Non-optimal levels of mod ℓ reducible Galois representations or Modularity of residually reducible representations

Kenneth A. Ribet

UC Berkeley

CRM
July 9, 2010

This talk concerns weight-two eigenforms with square free level and trivial character.

Surely the single best-known such form is the very first one: the level-11 form associated to the elliptic curve $y^2 + y = x^3 - x^2 - 10x - 20$ over $\mathbf{Q}$.

Fix a prime number ℓ and an embedding $\overline{\mathbf{Q}} \hookrightarrow \overline{\mathbf{Q}}_\ell$; then the coefficients of our forms are ℓ-adic numbers. Each form f then gives rise to a mod ℓ Galois representation

$$\rho = \rho_f : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathbf{GL}(2, \overline{\mathbf{F}}_\ell).$$

The representation is determined uniquely up to isomorphism once we insist that it be semisimple. If it is reducible, it must be $1 \oplus \chi_\ell$ (up to isomorphism).

If this were a talk on Serre's conjectures, we would focus on the irreducible case. We would fix a target representation ρ and explore the (non-empty!) set of *f*s that give rise to it.

This talk is about the opposite case: our target representation is $1 \oplus \chi_\ell$ instead.

This study was sparked by a question of Dieulefait–Jimenez, who sought to study situations where the field of coefficients $E_f = \mathbf{Q}(\ldots, a_n(f), \ldots)$ has large degree over $\mathbf{Q}$.

Assume that N is even and that $\ell > 2$. Then if $\rho_f \approx 1 \oplus \chi_\ell$, the degree of E_f is bounded from below by a constant times $\log \ell$.

Indeed, we have $a_2(f) \equiv 3 \bmod \lambda$, where λ is the prime of E_f induced by $E_f \hookrightarrow \overline{\mathbf{Q}}_\ell$. Because $a_2(f) - 3$ is a nonzero algebraic integer whose norm is divisible by ℓ, its norm is at least ℓ. At the same time, the norm is bounded from above by $(2\sqrt{2} + 3)^d$, where $d = [E_f : \mathbf{Q}]$. This phenomenon was first pointed out by Barry Mazur in his “Eisenstein ideal” article.

That article studies reducible representations in the case where N is a prime. As Mazur shows, there is an f giving $1 \oplus \chi_\ell$ if and only if ℓ divides the numerator of $(N-1)/12$.

We will take $\ell > 3$ (and are especially interested in the case $\ell = 5$ for computations). Then a prime number N yields our target representation if and only if $N \equiv 1 \bmod \ell$.

In one direction: If $N \equiv 1 \bmod \ell$, then $J_0(N)$ has a constant subgroup $\mathbf{Z}/\ell\mathbf{Z}$ (contained in the cuspidal subgroup of $J_0(N)$). The Hecke ring $\mathbf{T} \subseteq \operatorname{End} J_0(N)$ acts on the $\mathbf{Z}/\ell\mathbf{Z}$ in an Eisenstein fashion (T_r acts as $r+1$ if r is a generic prime number), and one builds f from there.

In the other direction, if $f \mapsto 1 \oplus \chi_\ell$, then f mod ℓ "looks Eisenstein" and can be related to an Eisenstein series: if $a_N(f) = -1$, this is a non-existent form (so we rule out this case), and if $a_N(f) = +1$, this is the standard $\Gamma_0(N)$ Eisenstein series whose constant coefficient is $\frac{N-1}{12}$. This coefficient must match up mod ℓ with f's, which is 0, so we get $N \equiv 1 \bmod \ell$.

More generally, we might have $N = p_1 \cdots p_t$ (product of distinct primes) and $a_{p_i}(f) = \epsilon_i = \pm 1$ for $i = 1, \ldots, t$. If $f \mapsto 1 \oplus \chi_\ell$, then the ϵ_i can't all be -1, and Mazur's argument proves $\prod_i (p_i - \epsilon_i) \equiv 0 \bmod \ell$.

Notation

It seems beneficial to shuffle the p_i so the signs ϵ_i start with a string of 1's and end with a (possibly empty) string of -1's. Let s be the number of 1's; we have $1 \le s \le t$. The number of -1's is $t - s$. We have

$$\epsilon_1 = \cdots = \epsilon_s = +1, \qquad \epsilon_{s+1} = \cdots = \epsilon_t = -1.$$

Let $P = \prod_i (p_i - \epsilon_i) \equiv 0$. Then

$$P = (p_1 - 1) \cdots (p_s - 1) \cdot (p_{s+1} + 1) \cdots (p_t + 1).$$

The question

Fix t (the number of prime factors) and $s \in \{1, \ldots, t\}$ (the number of plus signs).

We seek to characterize the t-tuples $(p_1, \ldots, p_s; p_{s+1}, \ldots, p_t)$ of distinct primes so that there is a newform f of level $N = p_1 \cdots p_t$ with weight two and trivial character such that

- $f|T_{p_i} = f$ for $i = 1, \ldots, s$
- $f|T_{p_i} = -f$ for $i = s+1, \ldots, t$
- The mod ℓ Galois representation associated to f is $1 \oplus \chi_\ell$.

We could call these t-tuples "admissible."

We are looking for the *non-optimal* levels of the Galois representation $1 \oplus \chi_\ell$.

The optimal level for this representation is arguably 1, but since there are no weight-2 cusp forms of level 1, all of our levels are non-optimal.

An immediate observation: if f gives $1 \oplus \chi_\ell$ and $\epsilon_i = -1$, then $p_i \equiv -1 \bmod \ell$. We see this by looking at ρ_f locally at p_i.

Hence in the case where not all signs are $+1$, the congruence $\prod_i (p_i - \epsilon_i) \equiv 1 \bmod \ell$ that we had earlier can be strengthened considerably: each of the last several factors of the product is divisible by ℓ.

We will henceforth assume that all p_i with $i > s$ are $-1 \bmod \ell$. I like to call these primes q_i as well as p_i in order to emphasize that they play a different role from $p_1, \ldots, p_s$.

When all signs are $+1$, the earlier congruence $\prod_i (p_i - \epsilon_i) \equiv 0 \bmod \ell$ just means that ℓ divides $\phi(N)$ (Euler phi).

Overview of the situation

1. In the case that $s = t$ (no minus signs!) and s is *odd*, $(p_1, \ldots, p_s)$ is admissible if and only if ℓ divides $\phi(p_1 \cdots p_t)$.

2. If $(p_1, \ldots, p_t)$ is admissible and q is a $t + 1$st prime (not one of the p_i), then $(p_1, \ldots, p_t, q)$ is admissible (with s unchanged but t augmented by 1). *This has been proved (so far) only when t is odd.*

3. In the case $t = s + 1$ and s odd, $(p_1, \ldots, p_s; q)$ is admissible. Here there is one minus sign and an even number of primes in total. There is no hypothesis that $(p_1, \ldots, p_s)$ be admissible.

4. If $s = t = 2$, I will describe what happens; the description is a bit complicated. (Here there are two plus signs and no minus signs.)

5. If $s = 2$ and $t = 1$, the numerical results are not conclusive.

Take $\ell = 5$ and $p_1 = 11$ and consider only situations with all signs $+1$. As mentioned before, if $(p_1, \ldots, p_s)$ is admissible, then ℓ divides $\phi(p_1 \cdots p_s)$. The converse is true when s is odd but not when s is even.

For a numerical example, take $\ell = 5$ and $p_1 = 11$. Then $(11, 7, 13)$ is admissible but neither $(11, 7)$ nor $(11, 13)$ is admissible. Starting at level 11, you can add 5 and 7 to the level simultaneously but you can neither to the level alone.

Now here's the promised complicated description of what happens when $s = t = 2$:

In order that (p_1, p_2) be admissible, it is necessary that ℓ divide $\phi(p_1 p_2) = (p_1 - 1)(p_2 - 1)$. Assume that this necessary condition is satisfied and that specifically $p_1 \equiv 1 \bmod \ell$.

Then (p_1, p_2) is admissible if and only if p_2 is a *bad* prime for $J_0(p_1)$ and ℓ in the sense of Mazur's Eisenstein ideal paper. This means that $p_2 + 1 - T_{p_2}$ is not a generator of the Eisenstein ideal for $J_0(p_1)$ locally at the Eisenstein prime of residue characteristic ℓ. Equivalently (Mazur), p_2 needs to satisfy at least one of the following two conditions:

- $p_2 \equiv 1 \bmod \ell$,
- p_2 is an ℓth power in $(\mathbf{Z}/p_1\mathbf{Z})^*$.

An empirical observation

Suppose that $(p_1, \ldots, p_t)$ is admissible, and let $N = p_1 \cdots p_t$. Inside $J = J_0(N)$, consider the cuspidal subgroup C of J along with the abelian subvariety J_{new} of J. Computations in sage suggest that $C \cap J_{\mathrm{new}}$ has order divisible by ℓ. Presumably, this would remain true if we replaced C by the appropriate component of C relative to the action of the Atkin–Lehner operators w_{p_i}.

For example, in the case $N = 1001 = 11 \cdot 7 \cdot 13$, the command

```
J.new_subvariety().rational_cusp_subgroup()
```

yields:

```
Finite subgroup with invariants [2, 2, 60]
over QQ of Abelian subvariety of dimension 59
of J0(1001).
```

Methods of proof

Consider for instance the statement that $(p_1, \ldots, p_s)$ is admissible if s is odd and ℓ divides one of the $p_i - 1$. Losing no generality, we assume that ℓ divides $p_1 - 1$. Put $p = p_1$ and $D = p_2 \cdots p_s$.

Let $J = J_0^D(p)$ and consider the component group $\Phi_p(J)$. This group is understood from the work of Deligne–Rapoport and Buzzard; it is Eisenstein and aside from some stuff killed by 6, it is cyclic of order $p - 1$.

One can check that each of the Hecke operators T_{p_i} operates as $+1$ on this cyclic subgroup.

This subgroup cuts out an Eisenstein maximal ideal with residue field $\mathbf{F}_\ell$ in the Hecke algebra associated with the definite quaternion algebra of discriminant Dp. We use the Jacquet–Langlands correspondence to move over to newforms on $\mathbf{GL}(2)$.

More details:

The component group occurs as a quotient $\mathrm{Hom}(X, \mathbf{Z})/X$, where X is the group of degree-0 elements in the free abelian group on the set S of isomorphism classes of left ideals for a fixed maximal order in a quaternion algebra of discriminant Dp. The cyclic group of order $p - 1$ is generated by $\frac{6}{e(s)}\alpha_s$, where $s \in S$ is arbitrary, α_s is the linear form that picks out the coefficient of s in a sum, and $e(s)$ is one-half the order of the group of units in the right order attached to s.

As you can readily see, this argument makes no real use of the Jacobian J; it is purely combinatorial and can be treated in the context of group cohomology.

Basically, this proof that tuples are admissible revisits level-raising techniques, employing quaternion algebras in order not to lose primes that have already been added. These techniques were used definitively by Diamond–Taylor for irreducible residual representations. In the Eisenstein case, complications occur because the usual condition "$T_q \equiv \pm(1+q)$" for raising level is not sufficient by itself.

For example, imagine that we work with the mod 5 representation attached to $J_0(11)$ and wish to raise levels from 11 to $11q$. We can't always do this even though we have $T_q \equiv 1 + q \bmod 5$ for every q. We need a stronger congruence in the case where the sign of the new T_q (known to most as U_q) will be $+1$; this corresponds to the condition that $1 + q - T_q$ not be a local generator of $(5) \subseteq \mathbf{Z}$ at the prime (5) of $\mathbf{Z}$.