mod 691 case), found congruences involving the coefficients $\tau(\ell)$ for prime ℓ, modulo powers of primes. Below are a few examples for, though others exist for higher powers of these primes.

$$\tau(\ell) \equiv 1 + \ell^{11} \pmod{2^8}, \text{ if } \ell \neq 2, \tag{1}$$

$$\tau(\ell) \equiv \ell^2 + \ell^9 \pmod{3^3}, \text{ if } \ell \neq 3, \tag{2}$$

$$\tau(\ell) \equiv \ell + \ell^{10} \pmod{5^2}, \tag{3}$$

$$\tau(\ell) \equiv \ell + \ell^4 \pmod{7}, \tag{4}$$

$$\tau(\ell) \equiv \left.\begin{cases} 0 \pmod{23} & \text{if } \left(\frac{\ell}{23}\right) = -1, \\ 2 \pmod{23} & \text{if } \ell \text{ is of the form } u^2 + 23v^2, \\ -1 \pmod{23} & \text{otherwise,} \end{cases}\right\} \text{ if } \ell \neq 23, \tag{5}$$

$$\tau(\ell) \equiv 1 + \ell^{11} \pmod{691}. \tag{6}$$

The original proofs of these congruences were in many cases quite involved and did not all work in the same manner. So in order to try to explain all of these congruences in a unified manner, Serre predicted [Ser67] the existence of p-adic Galois representations ρ_p for each prime p such that

1. $\mathrm{tr}(\rho_p(\mathrm{Frob}_\ell)) = \tau(\ell)$ for all $\ell \neq p$,
2. $\det(\rho_p(\mathrm{Frob}_\ell)) = \ell^{11}$ for all $\ell \neq p$.

The congruences would then follow from these Galois representations being of specific forms. For example Eqs. (1) to (4) and (6) can all be obtained from these Galois representations if the ρ_p satisfy

$$\rho_p \equiv \begin{pmatrix} \chi_p^a & * \\ 0 & \chi_p^{11-a} \end{pmatrix} \pmod{p^b},$$

where a is 0, 2, 1, 1 or 0 respectively and b is as in the original congruences. Here in each case we can see that $\det \rho_p \equiv \chi_p^{11}$, which is consistent with Item 2 above, and knowing Item 1 in each case would give us the desired congruences.

Serre's prediction for the representation ρ_{23} has a more interesting form, but nevertheless the images of Frobenius elements can be described explicitly. Following Serre we take K to be the splitting field of $x^3 - x - 1$, this is ramified only at 23 and has Galois group S_3. We then let r be the unique irreducible degree 2 representation of S_3 taken with coefficients in $\mathbf{Q}_{23}$, this satisfies

$$\mathrm{tr}(r(\sigma)) = \begin{cases} 0 & \text{if } |\sigma| = 2, \\ 2 & \text{if } |\sigma| = 1, \\ -1 & \text{if } |\sigma| = 3, \end{cases}$$

for each $\sigma \in S_3$. As $\mathrm{Gal}(K/\mathbf{Q})$ is a quotient of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ the representation r extends to a representation of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$. If ρ_{23} exists and is isomorphic to r then this gives rise to Eq. (5) in the same way as before.

The representations were constructed for all primes p by Pierre Deligne shortly after Serre hypothesised their existence [Del69]. In doing so he also reduced Ramanujan's conjecture that $|\tau(p)| \leq 2p^{11/2}$ to the Weil conjectures. Being able to compute these associated representations makes it possible to read off many more congruences for $\tau(n)$ (see, for example, [Mas13]).

Given the above example one might wonder whether such a relationship holds more generally. Indeed Serre also asked if one could associate to each normalised cuspidal eigenform a Galois representation whose traces of Frobenius elements match the q-expansion coefficients mod p. Serre's conjectures on this led to the following more general theorem.

Theorem 3.1 (Deligne). *Let $k \geq 2$, $N \geq 1$ and $\varepsilon\colon (\mathbf{Z}/N\mathbf{Z})^* \to \overline{\mathbf{F}}_p^*$. Given a normalised cuspidal $f \in S_k(N, \varepsilon; \overline{\mathbf{F}}_p)$ there exists a two-dimensional mod p Galois representation ρ_f such that*

(i) ρ_f *is semi-simple,*

(ii) ρ_f *is unramified outside* Np,

(iii) $\mathrm{tr}(\rho_f(\mathrm{Frob}_\ell)) = a_\ell$ *for all* $\ell \nmid Np$,

(iv) $\det(\rho_f(\mathrm{Frob}_\ell)) = \varepsilon(\ell)\ell^{k-1}$ *for all* $\ell \nmid Np$.

We often refer to the representation ρ_f as arising from, or being attached to, f.

The construction of these representations in this generality is due to Deligne [Del69, Del04], building on work of Shimura and others. There is also a similar statement for weight 1 due to Deligne–Serre [DS74], however as we will be following Serre we will ignore weight 1 forms for the purposes of the conjecture.

In fact the representations obtained in these constructions are p-adic Galois representations $\rho_f\colon \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathrm{GL}_2(\mathbf{Q}_p)$, as in the example. The representations of the theorem are then obtained from the p-adic ones by reducing and semisimplifying. The mod p representations are the ones that we will be most interested in from here on however.

Remark 3.1. Looking at the representation ρ_f coming from this theorem we can see that as

$$\det(\rho_f(\mathrm{Frob}_\ell)) = \chi_p^{k-1}(\mathrm{Frob}_\ell)\varepsilon(\mathrm{Frob}_\ell)$$

for all $\ell \nmid Np$ (here viewing ε as character of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ now) and by applying Chebotarev (Theorem 2.1) we get

$$\det \rho_f = \varepsilon\chi_p^{k-1}.$$

By looking at the action of $-I_2$ on f we find $\varepsilon(c)f = \langle -1\rangle f = (-1)^k f$, and so

$$\varepsilon(c)\chi_p^{k-1}(c) = (-1)^k(-1)^{k-1} = -1,$$

hence $\det \rho_f$ must be odd (i.e ρ_f is odd).

We will look at some more properties of this construction in Section 4.3, but first we move on to the conjecture itself.

4 Serre's conjecture

4.1 The qualitative form

Given the above result it is natural to ask about the converse statement, given a Galois representation satisfying some necessary conditions, does it arise from an eigenform? Serre's conjecture was that the answer to this question is yes, all Galois representations that could possibly arise from an eigenform based on Theorem 3.1 and the remarks following it do.

The conjecture naturally comes into two parts, one weaker existence statement, and another refined form that makes exact predictions about the eigenform involved. We look at the existence statement, or *qualitative form* first.

Conjecture 4.1 (Serre's conjecture, qualitative form)**.** *Let $\rho\colon \operatorname{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathrm{GL}_2(\overline{\mathbf{F}}_p)$ be a continuous, odd, irreducible Galois representation. Then there exists a normalised cuspidal mod p eigenform f such that ρ is isomorphic to ρ_f, the Galois representation associated to f.*

This is already a very useful thing to know: any statement one could prove about Galois representations attached to modular forms, by using the theory of these forms for example, would hold for all odd 2-dimensional mod p Galois representations (see, for example, Section 6.3). One interesting consequence of this type stems from the fact that Deligne's construction of mod p Galois representations from modular forms is actually of λ-adic representations. If we were to assume Conjecture 4.1 and then use this construction, we would be able to lift all irreducible odd 2-dimensional mod p Galois representations to λ-adic representations.

This conjecture (at least for Galois representations unramified outside p) appeared much earlier than the Duke paper and is mentioned by Serre in a 1975 paper [Ser75, sec. 3]. It was computations performed by J.-F. Mestre that convinced Serre that there was a plausible strengthening of this conjecture, and this led to the form we are about to see.

A similar statement to the one above also holds for reducible representations, which correspond to Eisenstein series instead. However we do not consider this case here as it is not what the refined conjecture deals with.

4.2 The refined form

Given the above statement one might also ask about the properties of the form f whose existence is claimed. Can anything be said about the weight and level of f based only on the properties of ρ? Serre also conjectured that the answer to this question is yes. He defined a weight, level and character for each ρ, such that there should be a form f of that weight, level and character that ρ is attached to. In a slightly backwards manner we will first state this refined form of the conjecture, before moving on to motivate and define the integers $N(\rho)$, $k(\rho)$ and character

$$\varepsilon(\rho)\colon (\mathbf{Z}/N(\rho)\mathbf{Z})^* \to \overline{\mathbf{F}}_p^*$$

used in the statement.

Conjecture 4.2 (Serre's conjecture, refined form)**.** *Let* $\rho\colon \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathrm{GL}_2(\overline{\mathbf{F}}_p)$ *be a continuous, odd, irreducible Galois representation. Then there exists a normalised eigenform*

$$f \in S_{k(\rho)}(N(\rho), \varepsilon(\rho); \overline{\mathbf{F}}_p)$$

whose associated Galois representation ρ_f *is isomorphic to* ρ*.*

Moreover the $N(\rho)$ *and* $k(\rho)$ *are the minimal weight and level for which there exists such a form* f*.*

This conjecture is very bold, even given the existence statement of Conjecture 4.1 it is not clear that a minimal weight and level should exist simultaneously, let alone be given by the relatively straightforward (though intricate) description that we are about to see.

From now on we refer to a Galois representation ρ satisfying the hypotheses of this conjecture as being of *Serre-type*.

4.3 Results on Galois representations associated to modular forms

In order to try and understand which eigenforms can give rise to a particular representation, it is useful to take an arbitrary eigenform and study the properties of the representation attached to it, in an attempt to see what information about the eigenform may be recovered. Several people have obtained interesting results of this type. The following results will be helpful for our definition of the weight and level.

We fix a prime p and a normalised eigenform $f \in S_k(N, \varepsilon; \overline{\mathbf{F}}_p)$ with q-expansion

$$f = \sum_{n \geq 1} a_n q^n.$$

Let ρ_f be the mod p Galois representation attached to f by Theorem 3.1. Concerning the conductor of ρ_f there is the following result due to Carayol and Livné [Car86, Liv89].

Theorem 4.1. *Let $N(\rho_f)$ be the level associated to ρ_f (which we will define explicitly in Section 4.4), then*

$$N(\rho_f) | N.$$

Given this it is natural to hope that any Galois representation of Serre-type arises from a form of level exactly $N(\rho)$, of course we still have yet to define this quantity!

We can also make useful observations concerning the restriction of ρ_f to G_p, and its subgroups, these have implications for our definition of the weight. There are two main cases depending on whether $a_p \neq 0$ (the *ordinary* case) or otherwise (the *supersingular* case).

Theorem 4.2 (Deligne). *Suppose $2 \leq k \leq p+1$ and $a_p \neq 0$ then $\rho_f|_{\mathrm{G}_p}$ is reducible, moreover, letting $\lambda(a) \colon \mathrm{G}_p \to \overline{\mathbf{F}}_p^*$ be the unramified character of G_p that takes each $\mathrm{Frob}_p \in \mathrm{G}_p / I_p$ to $a \in \overline{\mathbf{F}}_p^*$, we have*

$$\rho_f|_{\mathrm{G}_p} \sim \begin{pmatrix} \chi_p^{k-1} \lambda(\varepsilon(p)/a_p) & * \\ 0 & \lambda(a_p) \end{pmatrix}.$$

In particular when we look at the restriction to inertia we get

$$\rho_f|_{I_p} \sim \begin{pmatrix} \chi_p^{k-1} & * \\ 0 & 1 \end{pmatrix}.$$

A proof of this result when $k \leq p$ is given in [Gro90] and the general case was originally proved in an unpublished letter from Deligne to Serre.

Now in the supersingular case we have slightly different behaviour.

Theorem 4.3 (Fontaine). *Suppose $2 \leq k \leq p+1$ and $a_p = 0$ then $\rho_f|_{\mathrm{G}_p}$ is irreducible, moreover, letting ψ_1 and ψ_2 be the two fundamental characters of level 2, we have*

$$\rho_f|_{I_p} \sim \begin{pmatrix} \psi_1^{k-1} & 0 \\ 0 & \psi_2^{k-1} \end{pmatrix}.$$

This was originally proved by Fontaine in letters to Serre in 1979. There is a published proof in [Edi92, sec. 6].

Theorem 4.4 (Mazur)**.** *Let $k = p+1$ and assume moreover that f has* filtration *$p+1$ and that ρ_f is irreducible then $\rho_f|_{G_p}$ très ramifé.*

For $p > 2$ and trivial character this is due to Mazur [Rib90, sec. 6]. In [Edi92, sec. 2] Edixhoven gives a modification to the general case.

Finally, recall that the Θ operator preserves the set of mod p normalised cuspidal eigenforms of a particular level. So we may consider how the action of Θ affects the associated Galois representations, it turns out that Θ changes this representation in a very simple way.

Proposition 4.1. *Let*

$$\Theta\colon S_k(N, \epsilon; \overline{\mathbf{F}}_p) \to S_{k+p+1}(N, \epsilon; \overline{\mathbf{F}}_p)$$

be the operator defined in Definition 2.5. Then if $f \in S_k(N, \epsilon; \overline{\mathbf{F}}_p)$ is a normalised eigenform the Galois representation associated to $\Theta(f)$ is

$$\rho_{\Theta(f)} \cong \chi_p \otimes \rho_f.$$

Proof. In Proposition 2.3 we saw that Θ took eigenforms to eigenforms, but with the eigenvalue for each T_ℓ being ℓ times the original. So

$$\mathrm{tr}(\rho_{\Theta(f)}(\mathrm{Frob}_\ell)) = \ell a_\ell = \mathrm{tr}((\chi_p \otimes \rho_f)(\mathrm{Frob}_\ell))$$

and

$$\begin{aligned} \det(\rho_{\Theta(f)}(\mathrm{Frob}_\ell)) &= \ell^{k+p+1}\varepsilon(\ell) \\ &= \ell^{k+1}\varepsilon(\ell) \\ &= \ell^2\ell^{k-1}\varepsilon(\ell) \\ &= \det((\chi_p \otimes \rho_f)(\mathrm{Frob}_\ell)). \end{aligned}$$

By Chebotarev and Brauer–Nesbitt we have that the representations involved are isomorphic. □

So if $p \nmid k$ then applying Θ shifts the level up by $p+1$ and twists the associated representation by χ_p.

It is worth noting that proofs of some of the above theorems are very involved and actually came after Serre's paper. However it seems likely that observations of these results in specific examples informed the recipe below.

4.4 The optimal level

Assume that we have a Galois representation $\rho\colon \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathrm{GL}_2(\overline{\mathbf{F}}_p)$ of Serre-type. We now define the integer $N(\rho) \geq 1$ which plays the role of the optimal level in the refined conjecture.

We can equivalently view our representation ρ as a homomorphism

$$\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathrm{Aut}(V),$$

where V is a two-dimensional $\overline{\mathbf{F}}_p$ vector space. Letting $\mathrm{G}_{\ell,i} \subset \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ be the ith ramification group at ℓ for a prime ℓ, as defined in Definition 2.8, we can consider the fixed subspace of V for each ℓ and i,

$$V^{\ell,i} = \{v \in V : \rho(\sigma)v = v \;\forall \sigma \in \mathrm{G}_{\ell,i}\}.$$

For each ℓ we can then define

$$\nu_\ell(\rho) = \sum_{i=0}^{\infty} \frac{1}{[\mathrm{G}_{\ell,0} : \mathrm{G}_{\ell,i}]} \dim\left(V/V^{\ell,i}\right),$$

this quantity is (non-trivially) an integer [GS95, p. 99].

We then define our level by

$$N(\rho) = \prod_{\substack{\ell \neq p \\ \ell \text{ prime}}} \ell^{\nu_\ell(\rho)},$$

which is indeed a positive integer, by construction it is coprime to p. This definition is almost that of the *Artin conductor* of a representation, but here the p part is ignored.

Remark 4.1. Unwinding this definition when ρ is unramified at some ℓ, we see that each $V^{\ell,i}$ is in fact the whole of V, as the ramification groups involved are trivial. Hence in this case $\nu_\ell(\rho) = 0$ and so $N(\rho)$ is only divisible by the primes $\ell \neq p$ at which ρ is ramified.

Theorem 4.1 stated that when ρ comes from a modular form f the integer $N(\rho)$ defined here divides the level of f. With that in mind conjecturing that any Serre-type representation comes from one of level exactly $N(\rho)$ is fairly logical, though perhaps optimistic.

4.5 The character and the weight mod $p-1$

Beginning with a Galois representation of Serre-type, as before, we now define the character

$$\varepsilon(\rho)\colon (\mathbf{Z}/N(\rho)\mathbf{Z})^* \to \overline{\mathbf{F}}_p^*.$$

We also state the class of $k(\rho)$ mod $p-1$, though the full definition of $k(\rho)$ will be given in the next section.

Given a continuous mod p Galois representation ρ we can compose with the determinant map to obtain a continuous character

$$\det\rho\colon \operatorname{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \overline{\mathbf{F}}_p^*.$$

As outlined in Remark 2.1 the image of a continuous mod p Galois representation is finite. Hence the image of $\det\rho$ is a finite multiplicative subgroup of a field, so the image is cyclic.

We now compute the conductor of $\det\rho$. Let V_1 be the 2-dimensional vector space realising ρ and V_2 be the 1-dimensional vector space realising $\det\rho$. If $\det\rho|_{G_{\ell,i}}$ is not trivial then $\rho|_{G_{\ell,i}}$ cannot be trivial, hence $\dim(V_2/V_2^{\ell,i}) > 0$ implies $\dim(V_1/V_1^{\ell,i}) > 0$. As $0 \leq \dim(V_2/V_2^{\ell,i}) \leq 1$ we get that

$$\dim(V_2/V_2^{\ell,i}) \leq \dim(V_1/V_1^{\ell,i})$$

for all ℓ and i, and hence

$$\nu_\ell(\det\rho) \leq \nu_\ell(\rho).$$

This gives us that

$$N(\det\rho) \mid N(\rho).$$

As the restriction of $\det\rho$ to $I_{p,w}$ is trivial (see the proof of Proposition 4.2, using that characters are simple) we find that $\nu_p(\det\rho) \leq 1$. So the full Artin conductor of $\det\rho$ (i.e. the conductor as introduced earlier, but including the p-part now) divides $pN(\rho)$.

The Artin conductor of a 1-dimensional Galois representation is actually equal to the conductor of the associated Dirichlet character [GS95, p. 228]. We can therefore identify $\det\rho$ with a homomorphism

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

or equivalently with a pair of homomorphisms

$$\phi\colon (\mathbf{Z}/p\mathbf{Z})^* \to \overline{\mathbf{F}}_p^*,$$

$$\varepsilon\colon (\mathbf{Z}/N(\rho)\mathbf{Z})^* \to \overline{\mathbf{F}}_p^*.$$

The group $(\mathbf{Z}/p\mathbf{Z})^*$ is cyclic of order $p-1$ and so the image of ϕ lies inside $\mathbf{F}_p^*$. So ϕ is an endomorphism of the cyclic group $(\mathbf{Z}/p\mathbf{Z})^*$ and hence of the form

$$x \mapsto x^h,$$

for some $h \in \mathbf{Z}/(p-1)\mathbf{Z}$. So we have expressed that $\phi = \chi_p^h$, where χ_p is the mod p cyclotomic character.

We have now written

$$\det \rho = \varepsilon \chi_p^h$$

and so, comparing with Remark 3.1, we set $\varepsilon(\rho)$ to be the ε obtained here. We also see that h had better be the same as $k(\rho) - 1$ modulo $p-1$. Now all we have left to do is define the actual value of $k(\rho)$, knowing its class mod $p-1$.

4.6 The optimal weight

We now come to the final ingredient in Serre's recipe, that of the weight $k(\rho)$.

The general strategy of our approach is to express a representation of Serre-type as a twist of another representation, one that looks like it comes from a cusp form. We then read off the minimal weight of a cusp form that could give this twisted representation. Then we can apply the results above regarding the Θ operator (Proposition 4.1) to define the weight of the original representation.

Given our Galois representation

$$\rho\colon \operatorname{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \operatorname{Aut}(V)$$

recall from Section 2.2 that we can form a representation of G_p by composing with a restriction map $\mathrm{G}_p \to \operatorname{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$, to obtain

$$\rho_p\colon \mathrm{G}_p \to \operatorname{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \operatorname{Aut}(V).$$

The definition of $k(\rho)$ will only depend on this ρ_p (in fact only on $\rho_p|_{I_p}$). As such the weight will only reflect the behaviour at p of the representation, whereas the level reflected the behaviour away from p. We will from here on refer to $k(\rho)$ as $k(\rho_p)$ to emphasise this fact.

Proposition 4.2. *(Serre [Ser72, prop. 4]) The semisimplification ρ^{ss} of ρ is trivial when restricted to $I_{p,w}$.*

Proof. It suffices to prove this for simple representations ρ, as a sum of trivial representations is trivial.

The wild inertia $I_{p,w}$ is a pro-p-group, and so the image is also a pro-p-group. This group is finite, so it is simply a p-group, and defined over some finite field $\mathbf{F}_q$. Consider $\mathbf{F}_q$-vector space V that realises $\rho^{\mathrm{ss}}|_{I_{p,w}}$, additively V is a p-group too. Looking at the action of $\rho^{\mathrm{ss}}|_{I_{p,w}}$ on V we see that there is a singleton orbit $\{0\}$. As all orbits are of p-power order there must be an additional $p-1$ singleton orbits at least, else the orbits could not partition V. Therefore the fixed subspace W of V is non-trivial. However as $I_{p,w}$ is normal in G_p the subspace W is stable under G_p, hence must equal V by simplicity. □

We may therefore view ρ^{ss} as a representation of $I_{p,t}$ we shall write ρ_t^{ss} for this new representation. The tame inertia group is an abelian, and so this representation is diagonalisable. The representation ρ_t^{ss} is therefore given by a pair of characters

$$\phi_1,\, \phi_2 \colon I_{p,t} \to \overline{\mathbf{F}}_p^*.$$

Proposition 4.3. *Both of the characters ϕ_1 and ϕ_2 are of the same level, and that level is either 1 or 2.*

Moreover if they are both of level 2 then they are pth powers of each other.

Proof. Letting a Frobenius element at p act by conjugation on $\sigma \in I_p$ we see that

$$\mathrm{Frob}_p\, \sigma\, \mathrm{Frob}_p^{-1} \equiv \sigma^p \pmod{I_{p,w}},$$

and so

$$\rho_t^{\mathrm{ss}}(\mathrm{Frob}_p)\rho_t^{\mathrm{ss}}(\sigma)\rho_t^{\mathrm{ss}}(\mathrm{Frob}_p^{-1}) = \rho_t^{\mathrm{ss}}(\mathrm{Frob}_p\, \sigma\, \mathrm{Frob}_p^{-1}) = \rho_t^{\mathrm{ss}}(\sigma^p) = \rho_t^{\mathrm{ss}}(\sigma)^p,$$

so we have an equivalence of representations

$$\rho_t^{\mathrm{ss}} \cong (\rho_t^{\mathrm{ss}})^p.$$

Hence the set $\{\phi_1,\, \phi_2\}$ must be fixed by pth powering.

We then have two possibilities, either taking the pth power fixes each of ϕ_1 and ϕ_2 or it swaps them. If they are both fixed then their images lie in the prime field, so they are of level 1. Otherwise, if they swap under pth powering, each of them is fixed under powering by p^2, and hence they are of level 2. □

We now treat three different cases separately, based on the levels of the characters just obtained and whether or not $\rho|_{I_{p,w}}$ is trivial.

4.6.1 The level 2 case

If the two characters ϕ_1 and ϕ_2 are of level 2 then ρ is irreducible.

To see this, assume otherwise and consider some fixed subspace of the vector space realising ρ. This space must be 1-dimensional, so the representation acts by a character ϕ. The character is defined on G_p, hence we have

$$\phi(\sigma) = \phi(\mathrm{Frob}_p\, \sigma\, \mathrm{Frob}_p^{-1}) = \phi^p(\sigma)$$

so elements in the image of ϕ are fixed by pth powering. Hence ϕ must factor through $\mathbf{F}_p^*$, i.e. ϕ is of level 1, which is a contradiction.

So $\rho = \rho^{\mathrm{ss}}$ and the characters ϕ_1 and ϕ_2 above define the representation ρ. We can write them in terms the fundamental characters of level 2, ψ_1 and ψ_2, (as defined in Definition 2.13) and use this description to define $k(\rho_p)$. Specifically we can write ϕ_1 as

$$\phi_1 = \psi_1^a \psi_2^b$$

with $0 \leq a,\, b \leq p-1$. If $a = b$ then $\phi_1 = (\psi_1\psi_2)^a$, which contradicts ϕ_1 being of level 2 as $\psi_1\psi_2$ is a level 1 character (see Remark 2.3). Now we observe that

$$\phi_2 = \phi_1^p = (\psi_1^a\psi_2^b)^p = \psi_2^a\psi_1^b,$$

so by switching the places of ϕ_1 and ϕ_2 we may assume that in fact $0 \leq a < b \leq p-1$. So

$$\rho_p \sim \begin{pmatrix} \psi_1^b\psi_2^a & 0 \\ 0 & \psi_1^a\psi_2^b \end{pmatrix}.$$

This now looks a bit like the supersingular case of Theorem 4.3. So we massage our representation into the form seen in the theorem by factoring some characters out of ρ^{ss} to get

$$\rho_p \sim \begin{pmatrix} \psi_1^b\psi_2^a & 0 \\ 0 & \psi_1^a\psi_2^b \end{pmatrix} = \psi_2^a\psi_1^a \begin{pmatrix} \psi_1^{b-a} & 0 \\ 0 & \psi_2^{b-a} \end{pmatrix} = \chi_p^a \begin{pmatrix} \psi_1^{b-a} & 0 \\ 0 & \psi_2^{b-a} \end{pmatrix}.$$

If we were just considering the matrix on the right we would like to set $k(\rho_p) - 1 = b - a$, however we have twisted by χ_p^a. Recalling Proposition 4.1 we make the definition

$$k(\rho_p) - 1 = b - a + a(p+1),$$

or equivalently

$$k(\rho_p) = 1 + pa + b. \tag{7}$$

As we have $0 \leq a < b \leq p-1$ we see that

$$2 \leq k(\rho_p) \leq 1 + p(p-2) + p - 1 = p^2 - p.$$

4.6.2 The level 1 tame case

Assuming ϕ_1 and ϕ_2 are of level 1 and the action of I_p on V is semisimple we can write

$$\rho_p|_{I_p} \sim \begin{pmatrix} \phi_1 & 0 \\ 0 & \phi_2 \end{pmatrix} = \begin{pmatrix} \chi_p^b & 0 \\ 0 & \chi_p^a \end{pmatrix}.$$

So we obtain integers a and b defined modulo $p-1$, we can assume that $0 \leq a \leq b \leq p-2$ by switching ϕ_1 and ϕ_2 if necessary. This looks a little like the ordinary case we covered in Theorem 4.2. So we factor out a character again to get something that looks exactly like that theorem,

$$\rho_p|_{I_p} \sim \begin{pmatrix} \chi_p^b & 0 \\ 0 & \chi_p^a \end{pmatrix} = \chi_p^a \begin{pmatrix} \chi_p^{b-a} & 0 \\ 0 & 1 \end{pmatrix}.$$

If we just had the right hand matrix we would want to set $k(\rho_p) - 1 = b - a$, but once again we have a twist. Taking this into account we try to set

$$k(\rho_p) - 1 = b - a + a(p+1),$$

or equivalently

$$k(\rho_p) = 1 + pa + b$$

as above, but there is a small issue this time. It is possible that $a = b = 0$, in which case this definition would give us $k(\rho_p) = 1$, however we do not wish to consider weight 1 forms at all here, so our formula needs modifying in this case. Looking at Section 4.5 and Proposition 2.1 we see that it is only permissible to change the weight by multiples of $p-1$. So to remedy the situation we add $p-1$ when we are in the problem case. The definition in this case is then

$$k(\rho_p) = \begin{cases} 1 + pa + b & \text{if } (a, b) \neq (0, 0), \\ p & \text{if } (a, b) = (0, 0). \end{cases} \tag{8}$$

With this definition we have

$$2 \leq k(\rho_p) \leq 1 + p(p-2) + p - 2 = p^2 - p - 1,$$

unless $p = 2$, where the above inequality makes no sense, in which case $k(\rho_p) = 2$ is the only possibility.

4.6.3 The level 1 non-tame case

The final case is where ϕ_1 and ϕ_2 are of level 1 but the action of $I_{p,w}$ on V is not trivial.

If we consider the subspace of V fixed by $I_{p,w}$ the same argument we used in Proposition 4.2 shows that there is a non-trivial subspace of V fixed by $I_{p,w}$. However $I_{p,w}$ is assumed to act non-trivially and so $V^{I_{p,w}}$ is a 1-dimensional subspace. This subspace is stable under the action of G_p as is the space $V/V^{I_{p,w}}$, so we may write

$$\rho_p \sim \begin{pmatrix} \theta_2 & * \\ 0 & \theta_1 \end{pmatrix},$$

where θ_1 and θ_2 are characters.

We can then decompose θ_1 and θ_2 as $\chi_p^\beta \varepsilon_1$ and $\chi_p^\alpha \varepsilon_2$ respectively, where ε_1 and ε_2 are unramified characters and $\alpha, \beta \in \mathbf{Z}/(p-1)\mathbf{Z}$. Using this decomposition we see that on restricting to I_p we have

$$\rho_p|_{I_p} \sim \begin{pmatrix} \chi_p^\beta & * \\ 0 & \chi_p^\alpha \end{pmatrix}.$$

We fix representatives α and β now such that

$$0 \leq \alpha \leq p-2,$$
$$1 \leq \beta \leq p-1.$$

We can then proceed as normal, observing that

$$\rho_p|I_p \sim \begin{pmatrix} \chi_p^\beta & * \\ 0 & \chi_p^\alpha \end{pmatrix},$$

then factoring out a twist by χ_p^a to get

$$\rho_p|I_p \sim \chi_p^\alpha \begin{pmatrix} \chi_p^{\beta-\alpha} & * \\ 0 & 1 \end{pmatrix}.$$

We then see that the representation given by the right hand matrix at first glance looks like it comes from an eigenform of weight $\beta - \alpha + 1$. However if $\beta - \alpha = 1$ this representation could have come from a form of weight $\beta - \alpha + p$ instead, as we are unable to tell the difference between 2 and $p + 1 \bmod p - 1$.

This is a real problem as it is incorrect to simply use the smallest weight here (or the largest for that matter). For example, let ρ be the mod 11 representation arising from the mod 11 reduction of the eigenform Δ of weight 12. This representation is unramified outside of 11 and so $N(\rho) = 1$. Then, as the 11th Fourier coefficient of Δ is $534612 \equiv 1 \pmod{11}$, Theorem 4.2 tells us that

$$\rho|_{I_{11}} \sim \begin{pmatrix} \chi_{11}^{11} & * \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} \chi_{11} & * \\ 0 & 1 \end{pmatrix}.$$

So if we use $\beta - \alpha + 1$ for our definition here this would predict the existence of a mod 11 eigenform of weight 2 and level 1 from which ρ arises, but there are no such forms.

If $\beta \neq \alpha + 1$ we do not have this problem, so Serre lets

$$a = \min(\alpha, \beta),$$
$$b = \max(\alpha, \beta).$$

and defines, as we did in Section 4.6.1,

$$k(\rho_p) = 1 + pa + b. \tag{9}$$

When $\beta = \alpha + 1$ we have to deal with the ambiguity by finding some way of distinguishing representations that come from eigenforms of weight 2 and $p + 1$. In order to decide case we are in we can make use of Theorem 4.4. This theorem stated that if a Galois representation arises from a filtration $p + 1$ form, then the representation at p is très ramifé.

So if ρ_p is peu ramifé this cannot be the case, and the twist of ρ_p looks like it came from an eigenform of weight 2 rather than $p + 1$. We then define $k(\rho_p)$ as we did earlier via

$$k(\rho_p) = 1 + pa + b = 2 + \alpha(p + 1). \tag{10}$$

If ρ_p is très ramifé then it looks as if the twist comes from a form of weight $p + 1$. So we make an analogous definition to what we have done before, simply accounting for the twist starting from a weight $p + 1$ form. We have one final issue to deal with, if $p = 2$ this definition would give $k(\rho_p) = 3$, we don't like this either so we make it 4. In the end we obtain the following definition

$$k(\rho_p) = \begin{cases} 1 + pa + b + p - 1 = p + 1 + \alpha(p + 1) & \text{if } p \neq 2, \\ 4 & \text{if } p = 2. \end{cases} \tag{11}$$

Looking at the bounds for $k(\rho_p)$ now we see that if $\beta \neq \alpha + 1$ or if ρ_p is peu ramifé then for all p

$$2 \leq k(\rho_p) \leq 1 + p(p-2) + p - 1 = p^2 - p.$$

Otherwise for the très ramifé case we get

$$2 \leq k(\rho_p) \leq p^2 - p + p - 1 = p^2 - 1,$$

unless $p = 2$ where $k(\rho_p) = 4$ instead.

Considering all cases together we see that $k(\rho_p)$ has range of

$$2 \leq k(\rho_p) \leq p^2 - p$$

for odd p, and $k(\rho_p) \in \{2, 4\}$ for $p = 2$.

To see why this approach might be expected to produce the minimal weight when twisting is involved depends on analysis of the sequences of filtrations

$$w(\Theta^i f),\ 0 \leq i \leq p+1,$$

for different mod p eigenforms f. These sequence is known as a Θ-cycle and

4.7 A counterexample

In fact the conjecture exactly as stated above is in fact *incorrect* in general, this was noted by Serre in a letter to K. Ribet in 1987. The following counterexample is due to Serre and is given in [Rib95, sec. 2] and also in [RS11, sec. 21.6.1] which we follow here (see also the notes for Serre's paper in his collected papers).

Example 4.1. Let α be a root of $x^2 + 3x + 3$, then $\mathbf{Q}(\alpha) = \mathbf{Q}(\sqrt{-3})$. The space $S_2(13; \overline{\mathbf{Z}})$ is spanned by the normalised eigenform

$$q + (-\alpha - 3)q^2 + (2\alpha + 2)q^3 + (\alpha + 2)q^4 + (-2\alpha - 3)q^5 + O(q^6)$$

and its $\mathrm{Gal}(\mathbf{Q}(\alpha)/\mathbf{Q})$ conjugate form

$$q + \alpha q^2 + (-2\alpha - 4)q^3 + (-\alpha - 1)q^4 + (2\alpha + 3)q^5 + O(q^6),$$

which is the other normalised eigenform in $S_2(13; \overline{\mathbf{Z}})$.

If we look at the associated mod 3 Galois representation it has determinant $\chi_3\phi$ where ϕ is the Galois character coming from the extension $\mathbf{Q}(\sqrt{13})/\mathbf{Q}$. Serre's conjecture tells us that this character is our $\varepsilon(\rho)$ and so ρ should arise from some eigenform f in $S_2(13, \phi; \overline{\mathbf{F}}_3)$. If we let H be the group of squares in $(\mathbf{Z}/13\mathbf{Z})^*$ then such an f may be viewed as an modular form of weight 2 for the group

$$\Gamma_H(13) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbf{Z}) : c \equiv 0 \pmod{13},\, d \in H \right\}.$$

While we did not define mod p modular forms for more general congruence subgroups, the definition is the same. However the space of weight 2 cusp forms on $\Gamma_H(13)$ is zero, and so f does not exist.

This problem is fairly isolated and only arises when we work with mod 2 Galois representations, or mod 3 Galois representations that have abelian restriction to $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}(\sqrt{-3})$. In order to fix this issue using our definition of modular forms it is necessary to change the definition of the character in these cases. This is slightly as the definition of the character was rather clean and simple before.

4.8 The proof

As mentioned at the start, this conjecture is in fact now a theorem, due to Khare and Wintenberger using results of Kisin.

For $p \neq 2$ it was known that the qualitative and refined forms were equivalent before either was known in general. This reduction of the refined form to the qualitative form was incremental and is due to a large number of people, for example Ribet [Rib94] lists N. Boston, H. Carayol, F. Diamond, B. Edixhoven, G. Faltings, B. H. Gross, B. Jordan, K. Ribet, H. W. Lenstra, Jr., R. Livné, B. Mazur and J-P. Serre. This was completed by Diamond around 1993 [Dia95]. The missing case of $p = 2$ was completed by Khare and Wintenberger as part of their proof of the conjecture.

Many special cases of Serre's conjecture were also known long before the general case. Indeed John Tate proved the $p = 2$ unramified case in 1973, 14 years before the Duke paper [Tat94]. Serre himself used similar techniques to prove the $p = 3$ case (published as a note on page 710 of his collected works volume III). As we saw in Section 6.2 for these small cases what needs to be shown is that no such Galois representations exist, to match the lack of cusp forms of level 1 for weights less than 12. It is interesting to note that these proofs were not completely subsumed or rendered obsolete by the the proof of Khare–Wintenberger. Rather they help form the base case for an induction type argument which gives the full conjecture.

Regarding the difficulties with the character mentioned in Section 4.7 it is shown in ???? that if the refined version without the character condition holds then it holds with a modified character condition. The main theorems of [KW09a, KW09b] do not mention the character at all but combining them with the work of ???? gives the full Conjecture 4.2 excepting the cases discussed.

5 Examples

One of the great things about Serre's conjecture, even if it were not yet known to be correct, is the fact that it can be used in specific cases easily. Specifically, given a Galois representation of Serre-type we can calculate the optimal weight and level along with the character as detailed above, then in many instances we can compute the associated space of modular forms and look for a form from which our Galois representation arises.

Example 5.1. Let's return first to Example 3.1 which concerned the cusp form Δ, and check that everything we have just done is consistent with what we saw there.

We consider the 23-adic Galois representation ρ_{23} as out of the representations we considered there this is the only irreducible one. Recall that this was defined by taking K to be the splitting field of $x^3 - x - 1$, which is ramified only at 23 and has Galois group S_3. We then took r be the unique irreducible degree 2 representation of S_3 taken with coefficients in $\mathbf{Q}_{23}$, this satisfies

$$\operatorname{tr}(r(\sigma)) = \begin{cases} 0 & \text{if } |\sigma| = 2, \\ 2 & \text{if } |\sigma| = 1, \\ -1 & \text{if } |\sigma| = 3, \end{cases}$$

for each $\sigma \in S_3$. The Galois representation ρ_{23} was then the composition

$$\operatorname{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \operatorname{Gal}(K/\mathbf{Q}) \xrightarrow{\sim} S_3 \to \operatorname{GL}_2(\mathbf{Q}_{23}).$$

In order to use Serre's conjecture we need a mod p representation so we reduce mod 23 to obtain $\rho = \overline{\rho}_{23}$.

Straight away we see that $N(\rho) = 1$ due to the fact K is unramified outside 23, see Remark 4.1.

In order to determine $k(\rho)$ we need to study the local representation at 23.

So ρ should have arisen from a normalised eigenform

$$f \in S_{12}(1, \mathrm{Id}; \overline{\mathbf{F}}_p) = \overline{\mathbf{F}}_p \cdot \overline{\Delta},$$

as we would hope.

Now we move to a new example, once again arising from the Galois group of a number field.

Example 5.2. Take the K to be the splitting field of

$$f = x^4 + ??x + ??.$$

This has Galois group A_4 and we may consider the restriction map

$$\rho\colon \operatorname{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \operatorname{Gal}(K/\mathbf{Q}) \simeq A_4.$$

We can turn this into a mod 2 Galois representation using the fact that A_4 is isomorphic to $\mathrm{GL}_2(\mathbf{F}_4)$ via the identification

$$(1,2) \mapsto \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix},\ (1,3) \mapsto \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}.$$

So, viewing ρ as a mod 2 Galois representation, what does Serre have to say about it? Well for starters $N(\rho)$ should be the odd part of disc $K =$, which is ??.

So ρ should come from some eigenform $f \in S_?(?, ?; \overline{\mathbf{F}}_2)$. We can explicitly compute this space using, for example, Sage [S+15]. Doing this gives us that

$$S_?(?, ?; ?) = \overline{\mathbf{F}}_2 \cdot f.$$

6 Consequences

Serre's conjecture is a strong statement that implies many other difficult results within number theory. We now mention briefly a few of these. While some of these results were obtained via other means long before Serre's conjecture was shown in general they still serve to demonstrate the power and usefulness of the conjecture.

6.1 Finiteness of classes of Galois representations

First let us examine a very direct consequence. Fix a prime p and an integer N and consider Serre-type Galois representations

$$\rho\colon \operatorname{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathrm{GL}_2(\overline{\mathbf{F}}_p)$$

whose conductors $N(\rho)$ divide N. Serre's conjecture states that each corresponds to some normalised mod p eigenform of level $N(\rho)|N$ and weight $k(\rho)$ in the range $[2, p^2 - 1]$ (or $\{2, 4\}$ for $p = 2$). However there are only finitely many spaces of forms satisfying these requirements and only finitely many normalised eigenforms in each. Therefore for each prime p and integer N there are only finitely many isomorphism classes of mod p Serre-type Galois representations of conductor dividing N. Apparently there are no alternative methods of proving this result currently known [Wie13].

6.2 Unramified mod p Galois representations for small p

We can specialise the previous type of direct argument further to get more control over the number of representations with particular properties. In fact we can get enough control to prove the following non-existence result.

Let ρ be a Serre-type mod p Galois representation for some $p \leq 7$ that is unramified outside of p. In this case, due to the absence of ramification, $N(\rho)$ is simply 1 (recall Remark 4.1). The idea of our definition of the weight was that each Galois representation ρ should be the twist by a power of the cyclotomic character of another form ρ', such that $2 \leq k(\rho') \leq p + 1$.

So Serre's conjecture predicts there is some mod p cusp form of level 1 and weight ≤ 8 from which some twist of ρ arises. But there are no cusp forms of level 1 of weight < 12 and so such a twisted representation cannot exist, hence the original ρ cannot exist either.

6.3 The Artin conjecture

Definition 6.1. An *Artin representation* is a complex Galois representation

$$\rho\colon \operatorname{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathrm{GL}_2(\mathbf{C}).$$

We may consider the L-function

$$L(s, \rho) = \prod_p L_p(s, \rho) = \prod_p \frac{1}{\det(I_n - p^{-s}\rho(\mathrm{Frob}_p)|_{V^{p,0}})}.$$

Given any $L(s,\rho)$ we introduce a related function which has a nice functional equation. We define

$$\Lambda(s,\rho) = N^{s/2}(2\pi)^{-s}\Gamma(s)L(s,\rho),$$

where N is the Artin conductor, recalling the notation of Section 4.4 this is given by

$$N = \prod_p p^{\nu_p(\rho)},$$

the product running over all p now. This function satisfies

$$\Lambda(1-s,\rho) = W(\rho)\Lambda(s,\rho),$$

where $W(\rho)$ is a constant of absolute value 1, called the *Artin root number*.

The following conjecture is a major open question concerning this function that dates back to ???.

Conjecture 6.1 (Weak Artin conjecture)**.** *Let*

$$\rho\colon \operatorname{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \operatorname{GL}_n(\mathbf{C})$$

be an Artin representation, then the meromorphic continuation of

$$\Lambda(s,\rho)$$

to the complex plane is holomorphic on the whole of $\mathbf{C}$*.*

In fact this follows from another related conjecture.

Conjecture 6.2 (Strong Artin conjecture)**.** *Any Artin representation*

$$\rho\colon \operatorname{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \operatorname{GL}_n(\mathbf{C}),$$

is modular, in the sense that it

As the L-function of a ??

Proposition 6.1. *Serre's conjecture implies the strong Artin conjecture for odd 2-dimensional Artin representations.*

Proof. Given an odd Artin representation

$$\rho\colon \operatorname{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \operatorname{GL}_2(\mathbf{C})$$

□

6.4 Modularity of abelian varieties

In this section we look briefly at another strong result that follows from Serre's conjecture, despite it not obviously concerning the objects related in the conjecture. This was a genuinely new result that was not known before the proof of Serre's conjecture and so serves as a good example of the usefulness of the conjecture outside of its immediate domain. Going into detail would take us too far afield so this section is necessarily sketch-like and without background material. For more details see [Rib04] or [RS11, chap. 15].

Definition 6.2. An abelian variety A over $\mathbf{Q}$ is modular if there is a surjection defined over $\mathbf{Q}$

$$J_1(N) \twoheadrightarrow A,$$

for some N.

Definition 6.3. An abelian variety A defined over $\mathbf{Q}$ is said to be of GL_2-*type* if its endomorphism algebra

$$\mathbf{Q} \otimes \mathrm{End}_{\mathbf{Q}}(A)$$

contains a number field E whose degree is equal to the dimension of A.

Example 6.1. Elliptic curves are of GL_2-type because all endomorphism rings over characteristic 0 fields of elliptic curves contain $\mathbf{Z}$ and hence

$$\mathbf{Q} \subset \mathbf{Q} \otimes \mathrm{End}_{\mathbf{Q}}(E).$$

Ken Ribet has shown [Rib04] that Serre's conjecture implies the following nice classification of which abelian varieties are modular.

Theorem 6.1. *Every abelian variety of* GL_2*-type is modular.*

This theorem implies the Taniyama–Shimura–Weil conjecture, or modularity theorem, first proved by Breuil, Conrad, Diamond and Taylor in 2001 [BCDT01]. However this modularity statement is significantly stronger and uses the full power of Serre's conjecture.

7 References

[BCDT01] Christophe Breuil, Brian Conrad, Fred Diamond, and Richard Taylor. On the modularity of elliptic curves over $\mathbf{Q}$: wild 3-adic exercises. *Journal of the American Mathematical Society*, pages 843–939, 2001.

[Cai09] Bryden Cais. Serre's conjectures. `http://math.arizona.edu/~cais/Papers/Expos/Serre05.pdf`, November 2009.

[Car86] Henri Carayol. Sur les représentations l-adiques associées aux formes modulaires de Hilbert. *Annales Scientifiques de l'Ecole Normale Supérieure*, 19(3):409–468, 1986.

[Coh08] Henri Cohen. *Number Theory: Volume I: Tools and Diophantine Equations*. Graduate Texts in Mathematics. Springer New York, 2008.

[Dar95] Henri Darmon. Serre's conjectures. In Vijaya Kumar Murty, editor, *Seminar on Fermat's Last Theorem: 1993-1994, the Fields Institute for Research in the Mathematical Sciences, Toronto, Ontario, Canada*, volume 17 of *CMS conference proceedings*, pages 135–153. American Mathematical Society, 1995.

[Del69] Pierre Deligne. Formes modulaires et représentations ℓ-adiques. *Séminaire Bourbaki*, 11:139–172, 1968-1969.

[Del04] Pierre Deligne. Formes modulaires et représentations ℓ-adiques (translation). `http://publications.ias.edu/sites/default/files/5_FormesModulaires.pdf`, June 2004.

[Dia95] Fred Diamond. The refined conjecture of Serre. In J. Coates and S. Yau, editors, *Elliptic curves, modular forms, and Fermat's last theorem*, pages 172–186, 1995.

[DS74] Pierre Deligne and Jean-Pierre Serre. Formes modulaires de poids 1. *Annales scientifiques de l'cole Normale Suprieure*, 7(4):507–530, 1974.

[Edi92] Bas Edixhoven. The weight in Serre's conjectures on modular forms. *Inventiones mathematicae*, 109(1):563–594, 1992.

[Edi97] Bas Edixhoven. Serre's conjecture. In Gary Cornell, Joseph H. Silverman, and Glenn Stevens, editors, *Modular Forms and Fermat's Last Theorem*, pages 209–242. Springer New York, 1997.

[Ghi] Alex Ghitza. On the two-dimensional modular representations of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ (translation). `http://www.ms.unimelb.edu.au/~aghitza/nuts/serre.pdf`.

[Gro90] Benedict H. Gross. A tameness criterion for Galois representations associated to modular forms (mod p). *Duke Mathematical Journal*, 61(2):445–517, 1990.

[GS95] Marvin J. Greenberg and Jean-Pierre Serre. *Local Fields*. Graduate Texts in Mathematics. Springer New York, 1995.

[Joc82] Naomi Jochnowitz. A study of the local components of the Hecke algebra mod l. *Transactions of the American Mathematical Society*, 270(1):253–267, 1982.

[Kis09] Mark Kisin. Modularity of 2-adic Barsotti-Tate representations. *Inventiones mathematicae*, 178(3):587–634, 2009.

[KW09a] Chandrashekhar Khare and Jean-Pierre Wintenberger. Serre's modularity conjecture (I). *Inventiones mathematicae*, 178(3):485–504, 2009.

[KW09b] Chandrashekhar Khare and Jean-Pierre Wintenberger. Serre's modularity conjecture (II). *Inventiones mathematicae*, 178(3):505–586, 2009.

[Liv89] Ron Livné. On the conductors of mod l Galois representations coming from modular forms. *Journal of Number Theory*, 31(2):133–141, 1989.

[Mas13] Nicolas Mascot. Computing modular Galois representations. *Rendiconti del Circolo Matematico di Palermo*, 62(3):451–476, 2013.

[Rib90] Kenneth A. Ribet. On modular representations of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ arising from modular forms. *Inventiones mathematicae*, 100(1):431–476, 1990.

[Rib94] Kenneth A. Ribet. Report on mod l representations of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$. In *Proceedings of Symposia in Pure Mathematics*, volume 55, pages 639–676, 1994.

[Rib95] Kenneth A. Ribet. Irreducible Galois representations arising from component groups of Jacobians. In J. Coates and S. Yau, editors, *Elliptic curves, modular forms, and Fermat's last theorem*, pages 131–147, 1995.

[Rib04] Kenneth A. Ribet. Abelian Varieties over $\mathbf{Q}$ and Modular Forms. In John E. Cremona, Joan-Carles Lario, Jordi Quer, and Kenneth A. Ribet, editors, *Modular Curves and Abelian Varieties*, volume 224 of *Progress in Mathematics*, pages 241–261. Birkhuser Basel, 2004.

[RS99] Kenneth A. Ribet and William A. Stein. Lectures on Serre's conjectures. In B.D. Conrad and K. Rubin, editors, *Arithmetic Algebraic Geometry*, IAS Park City mathematics series: Institute for Advanced Study, pages 143–232. American Mathematical Soc., 1999.

[RS11] Kenneth A. Ribet and William A. Stein. Lectures on modular forms and Hecke operators. `http://wstein.org/books/ribet-stein/main.pdf`, November 2011.

[S$^+$15] W. A. Stein et al. *Sage Mathematics Software (Version 6.5)*. The Sage Development Team, 2015. `http://www.sagemath.org`.

[Ser67] Jean-Pierre Serre. Une interprétation des congruences relatives à la fonction τ de Ramanujan. *Séminaire Delange-Pisot-Poitou. Théorie des nombres*, 9(1):1–17, 1967.

[Ser72] Jean-Pierre Serre. Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. *Inventiones mathematicae*, 15(4):259–331, 1972.

[Ser73a] Jean-Pierre Serre. Congruences et formes modulaires (d'après H.P.F. Swinnerton-Dyer). In *Séminaire Bourbaki vol. 1971/72 Exposés 400–417*, pages 319–338. Springer, 1973.

[Ser73b] Jean-Pierre Serre. Formes modulaires et fonctions zêta p-adiques. In *Modular functions of one variable III*, pages 191–268. Springer, 1973.

[Ser75] Jean-Pierre Serre. Valeurs propres des opérateurs de Hecke modulo l. *Astérisque*, 24:109–117, 1975.

[Ser87] Jean-Pierre Serre. Sur les représentations modulaires de degré 2 de $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$. *Duke Mathematical Journal*, 54(1):179–230, 1987.

[Tat94] John Tate. The non-existence of certain Galois extensions of $\mathbf{Q}$ unramified outside 2. *Contemporary Mathematics*, 174:153–153, 1994.

[Wie12] Gabor Wiese. Galois Representations. `http://math.uni.lu/~wiese/notes/GalRep.pdf`, February 2012.

[Wie13] Gabor Wiese. Modular Galois Representations and Applications. `http://math.uni.lu/~wiese/notes/2013-ModGalRepApp.pdf`, April 2013.