Serre's Duke paper:

Plan

Serre's 1979 article surveys a conjecture about the relationship between mod p Galois reps and mod p cusp forms. We will begin by looking at his definitions of those two objects

① Introduction

We will then motivate and state the conjecture from the paper

② statement of conjecture

Before going into detail about his recipe for the level N and character ε

③ Recipe for level and character

And then for the weight k

④ Recipe for weight

Finally if there is time we will briefly explore an application of Serre's conjecture

⑤ Application.

§1 Introduction

§1.1 Modular (cusp) forms.

Fix throughout p a prime

$N \geq 1$ an integer prime to p

$k \geq 2$ an integer

ε a character $(\mathbb{Z}/N\mathbb{Z})^* \longrightarrow \bar{\mathbb{F}}_p^*$

suppose aswell that if $p = 2$ k is even otherwise $\varepsilon(-1) = (-1)^k$.

subgroup of $SL_2(\mathbb{Z})$ s.t. $\left(\begin{smallmatrix} & \\ * & \end{smallmatrix}\right)$ $* \equiv 0 \bmod N$

Def: A cusp form of type (k, ε_0) on $\Gamma_0(N)$ is a formal power series $F = \sum_{n \geq 1} A_n q^n$ $A_n \in \bar{\mathbb{Z}}$, $q = e^{2\pi i z}$ which converges in the half plane $\mathrm{Im}(z) > 0$ satisfying for $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N)$ $z \in \mathbb{C}$ $\mathrm{Im}(z) > 0$

$$F((az+b)/(cz+d)) = \varepsilon_0(d)(cz+d)^k F(z)$$

and vanishing at cusps.

Identifying $\bar{\mathbb{Q}}$ with a subfield of $\mathbb{C}$ and choosing a place over p defines a homomorphism $\bar{\mathbb{Z}} \to \bar{\mathbb{F}}_p$

$z \longmapsto \tilde{z}$

Def : A mod p cusp form of type (N, k, ε) is a formal power series $f = \sum a_n q^n$ with $a_n \in \overline{\mathbb{F}}_p$ such that lifting the coeffients a_n under the map above gives a cusp form $F = \sum_{n \geq 1} A_n q^n$ $A_n \in \overline{\mathbb{Z}}$ of type (k, ε_0) on $\Gamma_0(N)$ where $\widetilde{\varepsilon_0(x)} = \varepsilon(x)$ and $\tilde{A}_n = a_n$.

Rmk: The space of such f Serre denotes by $S(N, k, \varepsilon)$. It is stable under Hecke operators and normalised Hecke eigenforms correspond (again via $z \to \tilde{z}$) to Hecke eigenforms in $S(k, \varepsilon_0)$ on $\Gamma_0(N)$ (not uniquley)

§ 1.2 Galois representations.

Let $G_{\mathbb{Q}} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$

Def : A mod p Galois rep is a continuous homomorphism of dim n

$$\rho : G_{\mathbb{Q}} \longrightarrow GL_n(\overline{\mathbb{F}}_p)$$

$\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ has profinite topology. The continuity of $\rho \Rightarrow$ it has an open kernel and therefore $\mathrm{Im}\, \rho$ is finite and so it factors through finite extensions.

If $n=1$ we call $\phi : G \to \overline{\mathbb{F}}_p^{\times}$ a character.

Again considering $\bar{\mathbb{Q}}$ as a subfield of $\mathbb{C}$ take c to be the element of $G_{\mathbb{Q}}$ corresponding to complex conjugation

Define the parity of a character ϕ to be odd if $\phi(c)=-1$ and even if $\phi(c)=1$.

The parity of a rep ρ is the parity of the character $\det\rho$.

FACT : semisimple mod p reps of dimension 2 are determined by $\mathrm{tr}\,\rho(\mathrm{Frob}_\ell)$ and $\det\rho(\mathrm{Frob}_\ell)$ $\forall\, \ell$ outside a finite set of primes, for which ρ is unramified

$\rho|_I$ trivial

§1.2.1 Note on cyclotomic characters

consider the Dirichlet character $\varepsilon : (\mathbb{Z}/N\mathbb{Z})^* \to \mathbb{F}_p^*$.

We have an isomorphism $(\mathbb{Z}/N\mathbb{Z})^* \cong \mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q})$ for ζ_N a primitive N^{th} root of unity. Kronecker-Weber theorem tells us that there is a bijection between the set of characters ϕ or $G_{\mathbb{Q}}$ that factor through $\mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q})$ and characters ε.

Applying this to $N=p$ and $\varepsilon = id$ the corresponding character χ_p is called the mod p cyclotomic character. We have $\chi_p(\mathrm{Frob}_\ell)=\ell$ for $\ell \neq p$ prime and $\chi_p(c)=-1$.

---

§2 Statement of conjecture

§2.1 Motivation

Consider the following thm of Deligne

Thm (Deligne 1975): If $f=\sum a_n q^n$ is a normalized Hecke eigenform with coeff in $\overline{\mathbb{F}}_p$ the there exists a cont. semisimple rep

$$\rho_f : G_{\mathbb{Q}} \longrightarrow GL_2(\overline{\mathbb{F}}_p)$$

characterised by the following properties:

For and $\ell \nmid pN$ ρ_f is unramified at ℓ and $\mathrm{Tr}\,\rho_f(\mathrm{Frob}_\ell)=a_\ell$ and $\det_{\rho_f}(\mathrm{Frob}_\ell)=\varepsilon(\ell)\ell^{k-1}$

Rmk: The reps are actually semisimplified p-adic $G_{\mathbb{Q}}$ reps reduced mod p ($\rho_f=\bar{\rho}$ where $\rho: G_{\mathbb{Q}} \to GL_2(\overline{\mathbb{Q}}_p)$)

Rmk using the remarks in section §1.2.1

we can see that the property

$\det \rho_f (\mathrm{frob}_\ell) = \varepsilon(\ell)\, \ell^{k-1}$ is equivalent to

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

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

check by looking at action of $\langle -1 \rangle$ on f.

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

$= -1$

hence ρ_f is odd.

§2.2 Serre's conjectures

① 'weak' form

Let $\rho : G_{\mathbb{Q}} \to GL(V) \cong GL_2(\overline{\mathbb{F}}_p)$

be an irreducible odd mod p Galois rep

then there exists a Hecke eigenform f with coeff in $\overline{\mathbb{F}}_p$ such that $\rho_f \cong \rho$

② 'strong' form

Not only does such a mod p cusp form f exist but it can be chosen to be of type (N, k, ε) where Serre provides an explicit recipe to find N, k and ε_n from the rep ρ.

This has been shown to be false in some cases ie ρ from $\mathbb{Q}(i)$ $p=2$

ρ from $\mathbb{Q}(\sqrt{-3})$ $p=3$

In fact k relates only to the 'local to p' properties of p

---

§3 Recipe for level N and character ε.

§3.1 The level N

Serre conjects the level N to be the Artin conductor minus the p part.

Let ℓ be a prime of $\mathbb{Q}$. For a finite Galois extension $K/\mathbb{Q}$ with Galois gp G and any prime λ of k over ℓ the decomposition gp of G at ℓ is $D_\ell = \{ g \in G : g\lambda = \lambda \}$ and for a nonnegative integer i the ith ramification gp $G_{\ell,i} = \{ g \in D_\ell : g(x) - x \in \lambda^{i+1} \ \forall x \in \mathcal{O}_K \}$ giving rise to a sequence of decreasing subgroups of D_ℓ.

The D_ℓ are subgroups of $G_\mathbb{Q}$ s.t. if λ' is a another prime of k over ℓ then the corresponding decomp groups will be conjugate in $G_\mathbb{Q}$. We can also define the decomposition group of ~~as~~ $G_\ell = \mathrm{Gal}(\overline{\mathbb{Q}}_\ell / \mathbb{Q}_\ell)$ identified with a subgroup of $G_\mathbb{Q}$ via a choice of embedding $\overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_\ell$. Varying the choice of embedding corresponds to conjugation.

Therefore choosing an embedding $\overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_\ell$ we can define a decreasing sequence of ramification subgroups of $G_\mathbb{Q}$ at ℓ

$D_\ell \supseteq G_0 \supseteq G_1 \supseteq \cdots$ where G_0 is the inertia subgroup i.e corresponds to kernel of $G_\ell \to \mathrm{Gal}(\overline{\mathbb{F}}_\ell / \mathbb{F}_\ell)$ The $G_{\ell,0}$ above will be the image of G_0 in G where λ corresponds to the embedding $k \hookrightarrow \overline{\mathbb{Q}}_\ell$ via the choice of embedding $\bar{\mathbb{Q}} \hookrightarrow \bar{\mathbb{Q}}_\ell$ + map $k \to \bar{\mathbb{Q}}$ must defined $G_{\mathbb{Q}} \to G$

We can now define $n(\ell, p) = \sum_{i \geq 0} \frac{1}{[G_0 : G_i]} \dim (V/V^i)$

$$= \dim (V/V^0) + b(V)$$

which is nontrivially an integer

'wild invariant' of G_0 module V

Serre conjects that the level $\boxed{N = \prod_{\substack{\ell \neq p \\ \text{prime}}} \ell^{n(\ell, p)}}$

Rmk : $n(\ell, p) = 0 \iff G_0 = \{1\}$ i.e ρ is unramified at ℓ

Context

$\widetilde{\text{Rmk}}$: Evidence to support / motivate such a prediction

Carayol and Livné showed if $\rho \cong \rho_f$ then this value at least divided the level of f.

~

§ 3.2 character ε and class of k mod$(p-1)$

Note $\det\rho : G_{\mathbb{Q}} \to \overline{\mathbb{F}}_p^*$ defines a character for which one can check the conductor divides pN.

Recall the bijection discussed in §1.2.1 that allows us to identify $\det\rho$ with a Dirichlet character $\phi \; (\mathbb{Z}/pN\mathbb{Z})^* \to \overline{\mathbb{F}}_p^*$

or equivalently the pair of characters

$$\varphi : (\mathbb{Z}/p\mathbb{Z})^* \to \overline{\mathbb{F}}_p^*$$

$$\boxed{\varepsilon : (\mathbb{Z}/N\mathbb{Z})^* \to \overline{\mathbb{F}}_p^*}$$

where ε is suggestively named as it refers to Serres prediction for the character of the mod p modular form we are looking for.

Furthermore $\varphi = \chi_p^h$ $h \in \mathbb{Z}/(p-1)\mathbb{Z}$ therefore for $\ell \nmid pN$ we have $\det(\text{frob}_{\ell,\rho}) = \ell^h \varepsilon(\ell)$ comparing this to the description of ρ_f in §2.1 that serre conjects is isomorphic to ρ we see that we want $k-1 \equiv h \bmod p$.

§4 Recipe for the weight k.

§4.1 "local at p" Galois reps.

Serre conjectures that the weight k depends on the "local at p" representation, that is the rep

$$\rho_p : G_p \longrightarrow GL(V) \cong GL_2(\overline{\mathbb{F}}_p)$$

where $G_p = Gal(\overline{\mathbb{Q}}_p / \mathbb{Q}_p)$.

In fact he describes a recipe for finding a weight k that depends only on the restriction of ρ_p to the inertia subgroup I of G_p

I is the kernel of $G_p \to Gal(\overline{\mathbb{F}}_p / \mathbb{F}_p)$ where $\overline{\mathbb{F}}_p$ is identified with the residue field of $\overline{\mathbb{Q}}_p$.

Let I_p be the largest pro-p-subgroup of I (the wild inertia) and set $I_t = I/I_p$ the tame inertia group.

We can identify I_t with $\varprojlim_{t} \mathbb{F}_{p^r}^*$

(kummer theory ℓ prime to p

$\varprojlim Gal(\overline{\mathbb{Q}}_p^I(\sqrt[\ell]{p}) / \overline{\mathbb{Q}}_p^I)$

$= \varprojlim \mathbb{F}_{p^n}^*$)

giving rise to the following definitions

Def: A character of I_t has level n if it factors through $\mathbb{F}_{p^n}^*$ but not $\mathbb{F}_{p^m}^*$ m strict divisor of n

Def: The set of n fundamental characters of level n are the $\overline{\mathbb{F}}_p$ characters

$\psi_n : I_t \to \mathbb{F}_{p^n}^* \hookrightarrow \overline{\mathbb{F}}_p^*$ corresponding to the n empbeddings $\mathbb{F}_{p^n}^* \hookrightarrow \overline{\mathbb{F}}_p^*$.

Fact: (Serre) These fundamental characters generate all level n characters.

Going back to our rep ρ, let V^{ss} be the semisimplication of V wrt the action of G_p

$\begin{pmatrix} a & * \\ 0 & b \end{pmatrix} \to \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$

Fact (Serre) I_p acts trivially on V^{ss}

Idea of proof: enough to show I_p trivially on simple V → Let $W \subset V$ be subspace fixed by I_p

① nontrivial $\rho(I_p)$ p-group over $\mathbb{F}_q$ -orbits of p power order; 0 is orbit so must p-1 other

② $I_p \triangleleft G_p$ so W stable under G_p so $W = V$ by simplicity.

Therefore defines an action of I_t on V^{ss} which is diagonalizable and can be written in terms of two characters $\varphi, \varphi' : I_t \to \mathbb{F}_p^*$ $\quad \rho^{ss}|_{I_t} = \begin{pmatrix} \varphi & 0 \\ 0 & \varphi' \end{pmatrix}$

Prop 1 from serre paper: φ and φ' have level 1 or 2 and if they have level 2 they are p^{th} powers of each other.

Idea of proof: $G_p \longrightarrow G_p/I = \mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$
$s \longmapsto \mathrm{Frob}_p$

$u \in I$ $sus^{-1} \in u^p I_p$ i.e $s \curvearrowright I_t$ by conjugation sending $u \mapsto u^p$ $\Rightarrow$ $\{\varphi, \varphi'\}$ stable under p^{th} power

i.e either $\varphi^p = \varphi$ $\varphi'^p = \varphi'$ level 1
or $\varphi^p = \varphi'$ $\varphi'^p = \varphi$ level 2

§4.2 Level 2 case

context

Thm (Fontaine 1979) $f = \sum a_n q^n$ mod p cusp form of type (N, k, ε) with $2 \le k \le p+1$ $a_p = 0$ then $\rho_f|_{G_p}$ irreducible and for ψ and ψ' the two fundamental characters of level 2

$$\rho_f|_I \sim \begin{pmatrix} \psi^{k-1} & 0 \\ 0 & \psi'^{k-1} \end{pmatrix}.$$

Let φ, φ' be as in the previous section be of level 2. Then V is irreducible since otherwise it would contain a one dim subspace which would correspond to a level 1 character of I_t.

Let ψ and ψ' be the two fundamental characters of I_t. As discussed they generate all level 2 characters so we can write

$$\varphi = \psi^a \psi'^b = \psi^{a+pb} \quad \text{some } 0 \le a, b \le p-1$$

($a \ne b$ since otherwise φ is a power of a cyclotomic character restricted to I_t and therefore of level 1)

$\varphi' = \psi^b \psi'^a$ so up to interchanging φ, φ'

we may assume $0 \le a \le b \le p-1$ and set $\boxed{k = 1+pa+b.}$

§4.3 level 1 tame case.

Suppose φ and φ' have level 1 and the action of I_p on V is trivial.

Then we have the action of I on V is semisimple and the characters φ and φ' are powers of the cyclotomic character

we can write $\rho_p|_I = \begin{pmatrix} \chi^a & 0 \\ 0 & \chi^b \end{pmatrix}$ a, b determined mod (p-1)

so up to swapping a, b and normalizing we may assume $0 \le a \le b \le p-2$

and set $k = \begin{cases} 1+pa+b & \text{if } (a,b) \neq (0,0) \\ p & \text{o/w} \end{cases}$ (unramified case $I \circlearrowright V$ trivial)

§4.4 level 1 non tame case

I_p does not act trivially on V and hence the action of I is not tame. Let D be the line of elements of V fixed by I_p that is stable under G_p

Let the charater θ_1 correspond to the action of G_p on V/D and θ_2 the action on V s.t. $\rho_p = \begin{pmatrix} \theta_2 & * \\ 0 & \theta_1 \end{pmatrix}$

we have $\theta_1 = \chi^{\alpha} \varepsilon_1$ $\quad \theta_2 = \chi^{\beta} \varepsilon_2$ $\quad \varepsilon_1, \varepsilon_2$ unramified characters of G_p. Then restricting to I we get

$\rho_p|_I = \begin{pmatrix} \chi^{\beta} & * \\ 0 & \chi^{\alpha} \end{pmatrix}$ normalizing α, β

we have $0 \le \alpha \le p-2$, $1 \le \beta \le p-1$ and setting $a = \min\{\alpha, \beta\}$ $b = \max\{\alpha, \beta\}$

Serre defines k corresponding to 3 different cases

① $\beta \neq \alpha + 1$

② $\beta = \alpha + 1$ $\quad \rho_p$ peu ramified $\Big\}$ $\boxed{k = 1 + pa + b}$

③ $\beta = \alpha + 1$ $\quad \rho_p$ très ramified

$$\boxed{k = \begin{cases} 1 + pa + b + p - 1 & p \neq 2 \\ 4 & p = 2. \end{cases}}$$

§5 Applications

Serre's conjecture could be used to prove FLT although its actual proof used only the special case required for the proof, not the full conjecture.

FLT: Assume Serre's conjecture then $\circledast$ $a^p + b^p + c^p = 0$ has no solutions $a, b, c \in \mathbb{Z}$ with $abc \neq 0$.

Idea of proof: suppose (a, b, c) was a solution let E be the elliptic curve corresponding to $\circledast$ at (a, b, c) the rep ρ_p^E of $G_{\mathbb{Q}}$ given by the p-torsion points of E is irreducible and Serre's conjecture would say $\rho_p^E \cong \rho_f$ where f is a cusp form of weight 2 and level 2 with coeff. in $\overline{\mathbb{F}}_p$ but such a cusp form does not exist.