# Reducible Galois representations arising from weight-two modular forms

Kenneth A. Ribet

UC Berkeley

Sage Days 22
June 30, 2010

Let's start with an elliptic curve $E$ over $\mathbf{Q}$. For each prime $\ell$, the action of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ on $E[\ell]$ (the group of $\ell$-division points of $E$) defines a representation

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

We can ask various questions about $\rho$, for instance: is $\rho$ *irreducible*? what is the image of $\rho$? These questions was studied intensively by Shimura, Serre and Tate in the late 1960s.

Serre's 1972 article made a big splash with the following result:

**Theorem**

*If $E$ does not have complex multiplication, then $\rho_\ell$ is surjective for all sufficiently large $\ell$.*

It is not known even today whether the “sufficiently large” in Serre’s theorem depends on $E$. On the other hand, B. Mazur’s 1978 article “Rational isogenies of prime degree” shows that if $\rho_\ell$ is reducible, then $\ell$ belongs to the list

$$2, 3, 5, 7, 11, 17, 19, 37, 43, 67, 163.$$

Mazur’s list recalls the set of fundamental discriminants of imaginary quadratic fields with class number 1:

$$-3, -4, -7, -8, -11, -19, -43, -67, -163.$$

There’s a direct connection between the two:

To fix ideas, let $E/\mathbf{Q}$ be an elliptic curve with potential complex multiplication by the ring of integers of $\mathbf{Q}(\sqrt{-163})$ and let $\lambda$ be the unique prime ideal of this integer ring that divides the rational prime 163. The subgroup $E[\lambda]$ of $E[163]$ may be viewed as a 1-dimensional $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$-invariant subspace of $E[163]$, even though the CM is not defined over $\mathbf{Q}$!

We will be interested in the very special case where *E* is semistable; this means that the conductor of *E* is square free. In this case, if $\rho_\ell$ is reducible, then each of the two characters "in the corner" is either the trivial character 1 or the mod $\ell$ cyclotomic character $\chi = \chi_\ell$. (This is the character giving the action of Gal($\overline{\mathbf{Q}}/\mathbf{Q}$) on the group of $\ell$th roots of 1 in $\overline{\mathbf{Q}}$.) Because det $\rho_\ell = \chi_\ell$, one character is 1 and the other is $\chi_\ell$.

If the "upper left-hand corner" character is 1, *E* has a rational point of order $\ell$. If it's $\chi_\ell$, then *E* has a rational subgroup isomorphic to $\mu_\ell$; after dividing by this subgroup, you get an *E*′ isogenous to *E* with a point of order $\ell$. Thus in both cases one emerges with an elliptic curve with a rational point of order $\ell$.

This is a rare event.

Mazur proved in 1977 that if an elliptic curve has a rational point of order $\ell$, then $\ell = 2, 3, 5, 7$. Ogg had predicted this result some years before, and Mazur's confirmation of Ogg's conjecture was viewed as a big breakthrough.

For perspective, it might be interesting to check out the Mazur–Tate article "Points of order 13 on elliptic curves" from 1973–1974 to get an idea of the techniques that were available when people first began to think about the conjecture.

We can start with one of these $\ell$-values. Let's take $\ell = 5$, since 2 and 3 are often "special" in various contexts. What are the elliptic curves with a rational point of order 5? According to the 1976 article "Universal bounds on the torsion of elliptic curves" by Dan Kubert, all such curves may be written

$$y^2 + (1-b)xy - by = x^3 - bx^2, \qquad \Delta = b^5(b^2 - 11b - 1) \neq 0,$$

with $b \in \mathbf{Q}$; the point of order 5 is then $(0, 0)$.

For each $b$, the corresponding curve $E_b$ is semistable; see the 1995 article "Semistable reduction and torsion subgroups of abelian varieties" by Silverberg and Zarhin for a much more general result.

Members of this audience might want to find a formula for the conductor of $E_b$ and then comment on the following question: *Which square-free positive integers are conductors of elliptic curves with a rational point of order 5?*

Actually, the question that I've just asked is unlikely to have a neat answer, but perhaps a more general question has a neat answer and the necessary conditions that emerge from the elliptic curve case will suggest what goes on in general.

It won't be helpful simply to record the conductor for each $E_b$; one should also keep track of some associated signs. Namely, suppose that $\mathrm{cond}(E_b) = p_1 \cdots p_t$, where the $p_i$ are distinct primes. Then, by definition, $E_b$ has multiplicative reduction at each of the $p_i$, and it has good reduction at the other primes. For each $i$, we should record a $+$ sign if the multiplicative reduction at $p_i$ is *split* and a $-$ sign if it's non-split.

# Modular forms

Let $f = \sum a_n q^n$ be the newform of weight two, trivial character and level $N = \mathrm{cond}(E_b)$ that the modularity theorem associates to $E_b$. Then $a_p = \pm 1$ for each $p|N$; the sign is $+$ or $-$ according as the bad multiplicative reduction is split or not.

Giving $f$ is the same thing as giving an isogeny class of elliptic curves. As $E$ runs through the isogeny class, the Galois representations $E[\ell]$ are not necessarily isomorphic, but their semisimplifications are isomorphic.

Accordingly, it is best to think in terms of the association

$$f \mapsto \rho_{f,\ell} := \text{the semisimplification of any } E[\ell].$$

(Here, $\ell$ is no longer specifically 5.)

Now let's remove the restriction that our newforms correspond to elliptic curves. First, we consider weight-two newforms $f = \sum a_n q^n$ with square-free level and trivial character; the $a_n$ are now allowed to be algebraic integers and are no longer required to be ordinary integers.

For a fixed $f$, one gets mod $\ell$ Galois representations as follows: The ring $R := \mathbf{Z}[\ldots, a_n, \ldots]$ is an order in a totally real number field. Each ring homomorphism $R \to \overline{\mathbf{F}}_\ell$ yields a well-defined semisimple representation

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

We focus on the situations where this representation is reducible; if it is, it will be the direct sum of the trivial representation and the mod $\ell$ cyclotomic character.

For later discussion, we should record the fact that reducibility of the representation thus means that we have

$$a_r \equiv 1 + r \quad \text{for almost all primes } r;$$

the congruence means "equality in $\overline{\mathbf{F}}_\ell$."

The ring $R = \mathbf{Z}[\ldots, a_n, \ldots]$ should be thought of as a quotient of the Hecke ring $\mathbf{T} = \mathbf{Z}[\ldots, T_n, \ldots]$ generated by Hecke operators acting on the space generated by the newforms of level $N$, so it might be more natural to write the congruence as

$$T_r \equiv 1 + r \quad \text{for almost all primes } r.$$

Next, we fix a square-free integer $N$ and ask whether there exists a newform $f$ as “above” with level $N$ for which an associated representation is reducible.

This question is slightly too coarse. Instead, we will fix what might be termed a “signed conductor”: we give ourselves a set of distinct prime numbers $p_i$ ($i = 1, \ldots, t$) and for each $p_i$ we give ourselves a sign $\pm$. We ask whether there is an $f$ of level $N = p_1 \cdots p_t$, for which the $a_{p_i}$ have the *chosen signs* and for which one of the associated mod $\ell$ representations is reducible.

To summarize a bit, our question is the following one: We take a prime $\ell$, and to avoid annoying complications we assume $\ell \geq 5$. For which signed conductors can we obtain $1 \oplus \chi_\ell$ as a mod $\ell$ semisimple representation from the set of weight-two cuspforms of signed level $N$?

In my ruminations on this question, I have always taken the conductors to be prime to $\ell$. This is surely not a necessary restriction.

Here are some fragmentary results and facts:

- If all the signs are $-$, we cannot obtain $1 \oplus \chi_\ell$.
- If $N = p$ is prime, and the unique sign is $+$, we can obtain $1 \oplus \chi_\ell$ if and only if $p \equiv 1 \bmod \ell$.
- If all signs are $+$ and $N$ yields $1 \oplus \chi_\ell$, then $\ell$ divides $\phi(N)$ (Euler phi function).
- Suppose that a signed conductor $N$ gives $1 \oplus \chi_\ell$. Then for each $p|N$ with sign $-$, we have $p \equiv -1 \bmod \ell$.
- If $N$ is a product of exactly two primes, we can answer the question, i.e., find necessary and sufficient conditions for $1 \oplus \chi_\ell$ to occur as an associated semisimple mod $\ell$ representation.

Before elaborating on the last point, I'll present two relatively easy theorems that are proved by studying the action of Hecke operators on the component groups of Jacobians of Shimura curves in characteristics where there is bad reduction.

### Theorem

*Suppose that N is a product of an even number of primes and that there is a unique prime p dividing N whose associated sign is $-$. Then N gives rise to $1 \oplus \chi_\ell$ if and only if $p \equiv -1 \bmod \ell$.*

### Theorem

*Suppose that N is a product of an odd number of primes and that all signs are $+$. Then N gives rise to $1 \oplus \chi_\ell$ if and only if $\ell$ divides $\phi(N)$.*

Now back to the case where $N = pq$ is the product of two distinct (signed) primes. One of the signs, at least, has to be $+$. If one sign is $+$ and one is $-$, then we have a necessary and sufficient condition for $N$ to give at least one reducible representation.

Let's assume now that both signs are $+$. Then $\ell$ must divide $(p-1)(q-1)$; without loss of generality, assume $p \equiv 1 \bmod \ell$. Then there's a newform at level $p$ giving rise to $1 \oplus \chi_\ell$, and we are asking whether or not we can "raise the level" and find a form of level $pq$ that gives this same representation.

## Theorem

*We can raise the level from p to pq in this context if and only if $1 + q - T_q$ is not a generator of the Eisenstein ideal at level p locally at the Eisenstein prime of level p that has residue characteristic $\ell$.*

Equivalently: we can raise the level if and only if at least one of the following conditions is satisfied: $q \equiv 1 \bmod \ell$; the image of $q$ in $(\mathbf{Z}/p\mathbf{Z})^*$ is an $\ell$th power.

For example, take $\ell = 5$ and $p = 11$. The first condition means that $q \equiv 1 \bmod 5$ and the second means that $q \equiv \pm 1 \bmod 11$.

# Three factors

Since we know what happens when $N$ is prime and when $N$ is a product of two primes, we should consider the situation $N = pqr$, where the factors are distinct prime numbers (different from $\ell$). Each prime is decorated with a sign, and we might as well shuffle the order of the factors so that the plus signs come first and the minus signs (if any) come at the end.

We already know that all the signs can't be $-$. Thus a priori there are three cases to consider: $(+,+,-)$, $(+,-,-)$, $(+,+,+)$. The third case is covered by the second of the two displayed theorems. Namely, we get $1 \oplus \chi_\ell$ at level $pqr$ if and only if $\ell$ divides $(p-1)(q-1)(r-1)$.

For example, if $\ell = 5$, we can take $N = 7 \cdot 11 \cdot 13$ in the $(+,+,+)$ case. As I pointed out in a lecture two years ago, it is striking that $1 \oplus \chi_\ell$ does *not* occur at level $11 \cdot 7$ or at level $11 \cdot 13$. This situation could not occur for irreducible representations.

In the $(+, -, -)$ case, a necessary condition for getting $1 \oplus \chi_\ell$ at level *pqr* is that we have $q \equiv r \equiv -1 \bmod \ell$. Computation suggests strongly that this condition is sufficient as well. A small challenge will be to establish rigorously what the computation suggests.

A bigger challenge is to figure out what happens is the $(+,+,-)$ case. Here we have $r \equiv -1 \bmod \ell$; let's take $\ell = 5$, $r = 19$ and look for pairs $(p, q)$ such that $1 \oplus \chi_5$ arises at level $19pq$. Adapting some code written by William S., I find that the following pairs $(p, q)$ appear to work:

$$(2,11),(2,23),(2,29),(2,31),(2,37),(2,41),(2,43)$$

and

$$(3,11),(3,29),(3,31),(3,41),(3,43),(3,47).$$

As you can see, we have $p = 2$ or $p = 3$ and $q \leq 47$. If $q \equiv -1$ mod 5, i.e., $q = 29$, $(p, q)$ gets on the list, but we're probably in the $(+,-,-)$ case here. If $q \equiv 1$ mod 5 (i.e., $q = 11$, $q = 31$, $q = 41$) we get on the list, but this time we're probably in the $(+,+,+)$ case.

But what about the pairs with $q \neq \pm 1$ mod 5: $(2,23)$, $(2,37)$, $(2,43)$, $(3,43)$, $(3,47)$? I'm a bit puzzled and could probably benefit from a good conjecture.