Serre's conjecture

Alex J. Best

April 10, 2015

Contents

1 Introduction **2**

2 Background **2**
2.1 Modular forms 2
2.2 Galois representations 3

3 Obtaining Galois representations from modular forms **6**

4 Serre's conjecture **8**
4.1 The qualitative form 8
4.2 The refined form 9
4.3 Results on Galois representations associated to modular forms 10
4.4 The optimal level 11
4.5 The character and the weight mod $p-1$ 12
4.6 The optimal weight 13
4.6.1 The level 2 case 14
4.6.2 The level 1 tame case 15
4.6.3 The level 1 non-tame case 15
4.7 A small issue 16
4.8 The proof 16

5 Examples **17**

6 Consequences **18**
6.1 Unramified mod p Galois representations for small p 18
6.2 The Taniyama–Shimura–Weil conjecture 18
6.3 The Artin conjecture 18
6.4 Modularity of abelian varieties 19

7 References **19**

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* to distinguish it from 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 standard 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 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.

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. Let $S_k(N, \varepsilon; \mathbf{Q})$ be the space of cusp forms of level k, weight N and character ε whose q-expansion coefficients lie in $\mathbf{Q}$.

Given a mod p character

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

we may lift to a character

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

We 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 $S_k(N, \hat{\varepsilon}; \mathbf{Q})$. We denote this space by

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

Definition 2.2. As usual we say a mod p cusp form

$$f = \sum_{n\geq 1} a_n q^n, \ (a_n \in \overline{\mathbf{F}}_p)$$

is *normalised* if $a_1 = 1$.

2.2 Galois representations

Definition 2.3. An *n-dimensional mod p Galois representation* is a homomorphism

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

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

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

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

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

Recall that $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ is defined as the inverse limit of $\mathrm{Gal}(K/\mathbf{Q})$ as K ranges over all number fields. So the group $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ naturally has the profinite topology, where the open subgroups are the subgroups of finite index. Our mod p representations are always continuous with respect to this topology and the discrete topology on $\mathrm{GL}_n(\overline{\mathbf{F}}_p)$, though we will often still say as such to remind ourselves.

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

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

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

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

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

to define a restriction map

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

In fact due to Krasner's lemma [Coh08, p. 238] the map $\mathrm{G}_\ell \to \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ is injective and so we may view G_ℓ as a subgroup of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$. The way this subgroup sits inside $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ 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 2.4. The first is the *inertia subgroup* I_ℓ which is defined as the kernel of the map

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

obtained by quotienting out $\overline{\mathbf{Q}}_\ell$ by its maximal ideal. The group $\mathrm{Gal}(\overline{\mathbf{F}}_\ell/\mathbf{F}_\ell)$ is topologically cyclic, generated by the Frobenius morphism $x \mapsto x^\ell$. We can then let $\mathrm{Frob}_\ell \in \mathrm{G}_\ell$ 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

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

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

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

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

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

Definition 2.5. 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.

Definition 2.6. Let $\phi\colon \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to K^*$ 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 $c \in \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$, 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

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

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

Definition 2.7. Each character

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

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.

Definition 2.8. The restriction map

$$\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathrm{Gal}(\mathbf{Q}(\zeta_p)/\mathbf{Q})$$

gives an action of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ on the primitive pth roots of unity, where each $\sigma \in \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ sends

$$\zeta_p \mapsto \zeta_p^{n_\sigma},$$

with $n_\sigma \in (\mathbf{Z}/p\mathbf{Z})^*$. So letting $\chi_p(\sigma) = n_\sigma$ gives a character

$$\chi_p\colon \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathbf{F}_p^* \hookrightarrow \overline{\mathbf{F}}_p^*,$$

called the mod p cyclotomic character. By definition this character is of level 1.

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

First, if $\ell \neq p$ then

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

as. Also fixing 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

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

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

Definition 2.9. Recall that $I_{p,t}$ can be identified with

$$\varprojlim \mathbf{F}_{p^n}^*$$

and so we have 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 canonical.

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.

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 some of 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 by Ramanujan and $\tau(n)$ became known as the Ramanujan τ function. The properties of this function provide the first glimpse of behaviours that extend to more general systems of Hecke eigenvalues.

Various people, including Ramanujan himself (in the mod 691 case) had found congruences involving the coefficients $\tau(n)$. Below are a few examples, though many more exist for higher powers of primes.

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

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

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

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

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

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

In order to explain these congruences Serre predicted [Ser67] the existence of p-adic Galois representations ρ_p for each prime p such that

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

The congruences would then follow from these Galois representations being of a specific from

These representations were constructed shortly after by Pierre Deligne [Del69], in doing so he proved the Ramanujan conjecture concerning $|\tau(p)|$ as p varies.

While we do not

Given the above example it is natural to 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:

Theorem 3.1. *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) $\operatorname{tr}(\rho_f(\mathrm{Frob}_\ell)) = a_\ell$ *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 is due to Shimura when $k = 2$ [**?**], and Deligne when $k > 2$ [Del69]. There is also a similar statement for $k = 1$ due to Deligne–Serre [DS74]. (There is an English translation of Deligne's paper available from the IAS [Del04], it has nicer typesetting too.)

In fact the representations obtained by these authors are p-adic Galois representations $\rho_f \colon \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathrm{GL}_2(\mathbf{Q}_p)$ and the representations in the theorem are then obtained from the p-adic one by a process of reduction and semisimplification. 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 Chebatorev we get

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

Hence as $\varepsilon(c)f = \langle -1\rangle f = (-1)^k f$ (by looking at the action of $-\mathrm{Id}$ on f) we calculate

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

and so $\det \rho_f$ must be odd.

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 is that the answer to this

question is yes, all Galois representations that could possibly arise from an eigenform based on the remarks following Theorem 3.1 do so.

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

Conjecture 4.1 (Serre's conjecture, qualitative 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 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 Galois representations (see Sections 6.2 and 6.3 for examples of this).

This conjecture (at least for Galois representations unramified outside p) appeared much earlier than the Duke paper and is mentioned by Serre in 1975 [Ser75, sec. 3].

4.2 The refined form

Given the above statement it is natural to 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 quantities $N(\rho)$, $k(\rho)$ 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 we are about to detail.

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 forms can give rise to a particular representation it is useful to take an arbitrary form and study the properties of the representation attached to it. This has been done by several people and the information which will be important to us is contained in the following theorems.

We fix a prime p and a normalised eigenform $f \in S_k(N, \varepsilon, \overline{\mathbf{F}}_p)$ to look at, let f have 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 we have 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 shortly), 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 interesting observations concerning the restriction of ρ_f to G_p, for this there are two theorems depending on whether $a_p \neq 0$ (the *ordinary case*) or otherwise.

Theorem 4.2 (Deligne)**.** *Suppose $2 \leq k \leq p+1$ and $a_p \neq 0$ then $\rho_{f,p}|_{\mathrm{G}_p}$ 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*

$$\rho_{f,p}|_{\mathrm{G}_p} = \begin{pmatrix} \chi_p^{k-1}\lambda(\varepsilon(p)/a_p) & * \\ 0 & \lambda(a_p) \end{pmatrix}$$

up to conjugation in $\mathrm{GL}_2(\overline{\mathbf{F}}_p)$.

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.

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

$$\rho_{f,p}|_{I_p} = \begin{pmatrix} \psi_1^{k-1} & 0 \\ 0 & \psi_2^{k-1} \end{pmatrix}$$

up to conjugation in $\mathrm{GL}_2(\overline{\mathbf{F}}_p)$.

It is worth noting that proofs of some of these theorems came after Serre's paper. However it seems likely that observations of the above 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 2.4, 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 in fact an integer []. 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, and by construction it is coprime to p.

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.

The definition above is that of the *Artin conductor* of a representation, but with the p part ignored.

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

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

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

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

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

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 ε we get by doing this is our character $\varepsilon(\rho)$.

The group $(\mathbf{Z}/p\mathbf{Z})^*$ is cyclic of order $p-1$ so any generator must map to an element of order dividing $p-1$ in $\overline{\mathbf{F}}_p^*$, hence its image must be in the prime field. Therefore this map is of the form

$$x \mapsto x^h,$$

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

So we have written

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

and so comparing with Remark 3.1 it looks like the class of h mod $p-1$ should be the same as that of $k(\rho)-1$. Now it remains to define the actual value of $k(\rho)$.

4.6 The optimal weight

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

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

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

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

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

Definition 4.1. The *semisimplification* of a 2-dimensional representation ρ is another representation ρ^{ss} obtained as follows. If ρ is irreducible (and hence semisimple) we leave it as it is and set $\rho^{\mathrm{ss}} = \rho$. Otherwise after picking a particular basis ρ is given by

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

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

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

Which is indeed semisimple, as hoped.

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

Now $\rho^{\mathrm{ss}}|_{I_{p,w}}$ is trivial and therefore ρ^{ss} may be viewed as a representation of $I_{p,t}$. This representation is diagonalisable and so it is given by a pair of characters

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

Proposition 4.1. *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. We have two possibilities, either taking the pth power fixes both ϕ_1 and ϕ_2 or it swaps them. If they are both fixed then they must be 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 $\rho|_{I_{p,w}}$ is trivial.

4.6.1 The level 2 case

When the characters are of level 2 we can write them in terms the fundamental characters ψ_1 and ψ_2 of level 2 (as defined in Definition 2.9) 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

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

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

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

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

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

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. We then set

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

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 $I_{p,w}$

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

we may 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 α, $\beta \in \mathbf{Z}/(p-1)\mathbf{Z}$. Using this decomposition we may write the restriction to I_p as

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

We fix representatives α and β now such that

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

Then we set

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

If $\beta \neq \alpha + 1$ we let

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

as we did in Section 4.6.1.

If we instead have $\beta = \alpha + 1$ we have to distinguish two cases, which, after Serre, we shall refer to as *peu ramifé* and *tres ramifé*. In order to define these cases we need to study the field K cut out by the kernel of ρ_p.

If we are in the peu ramifé case we define $k(\rho_p)$ as before via

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

the second equality holds as we have $\beta = \alpha + 1$.

Finally if we are in the tres ramifé case we add $p - 1$ to Eq. (10), unless $p = 2$, in which case we add 2 instead, obtaining

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

4.7 A small issue

It needs mentioning that the conjecture exactly as stated above is in fact *incorrect* and we have the following counterexample (due to Serre).

Example 4.1. Let .

This problem is fairly isolated and only arises from trying to specify the character in addition to the weight and level when we work with mod 2 or mod 3 Galois representations. The reason this happens is due to the failure of

4.8 The proof

As mentioned at the start, this conjecture is in fact now a theorem. We will not go into detail about the proof here and restrict ourselves to the following remarks:

It was known that the qualitative and refined forms were equivalent before either was known in general. The reduction of the refined form to the qualitative is due to a large number of people and . Once this reduction has been obtained it is only necessary to .

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 as detailed above, and 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 and check that everything we have just done is consistent with what we saw there.

So ρ_7 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 indeed it did.

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

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

$$f = x^3 + ??x + ??.$$

This has Galois group S_3 and we may consider the restriction map

$$\rho\colon \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathrm{Gal}(K/\mathbf{Q}) \simeq S_3.$$

We can turn this into a Galois representation using the fact that S_3 is isomorphic to $\mathrm{GL}_2(\mathbf{F}_2)$ 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 ρ can actually be viewed as a mod 2 Galois representation, what does Serre have to say about it? Well for starters $N(\rho)$

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 parts of many 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 Unramified mod p Galois representations for small p

First let us examine a very direct consequence. We take ρ to be be a mod p Galois representation for some $p < 11$ that is unramified outside of p. In this case, due to the absence of ramification, $N(\rho)$ is simply 1 (recall Remark 4.1). So Serre's conjecture predicts there is some mod p cusp form of level 1 and weight ?? from which ρ arises. But there are no cusp forms of level 1 of weight < 12 and so such a representation cannot exist.

We can make similarly simple conclusions using this type of argument in other low dimensional cases too, for example if we

6.2 The Taniyama–Shimura–Weil conjecture

6.3 The Artin conjecture

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

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

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

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

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 question concerning this function.

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

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

be an Artin representation, then the meromorphic continuation of

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

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

As the L-function of a ??

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

Proof. Given an odd Artin representation

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

□

6.4 Modularity of abelian varieties

The following result that can be deduced from Serre's conjecture does not obviously concern the objects related in the conjecture, nevertheless it does follow by the work of Ribet **[?]**.

7 References

[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] H. 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.

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

[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.

[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.

[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.

[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.

[Ser75] Jean-Pierre Serre. Valeurs propres des opérateurs de Hecke modulo l. *Astérisque*, 24(25):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.