Serre's modularity conjecture II

Chandrashekhar Khare

Theorem

These are slides for the talk which was a sequel to the earlier talk (this one was given only at Harvard).

Let us recall the theorem whose proof we want to talk about.

Main Theorem: (joint work with Wintenberger)

(i) For $p > 2$ Serre's conjecture is true for odd conductors, i.e., for $\overline{\rho}$ unramified at 2.

(ii) For $p > 2$ Serre's conjecture is true when $k(\overline{\rho}) = 2$.

Last time I sktched the ideas of the proof of the theorem in the level 1 case.

Killing ramification

We start by presenting a corollary of the level 1 case which introduces a key trick in the proof of the above theorem, that of “killing ramification”.

Corollary:

If $\overline{\rho} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}_p})$ is of S-type with $k(\overline{\rho}) = 2$, $N(\overline{\rho}) = q$, with q prime, and $p, q > 2$, then it arises from $S_2(\Gamma_1(q))$.

Proof of corollary

We consider a minimal lift of $\overline{\rho}$ to a ρ unramified outside p, q, Barostti-Tate at p and minimally ramified at q. Then ρ is part of a compatible system (ρ_λ). Consider ρ_q and $\overline{\rho}_q$: the latter is a level 1 representation, and modularity lifting theorems apply to prove that ρ_q is modular, hence ρ_p, hence $\overline{\rho}$.

General strategy

The proof of our theorem is a combination of the weight reduction technique that occured in the proof of the level one case, and the idea above about "killing ramification".

One of the technical difficulties is that modularity lifting theorems are trickier when $\overline{\rho}|_{\mathbb{Q}(\mu_p)}$ is reducible, and at present the only theorems available in this case are those of Skinner-Wiles. These apply when the lift is ordinary. Thus we have to ensure either that the modularity lifting theorems we need to invoke are in non-degenerate cases, or when the lifts considered are ordinary. Having done the level one case, it is possible to ensure the former.

The idea to do this is to rigidify the residual representations that arise by introducing ramification of "dihedral" type at a prime. Given a

$\overline{\rho}$, the residual representations that arise in the proof of the modularity of $\overline{\rho}$, using the techniques of:

(i) “weight reduction” and

(ii) “killing ramification”

are in characteristic at most that of $\overline{\rho}$ and the primes at which $\overline{\rho}$ ramifies. This motivates the following definition.

Locally good dihedral representations

Define the function $Q : \mathbb{N} \to \mathbb{N}$ such that $Q(1) = 1$, and for $n \geq 2$, $Q(n)$ is the largest prime that divides n.

Definition: Let $\overline{\rho} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}_p})$ be a continuous representation.

We say that $q \neq p$ is a good dihedral prime for $\overline{\rho}$ if

(i) $\overline{\rho}|_{I_q}$ is of the form

$$\begin{pmatrix} \psi & 0 \\ 0 & \psi^q \end{pmatrix},$$

where ψ is a non-trivial character of I_q of order a power of an odd prime $t \neq q$, such that t divides $q+1$, and $t > \max(Q(\frac{N(\overline{\rho})}{q^2}), 5, p)$;

(ii) q is 1 mod 8, and 1 mod r for every prime $r \neq q$ such that $r \leq \max(Q(\frac{N(\overline{\rho})}{q^2}), p)$.

If there exists a good dihedral prime q for $\overline{\rho}$ we say that $\overline{\rho}$ is locally good-dihedral (for the prime q), or q-dihedral.

Lemma: Let $\overline{\rho}$ be a locally good-dihedral representation (for a prime q).

(i) The image of $\overline{\rho}$ is not solvable.

(ii) Let (ρ_λ) be any strictly compatible system lifting of $\overline{\rho}$. Then for any prime $r \leq$ max$(Q(\frac{N(\overline{\rho})}{q^2}), p)$, any mod r representation $\overline{\rho}_r$ that arises from (ρ_λ) is locally good-dihedral (for the prime q) and hence has non-solvable image (which is projectively not isomorphic to A_5).

Proof of lemma

Proof. It is enough to prove (i) as strict compatibility of (ρ_λ) ensures that all the $\overline{\rho}_r$ of (ii) are q-dihedral. By definition $\overline{\rho}|_{I_q}$ is of the form

$$\begin{pmatrix} \psi & 0 \\ 0 & \psi^q \end{pmatrix},$$

where ψ is a character of I_q of order a power of a prime $t|q+1$, and t is bigger than $\max(r,p,5)$ where $r \neq q$ ranges over primes that divide $N(\overline{\rho})$. As t does not divide $q-1$, $\overline{\rho}|_{D_q}$ is irreducible, and hence so is $\overline{\rho}$. As $t > 5$, we see that the projective image cannot be A_5.

We see that if the image of $\overline{\rho}$ is solvable, as $t > 5$, then by Dickson's theorem the projective image of $\overline{\rho}$ is dihedral. Note that the primes s different from q at which $\overline{\rho}$ is ramified are such that q is 1 mod s (and 1 mod 8 if $s = 2$). Suppose $\overline{\rho}$ is induced from G_K with K a quadratic extension of $\mathbb{Q}$. Then K is unramified outside the primes that are ramified in $\overline{\rho}$. Thus the prime q either splits in K or is ramified in K: both possibilities lead to a contradiction. If q splits in K, this contradicts the fact that $\overline{\rho}|_{D_q}$ is irreducible. If K is ramified at q we again get a contradiction as $t > 1$ is odd. $\square$

Shape of the proof

Consider the following hypotheses (for integers $r \geq 1$):

(L_r) All $\overline{\rho}$ of S-type which satisfy the following three conditions are modular: (a) $\overline{\rho}$ is locally good-dihedral; (b) $k(\overline{\rho}) = 2$ if $p = 2$; (c) $N(\overline{\rho})$ is odd and divisible by at most r primes.

(W_r) All $\overline{\rho}$ of S-type which satisfy the following three conditions are modular: (a) $\overline{\rho}$ is locally good-dihedral; (b) $k(\overline{\rho}) = 2$; (c) $N(\overline{\rho})$ is odd and divisible by at most r primes.

The proof of our main theorem proceeds by exhibiting relations between the (L_r)'s and (W_r)'s (besides the obvious one that (L_r) implies (W_r)!). Diagramatically the relations may be summarised as:

$$\begin{tikzcd}
W_1 \arrow[r, Rightarrow] & L_1 \arrow[dl, Rightarrow] \\
W_2 \arrow[r, Rightarrow] & L_2 \\
\cdots & \\
W_r \arrow[r, Rightarrow] & L_r \arrow[dl, Rightarrow] \\
W_{r+1} \arrow[r, Rightarrow] & L_{r+1} \\
\cdots &
\end{tikzcd}$$

Auxiliary theorems

The following theorem is the idea of “killing ramification”:

Theorem 1: (killing ramification in weight 2) For a positive integer r, (L_r) implies (W_{r+1}).

The following theorem is the idea of “weight reduction” used in the level 1 case:

Theorem 2: (reduction to weight 2) For a positive integer r, (W_r) implies (L_r).

The following theorem provides a starting point from which to apply Theorems 1 and 2.

Theorem 3: (a starting point) The hypothesis (W_r) is true if $r = 1$.

The following theorem uses an analog, for Galois representations, of a result for modular forms due to Carayol.

Theorem 4: (raising levels)

Assume the following hypothesis:

(D) All $\overline{\rho}$ of S-type which satisfy the following three conditions are modular: (a) $\overline{\rho}$ is locally good-dihedral; (b) the residue characteristic of $\overline{\rho}$ is an odd prime; (c) $N(\overline{\rho})$ is an odd integer.

Then any $\overline{\rho}$ of S-type of residue characteristic p and of odd conductor, and with $k(\overline{\rho}) = 2$ if $p = 2$, is modular.

Auxiliary theorems $\longrightarrow$ Main Theorem

We will explain how hypothesis (D) follows from Theorems 1, 2 and 3. Then by Theorem 4 we get our Main Theorem.

Notice that hypothesis (D) will be satisfied if we prove (L_r) for each $r \geq 1$. We do this by induction on r.

(L_1): Theorem 3 (starting point) fulfills the hypothesis (W_1) of Theorem 2 (weight reduction). Thus Theorem 2 gives that (L_1) is true.

Induction step: Assume we have proved (L_r) for $r \geq 1$, and we want to prove (L_{r+1}). The hypothesis (L_r) implies the hypothesis (W_{r+1}) by Theorem 1 (killing ramification). This by Theorem 2 yields (L_{r+1}).

Modularity lifting result

Consider $\overline{\rho} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F})$ with $\mathbb{F}$ a finite field of characteristic p and $2 \leq k(\overline{\rho}) \leq p+1$ when $p > 2$, and $k(\overline{\rho}) = 2$ if $p = 2$. We assume that $\overline{\rho}$ has non-solvable image.

A continuous representation $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathcal{O})$, for $\mathcal{O}$ the ring of integers of a finite extension of $\mathbb{Q}_p$, is said to be a lift of $\overline{\rho}$ if the reduction of ρ modulo the maximal ideal of $\mathcal{O}$ is isomorphic to $\overline{\rho}$. We say that ρ is *odd* if $\det(\rho(c)) = -1$ for c a complex conjugation. If ρ is Hodge-Tate of weights $(k-1, 0)$ at p (for $k \in \mathbb{N}, k \geq 2$), we say that ρ is of weight k.

Theorem: (ML)

Consider $\overline{\rho} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F})$ with $\mathbb{F}$ a finite field of characteristic p and $2 \leq k(\overline{\rho}) \leq p+1$ when

$p > 2$, and $k(\overline{\rho}) = 2$ if $p = 2$. We assume that $\overline{\rho}$ has non-solvable image.

1. ($p = 2$) Let ρ be an odd, irreducible lift of $\overline{\rho}$ to a 2-adic representation that is unramified outside a finite set of primes and is Barsotti-Tate at 2.

Then ρ is modular.

2. ($p > 2$) Let ρ be an irreducible lift of $\overline{\rho}$ to a p-adic representation that is unramified outside a finite set of primes and is either (i) crystalline of weight k at p with $2 \leq k \leq p+1$, or (ii) potentially semistable at p of weight 2 (i.e., either up to twist semistable of weight 2, or potentially Barsotti-Tate (BT) at p).

Then ρ is modular.

We remark that some results towards (1) are proved by Dickinson. Part (2)(i) for weights $\leq p-1$ is proven in Diamond, Flach and Guo, the weight $p+1$ case is proved by Kisin. Part (2) (ii) is proved by Kisin and is the hardest of all. The remaining parts we do.

Chebyshev estimates on primes

In the proof of Theorem 2 ("weight reduction") we need that for each prime $p \geq 5$, there is a prime $P > p$ (for instance the next prime after p) and either

(i) an odd prime power divisor $\ell^r || (P-1)$ so that

$$\frac{P}{p} \leq \frac{2m+1}{m+1} - (\frac{m}{m+1})(\frac{1}{p}) \qquad (1)$$

where we have set $\ell^r = 2m+1$ with $m \geq 1$, or

(ii) $2^r || (P-1)$ (with $r \geq 4$) so that

$$\frac{P}{p} \leq \frac{2^r}{2^{r-1}+2} - (\frac{2^{r-1}-2}{2^{r-1}+2})(\frac{1}{p}). \qquad (2)$$

Proof of Theorem 1 (killing ramification in weight 2)

Assume (L_r).

Consider $\overline{\rho}$ of S-type which is good-dihedral for a prime q, with $k(\overline{\rho}) = 2$, and such that $N(\overline{\rho})$ is odd and at most divisible by $r+1$ primes. Choose a prime $s \neq q$ that divides $N(\overline{\rho})$.

Choose a minimal lifting ρ, fit it in a compatible lift (ρ_λ) and consider ρ_s. Then $\overline{\rho}_s$ is a S-type representation, is q-dihedral and hence has non-solvable image the lemma, and $N(\overline{\rho}_s)$ is divisible by at most r primes: the prime divisors of $N(\overline{\rho}_s)$ are a subset of the set of the prime divisors of the prime-to-s part of $N(\overline{\rho})$. Thus by (L_r) we know $\overline{\rho}_s$ is modular, and then by Theorem ML we are done.

Proof of Theorem 2 (weight reduction)

Assume (W_r). Then we have to prove that any $\overline{\rho}$ of S-type which is good-dihedral (for a prime q), such that p is odd, $N(\overline{\rho})$ is odd, and divisible by at most r primes, is modular.

This is very similar to the proof of the level 1 case and again we do this by induction on the prime p.

The case of $p = 2$ is part of the assumption (W_r) (as for $p = 2$ we only consider weight 2 representations). We only explain the passage from $p = 2$ to $p = 3$ as there is a slight twist here.

Mod 3: Consider $\overline{\rho}$ of S-type which is good-dihedral (for a prime q), $k(\overline{\rho}) \leq 4$ in residue characteristic 3, $N(\overline{\rho})$ is odd, and at most divisible by r primes. Choose a weight 2 lifting and fit it in a compatible system (ρ_λ) and consider ρ_2. The residual representation $\overline{\rho}_2$ is q-dihedral and hence has non-solvable image, $k(\overline{\rho}_2) = 2$ and $N(\overline{\rho}_2)$ is divisible by at most at $r+1$ primes. If $\overline{\rho}_2$ is unramified at 3, $N(\overline{\rho}_2)$ is divisible by at most r primes, and then $\overline{\rho}_2$ is modular by (W_r). Theorem ML yields that (ρ_λ) is modular and hence $\overline{\rho}$ is modular in this case.

Otherwise, note that $\overline{\rho}_2|_{I_3}$ is unipotent, and thus $\overline{\rho}_2|_{D_3}$ (up to unramified twist) is of the form

$$\begin{pmatrix} \overline{\chi}_2 & * \\ 0 & 1 \end{pmatrix}.$$

We lift $\overline{\rho}_2$ to ρ'_2 whih is minimally ramified outside 3 but at I_3 is of the form

$$\begin{pmatrix} \omega_{3,2}^2 & * \\ 0 & \omega_{3,2}^6 \end{pmatrix}.$$

Here $\omega_{3,2}$ is a character of I_3 which factors through its $\mathbb{F}_9^*$-quotient ($\omega_{3,2}^2$ and $\omega_{3,2}^6$ are all the characters of order 4 of $\mathbb{F}_9^*$) . Fit ρ'_2 in an odd compatible system (ρ'_λ). Consider ρ'_3 and the residual representation $\overline{\rho}'_3$ which is q-dihedral and hence has non-solvable image. By a result of Savitt a twist of $\overline{\rho}'_3$ has weight 2, and $N(\overline{\rho}'_3)$ is odd and divisible by at most r primes. Thus $\overline{\rho}'_3$ is modular by (W_r), and we are done by applying Theorem ML.

Proof of Theorem 3 (a starting point)

This follows from the corollary we started out with as we explain below.

Let us prove:

1. If $\overline{\rho}$ is an irreducible, odd, 2-dimensional, mod p representation of $G_{\mathbb{Q}}$ with $k(\overline{\rho}) = 2$, $N(\overline{\rho}) = q$, with q an odd prime, then it arises from $S_2(\Gamma_1(q))$.

2. If $\overline{\rho}$ is an irreducible, odd, 2-dimensional, mod p representation of $G_{\mathbb{Q}}$ with $k(\overline{\rho}) = 2$, unramified outside p and another odd prime q, tamely ramified at q, such that the order of $\overline{\rho}(I_q)$ is the power of an odd prime $t > 5$, then $\overline{\rho}$ arises from $S_2(\Gamma_1(q^2))$.

Proof. The first statement is exactly the corollary we started with (at least for $p > 2$).

We reduce the second statement to the first. We may assume that $t \neq p$, as otherwise this is covered by the first statement. Also as $\overline{\rho}$ is tamely ramified at q, we deduce that $t \neq q$. (We may also assume that $\mathrm{im}(\overline{\rho})$ is not solvable as otherwise we are done.)

Construct a minimal compatible system lift (ρ_λ) of $\overline{\rho}$. Thus ρ_p unramified outside $\{p, q\}$, is Barsotti-Tate at p, $|\rho_p(I_q)| = |\overline{\rho}_p(I_q)|$.

If the reduction $\overline{\rho}_t$ of an integral model of ρ_t is reducible, or unramified at q (which implies reducibility by the proof of the level 1 weight 2 case of Serre's conjecture), then we are done by applying the modularity lifting theorems of Skinner-Wiles, which allow us to conclude that

ρ_t is modular, hence (ρ_λ) is modular and hence so is $\overline{\rho}$.

If $\overline{\rho}_t$ is irreducible and ramified at q, then part (i) implies that the representation is modular (as in fact the ramification will be unipotent at q), and then by modularity lifting results of Wiles and Taylor, we again conclude that ρ_t is modular, hence (ρ_λ) is modular and hence so is $\overline{\rho}$. (The lifting theorems apply as one easily checks that $\overline{\rho}_t|_{\mathbb{Q}(\mu_t)}$ is irreducible.)

□

Proof of Theorem 4 (level raising)

Consider $\overline{\rho} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F})$ of S-type, $\mathbb{F}$ a finite field of characteristic p, with $k(\overline{\rho}) = 2$ if $p = 2$, and of odd conductor.

Let S be the primes other than p at which $\overline{\rho}$ is ramified. We may assume that $\overline{\rho}$ has non-solvable image.

Construct a minimal compatible system (ρ_λ) that lifts $\overline{\rho}$. If there is a $p' \notin S \cup \{p\}$ and $p' > 5$ at which the mod p' representation $\overline{\rho}_{p'}$ has solvable image we are done using the modularity lifting theorems in Skinner-Wiles and Taylor-Wiles. Note that for $p' \notin S \cup \{p\}$, $p' > 5$, $\overline{\rho}_{p'}$ cannot be irreducible and induced from the quadratic subfield of $\mathbb{Q}(\mu_{p'})$ (as $k(\overline{\rho}_{p'}) = 2$ and $p' > 5$).

Thus we may choose $p' > 5$ that is congruent to 1 modulo 4, with p' larger than all the primes in $S \cup \{p\}$, and such that $\overline{\rho}_{p'} : G_{\mathbb{Q}} \rightarrow GL_2(\mathbb{F}')$ has non-solvable image with $\mathbb{F}'$ a finite field of characteristic p'.

We have the following general easy lemma:

Lemma:

Let p be a prime that is congruent to 1 modulo 4, and $\overline{\rho} : G_{\mathbb{Q}} \to GL_2(\mathbb{F})$ a representation of S-type, with $\mathbb{F}$ a finite field of characteristic p. Assume that im($\overline{\rho}$) is not solvable. Denote by $\overline{\rho}_{\text{proj}}$ the projectivisation of $\overline{\rho}$, and $c \in G_{\mathbb{Q}}$ a complex conjugation. There is a set of primes $\{q\}$ of positive density that are unramified in $\overline{\rho}$ such that:

(i) $\overline{\rho}_{\text{proj}}(\text{Frob}_q)$ is the conjugacy class of $\overline{\rho}_{\text{proj}}(c)$,

(i) q is congruent to 1 modulo all primes $\leq p-1$ and is 1 modulo 8,

(iii) q is -1 mod p.

Proof. By Dickson's theorem, and as $\overline{\rho}$ has non-solvable image, the image of $\overline{\rho}_{\mathsf{proj}}$ is conjugate to either $\mathsf{PSL}_2(\mathbb{F}'')$ or $\mathsf{PGL}_2(\mathbb{F}'')$ for some subfield $\mathbb{F}''$ of $\mathbb{F}$, with $|\mathbb{F}''| \geq 4$, or is isomorphic to A_5. When the image is conjugate to $\mathsf{PGL}_2(\mathbb{F}'')$, note that as p is congruent to 1 mod 4, $\overline{\rho}_{\mathsf{proj}}(c)$ is inside $\mathsf{PSL}_2(\mathbb{F}'')$. As $\mathsf{PSL}_2(\mathbb{F}'')$ (for $|\mathbb{F}''| \geq 4$) and A_5 are simple (and non-cyclic), and as p is congruent to 1 modulo 4, we may appeal to the Cebotarev density theorem as follows. We choose q satisfying the following compatible conditions : $q \equiv 1 \mathrm{mod}(8)$, $\overline{\chi_\ell}(\mathsf{Frob}_q) = 1$ for ℓ odd $< p$, $\overline{\chi_p}(\mathsf{Frob}_q) = -1$, and $\overline{\rho}_{\mathsf{proj}}(\mathsf{Frob}_q)$ conjugate to $\overline{\rho}_{\mathsf{proj}}(c)$.

□

Proof of Theorem 4 (level raising) contd.

Apply the lemma to our $\overline{\rho}_{p'}$, and choose a prime q as in the lemma. Next one uses lifting techniques (LT) to lift $\overline{\rho}_{p'}$ to a compatible system (ρ'_λ) such that $\rho_{p'}|_{I_q}$ is of the shape

$$\begin{pmatrix} \chi' & * \\ 0 & \chi'^q \end{pmatrix}$$

for some χ' a p'-adic character of I_q of level 2 (i.e., factors through the $\mathbb{F}^*_{q^2}$ but not $\mathbb{F}^*_q$-quotient) and order a power of p'. Let s be the largest prime $< p'$: consider ρ'_s, and the corresponding residual representation $\overline{\rho}'_s$. Note that $s > 2$, $\overline{\rho}'_s$ is locally good-dihedral (for the prime q), and $N(\overline{\rho}'_s)$ is odd. Thus, by hypothesis (D), $\overline{\rho}'_s$ is modular and has non-solvable image. Hence by Theorem ML the compatible system (ρ'_λ) is modular. Observe that the compatible systems (ρ_λ) and (ρ'_λ) are linked at $\overline{\rho}_{p'}$. Applying Theorem ML again we conclude that that (ρ_λ) is modular, and hence $\overline{\rho}$ is modular.