Workshop on Serre's Modularity Conjecture: the level one case

Kenneth A. Ribet

UC Berkeley

Monte Verità
13 May 2009

Notation

We consider Serre-type representations of $G = \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$. They will always be 2-dimensional, continuous and *odd* (in the sense that $\det(\rho(\text{complex conjugation})) = -1$). They will usually be irreducible.

In this talk, the representations are ρ when they take values in $\mathbf{GL}(2)$ of a finite field (or the algebraic closure of a finite field) and $\tilde{\rho}$ when they are p-adic (or ℓ-adic or P-adic...) representations. In proving the conjecture, the mod p representations are the primary objects.

For each prime ℓ, we fix one $\iota : \overline{\mathbf{Q}} \hookrightarrow \overline{\mathbf{Q}}_\ell$. This allows us to refer to λ-adic representations as "ℓ-adic representations."

Modularity

A mod p representation is deemed *modular* if it is either *reducible* or associated with a cusp form $\sum a_n q^n$ (in the sense that tr $\rho(\text{Frob}_\ell) = a_\ell$ for almost all primes ℓ).

A p-adic representation $\tilde{\rho}$ is *modular* if it associated with a modular form. Our p-adic representations will always be irreducible.

The aim is to prove the modularity of mod p 2-dimensional irreducible representations of G that are unramified away from p. Serre's conjecture predicts that a given ρ arises from a cusp form on $\mathbf{SL}(2, \mathbf{Z})$ of a certain weight $k(\rho) \geq 2$.

This invariant is an even integer that is computed from the restriction of ρ to the inertia group of G at p. For $p > 2$, we have $2 \leq k(\rho) \leq p^2 - 1$, but we can and always do twist ρ by a suitable power of the mod p cyclotomic character to ensure

$$2 \leq k(\rho) \leq p + 1.$$

As we learned this morning, Khare–Wintenberger lift ρ to a $\tilde{\rho}_p$ and then insert the representation $\tilde{\rho}_p$ into a compatible system of ℓ-adic representations $(\tilde{\rho}_\ell)$ that reflect properties of the modular form(s) f whose existence we wish to establish.

Conjecturally, we have

$$\rho \overset{?}{\mapsto} f \mapsto (\tilde{\rho}_\ell),$$

but Khare–Wintenberger build $\rho \mapsto (\tilde{\rho}_\ell)$ unconditionally. We use the plural "forms" because it seems essential to use alternative kinds of modular forms (notably weight 2 with level > 1 as well as weight $k(\rho)$ of level 1).

In the simplest construction, Khare–Wintenberger build a system $(\tilde{\rho}_\ell)$ that looks as if it comes from a form of weight $k = k(\rho)$ and level 1. In particular, for each prime ℓ, $\tilde{\rho}_\ell$ is unramified away from ℓ. Locally at ℓ, it is crystalline with Hodge–Tate weights 0, $k - 1$.

We also bring to the table the theorems of modularity lifting that were discussed this morning. Using the results of Skinner–Wiles and Kisin, we infer that a given representation $\tilde{\rho}_\ell$ with $\ell \neq 2$ is modular if its reduction ρ_ℓ is modular and ℓ satisfies

$$k \leq \ell + 1.$$

Of course, once a specific $\tilde{\rho}_\ell$ is modular, the whole family of compatible representations is modular; in particular, ρ will be modular.

An important corollary of this observation is that Serre's conjecture modulo a prime ℓ implies Serre's conjecture for all primes $p \leq \ell$. Indeed, if $p \leq \ell$, then we always have $k \leq p + 1 \leq \ell + 1$; meanwhile, if Serre's conjecture is true mod ℓ, then ρ_ℓ is known to be modular.

In particular, *it suffices to prove Serre's conjecture for an infinite set of primes*!

In most of this discussion we consider only representations that are unramified away from the residue characteristic. (This is the definition of the 'level one case.")

However, in the proof it is necessary to consider some mod p representations that are ramified also at a second prime P.

The strategy of the Khare–Wintenberger proof is to begin with a small set of base cases and then to prove Serre's conjecture mod P (for some $P > p$) on the assumption that it's true mod p.

The proof begins with the base cases $p = 2$, $p = 3$. In the 1970s, Tate showed that all representations $\rho : G \to \mathbf{GL}(2, \overline{\mathbf{F}}_2)$ are reducible by using Odlyzko's discriminant bounds. Soon after, Serre adapted Tate's method to treat the case $p = 3$ in an analogous way.

The next case is $p = 5$. Here, the weight of ρ can take only the three values 2, 4, 6. The first two of these are covered by the inequality $k \leq 3 + 1$ and the fact that the conjecture is known mod 3. We have to worry only about $k = 6$.

If ρ (unramified outside 5) really came from a modular form of weight 6 on $\mathbf{SL}(2, \mathbf{Z})$, it would come alternatively from a weight 2 form on $\Gamma_0(5)$ and would thus arise from the group of 5-division points of the abelian variety $J_0(5)$—which happens to be 0. While it is not possible to use this information directly, we know from Taylor's work that each mod 5 Serre-type representation that's unramified away from 5 can be seen on the 5-division points of some semistable abelian variety over $\mathbf{Q}$ with good reduction outside 5. According to Brumer–Kramer and Schoof, il n'y en a pas.

Now consider $p = 7$. (There is no formal need to consider this case separately, but we can use this case to illustrate the general argument.) Here again, there is a single problematic case, $k = 8 = p + 1$; the other possible weights are no greater than $5 + 1$. Here, for the first time, we use the philosophy of reduction to weight 2.

The representation ρ, supposed to have weight 8, should arise from a weight 2 cusp form f on $\Gamma_0(7)$ with trivial character. Why we can't yet produce the form, we can make the associated "weight two" system of ℓ-adic representations $(\tilde{\rho}_\ell)$. These are semistable at 7 and crystalline at ℓ (if $\ell \neq 7$) of Hodge–Tate weights 0, 1 (i.e., they're Barsotti–Tate).

Let ω be the Teichmüller character character of order 6 and conductor 7. It is worth emphasizing that ω normally takes values in $\mathbf{Z}_7^*$ but can be viewed as taking values in $\overline{\mathbf{Q}}^*$ (because of ι_7) and then in each $\overline{\mathbf{Q}}_\ell^*$ (via ι_ℓ). We will take $\ell = 3$: the square of ω is a character of order 3, and thus trivial mod 3.

If we knew that f existed, we could apply a proposition of Carayol to deduce that there is a form f' of weight 2 on $\Gamma_1(7)$ with character ω^2 such that f and f' are congruent mod 3.

Strictly speaking, we'd need to knew that ρ_3 does not have dihedral image. But if it does, then it's unramified at 7, and we can deduce that it's modular by induction. Then $\tilde{\rho}_3$ is modular, so $\tilde{\rho}_7$ is modular, so $\rho = \rho_7$ is modular. Remarks like these need to be made at *many* places in Khare–Wintenberger.

Since we don't know that f exists, we work directly with the representations. We can construct a system $(\tilde{\rho}'_\ell)$ that has the look and feel of a system coming from the "shadow form" f'. For example, $\rho'_3 \approx \rho_3$, but each $\tilde{\rho}'_\ell$ acquires "everywhere good reduction" over the real subfield of $\mathbf{Q}(\mu_7)$.

The representation ρ'_7 has nothing whatsoever to do with $\rho = \rho_7$. For example, its determinant is ω^5 (as opposed to ω^1 for ρ). An analysis shows that either ρ'_7 has solvable image (so is easily proved to be modular) or has weight < 8 after suitable twisting by powers of the cyclotomic character. In this latter case, ρ'_7 is again modular, this time by induction. Thus the whole system $(\tilde{\rho}'_\ell)$ is modular; in particular, $\rho'_3 \approx \rho_3$ is modular. It follows by modularity lifting again that $(\tilde{\rho}_\ell)$ is modular and then finally that ρ is modular.

"An analysis shows that either ρ_7' has solvable image (so is easily proved to be modular) or has weight < 8 after suitable twisting by powers of the cyclotomic character."

To do this analysis, one has to apply results of a host of people, especially Takeshi Saito ("Hilbert modular forms and *p*-adic Hodge theory"). However, it is easy enough to explain why the indicated result *should* be true: ρ_7' is trying to arise from a weight 2 level-7 form with character ω^2. We get such forms mod 7 from forms of weight 4 on $\mathbf{SL}(2, \mathbf{Z})$ and also by using forms of weight 6 on $\mathbf{SL}(2, \mathbf{Z})$ to make weight 2 forms of level 7 and character ω^4, then twisting the weight 2 forms by ω^{-4} to get a conjugate form with character $\omega^4\omega^{-2\cdot 4} = \omega^{-4} = \omega^2$. Mod 7 eigenforms of weight 2, level 7 and character ω^2 arise either from one construction or the other.

As already mentioned, moving from 5 to 7 serves to illustrate what we need to do in the general induction step. Recall that the aim is to prove the level-one case of Serre's conjecture for an infinite set of primes. We assume that it is true for a prime $p \geq 5$ and show that it is true for a prime $P > p$. Relative to the argument just given, we will make the substitutions

- $5 \rightsquigarrow p$,
- $7 \rightsquigarrow P$,
- $3 \rightsquigarrow q$,

where q is a suitable odd prime dividing $P - 1$.

The fact that there is *some* odd prime dividing $P - 1$ implies that P is not a Fermat prime!

The meaning of "suitable" is that certain refined inequalities need to be satisfied. These inequalities imply the coarser bound $P < 2p - 1$. Thus we are going to visit the world of Bertrand's postulate.

The statement is that for each $p \geq 5$, there is a $P > p$ and an odd prime $q|(P-1)$ with the following property. Suppose that q^r divides $P-1$ exactly ($r \geq 1$) and write $q^r = 2m+1$. Then we have

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

In particular, P is a bit smaller than $2p$.

Let $n = (P-1)/(2m+1)$. It is clear that for each integer a, there is an integer i congruent to a mod n in the interval $[mn, (m+1)n]$. On the other hand, (*) implies that if i lies in this interval, then both $i+2$ and $P+1-i$ are $\leq p+1$.

Assume now that we know Serre's conjecture mod p, and let P be as "above" (i.e., as just discussed). Let ρ be an irreducible Serre-type representation mod P, twisted so as to have weight $k \leq P + 1$. In case $k \leq p + 1$, ρ is modular by the induction hypothesis. Similarly, if ρ has small image, we can prove directly that it is modular.

If ρ is supersingular in the sense that it remains irreducible after restriction to a decomposition group of G at P, then one checks from the definition of the Serre weight that a suitable twist of ρ has weight $P + 3 - k$. We can and do assume $k \geq p + 2$; then it follows from the inequality $P < 2p - 1$ that $P + 3 - k \leq p + 1$, and we can conclude in this case as well that ρ is modular.

The hard case is the remaining "ordinary" case. Here, we use the same philosophy that we used for the weight 8 case mod 7 (which is automatically ordinary).

Namely, we insert ρ into a system $(\tilde{\rho}_\ell)$ that appears to come from a form of weight 2 on $\Gamma_1(P)$ with character ω^{k-2}, where ω is now the mod P Teichmüller character, which has order $P-1$. We view this system as arising from a shadow form f of weight 2 and conductor P.

We examine the reduction of f mod q, which means literally that we look at the representation ρ_q mod q. It has the right to be ramified at P and at q. Its Serre weight is 2. If for some reason we already know that it is modular (e.g., because it happens not to be ramified at P), then we conclude as usual by modularity lifting and moving back to residue characteristic P.

In the most generic case, we don't have a clue about the modularity of ρ'_q. We write $\omega^{k-2} = \theta\omega^i$, where θ is a character of q-power order and i lies in the short interval that we considered before. (Thus i is roughly $P/2$.) Note that $\theta \equiv 1 \bmod q$. If the form f were in our possession, we could use a well known lemma of H. Carayol to show that f is congruent mod q to a form f' of weight 2 on $\Gamma_1(P)$ whose character is ω^i.

We work with what we have—Galois representations. We insert ρ_q into a system $(\tilde{\rho}'_\ell)$ that appears to come from a form like f'. We examine ρ'_P.

As in the case where $P = 7$, $k = 8$, there are two possible minimal weights for ρ'_P after twisting: $k' = i + 2$ and $P + 1 - i = P + 3 - k'$. We have to know that they are both $\leq p + 1$, but we do!

Conclusion

We find that ρ'_P is modular. By lifting, $(\tilde{\rho}'_\ell)$ is modular. Hence $\rho'_q \approx \rho_q$ is modular. Hence $(\tilde{\rho}_\ell)$ is modular, and finally $\rho = \rho_P$ is modular.

This is a real tour de force!