Pacific Journal of Mathematics

MOD p REPRESENTATIONS ON ELLIPTIC CURVES

FRANK CALEGARI

Volume 225 No. 1 May 2006

PACIFIC JOURNAL OF MATHEMATICS
Vol. 225, No. 1, 2006

MOD p REPRESENTATIONS ON ELLIPTIC CURVES

FRANK CALEGARI

Modular Galois representations $\bar{\rho} : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{F}_p)$ with cyclotomic determinant arise from elliptic curves for small p. We show that $\bar{\rho}$ does not necessarily arise from an elliptic curve whose conductor is as small as possible outside p. For $p = 3$ this disproves a conjecture of Lario and Rio.

1. Introduction

Let $E/\mathbb{Q}$ be an elliptic curve. For any prime number p, the p-torsion $E[p]$ is a Galois module that gives rise to a continuous Galois representation:

$$\bar{\rho} : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{F}_p).$$

Standard properties of elliptic curves (see [Silverman 1986]) imply that $\bar{\rho}$ is unramified outside p and primes dividing the conductor N_E of E, and that the composition of $\bar{\rho}$ with the determinant map to $\mathbb{F}_p^\times$ is the mod p reduction of the cyclotomic character. Conversely, one expects (by [Serre 1987], at least if $\bar{\rho}$ is irreducible) that such a $\bar{\rho}$ arises in the usual way from a modular form f of level $N(\bar{\rho})$ and weight $k(\bar{\rho})$, for certain prescribed N and k (referred to as the Serre level and weight, respectively). But $\bar{\rho}$ need not arise from an elliptic curve unless p is small.

Theorem 1.1. *Let $p \in \{2, 3, 5\}$. If $\bar{\rho} : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{F}_p)$ is a modular representation with cyclotomic determinant, then $\bar{\rho}$ arises from the p-torsion of an elliptic curve.*

A succinct proof of this result is provided in [Rubin 1997]. The result follows (not entirely formally) from the fact that $X(p)$ has genus zero for such p. In this paper, we address the question of whether the elliptic curve E whose existence is guaranteed by Theorem 1.1 can be chosen to have "minimal" conductor (for a more precise statement, see Theorem 2.1). A conjecture along these lines for $p = 3$ is made in [Lario and Rio 1996], and one of the main motivations for this paper is to find a counterexample to this conjecture. As an afterthought, we discuss some issues related to representations $\bar{\rho}$ with $p \geq 7$.

MSC2000: 11G05.
Keywords: elliptic curves, modular forms, Galois representations.
Supported in part by the American Institute of Mathematics.

2. Small *p*

Let $p \in \{2, 3, 5\}$, and let $\bar{\rho} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_p)$ be an absolutely irreducible Galois representation arising from an elliptic curve E. If $N(\bar{\rho})$ denotes the Serre level of E, then *a priori* one knows that $N(\bar{\rho})$ divides N_E, the conductor of E. By definition, however, the Serre level is coprime to p. Thus if $\bar{\rho}$ is not finite flat at p (and so E has bad reduction at p) we cannot hope to have an equality $N(\bar{\rho}) = N_E$. Allowing for this possibility, we may ask (given $\bar{\rho}$) whether there exists an elliptic curve E giving rise to $\bar{\rho}$ such that $N_E = p^n N(\bar{\rho})$ for some n. Our main result is:

Theorem 2.1. *Let $p \in \{2, 3, 5\}$. There exists a surjective modular representation*:

$$\bar{\rho} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{F}_p)$$

with determinant equal to the cyclotomic character such that $\bar{\rho}$ does not arise from any elliptic curve of conductor $p^n N(\bar{\rho})$ for some n, where $N(\bar{\rho})$ is the Serre level of $\bar{\rho}$.

When $p = 3$, the example we construct provides a counterexample to the following conjecture:

Conjecture 1 [Lario and Rio 1996]. *Let $\mathbf{P}\bar{\rho} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{PGL}_2(\mathbb{F}_3)$ be an irreducible representation. Assume that $\mathbf{P}\bar{\rho}$ has a linear lifting $\bar{\rho}$ to* $\mathrm{GL}_2(\mathbb{F}_3)$ *with cyclotomic determinant. Then there is a linear lifting $\rho_{E,3}$ where $E/\mathbb{Q}$ is an elliptic curve having conductor a power of* 3 *times $N(\mathbf{P}\bar{\rho})$, where $N(\mathbf{P}\bar{\rho})$ is the minimal Serre level of all such liftings.*

Let $\bar{\rho}$ be the representation constructed for $p = 3$ in the proof of Theorem 2.1. Then $N(\bar{\rho}) = 353$ is prime, and thus $N(\mathbf{P}\bar{\rho}) = 353$. Different linear liftings of $\mathbf{P}\bar{\rho}$ with cyclotomic determinant differ by a character χ with $\chi^2 = 1$, or equivalently by a quadratic character. The conjecture guarantees the existence of an elliptic curve $E/\mathbb{Q}$ with $\rho_{E,3} = \bar{\rho} \otimes \chi$, and conductor a power of 3 times 353. In particular, the character χ can only be ramified at three (if it was ramified at 353, the Serre level of $\bar{\rho}$ would be divisible by 353^2). If we let E' denote the quadratic twist of E by χ then E' will also therefore have conductor 353 times a power of 3. On the other hand, by construction, $\rho_{E',3} = \bar{\rho}$, contradicting the fact that $\bar{\rho}$ does not arise from an elliptic curve of such a conductor. Thus the conjecture is false.

The case $p = 2$. Given a Galois representation $\bar{\rho}$ with image $\mathrm{GL}_2(\mathbb{F}_2) \simeq S_3$, there is an obvious way to construct an associated elliptic curve: the associated S_3 field $L/\mathbb{Q}$ is the splitting field of an irreducible cubic polynomial $g(x)$, and the elliptic curve $y^2 = g(x)$ gives rise to $\bar{\rho}$. Let K be a cubic field inside L, and let F be the unique quadratic subfield of L. The Serre weight and level can easily be computed from the arithmetic of K (of course, L is determined from K). In particular, an odd prime p divides $N(\bar{\rho})$ if and only if it divides the field discriminant Δ_K. Let V be the Galois module corresponding to the representation $\bar{\rho}$. Let $\alpha \in \mathbb{O}_K \setminus \mathbb{Q}$, and let $f(x)$ be the minimal polynomial of α. Then $y^2 = f(x)$ is an elliptic curve whose Galois module $E[2]$ is isomorphic to V. Any such elliptic curve arises from such an α. Moreover, if α is not equal to $c+d^2\beta$ for some $c, d \in \mathbb{Z}$ and $\beta \in \mathbb{O}_K$ the equation $y^2 = f(x)$ provides a minimal model for E over $\mathbb{Z}[\frac{1}{2}]$. In particular, the ramification of E at odd primes ℓ can be determined directly from properties of $f(x)$. When does an α give rise to an elliptic curve with Serre level $2^m \cdot N(\bar{\rho})$? The polynomial discriminant of $f(x)$ is equal to Δ_K times the square of the index of $\mathbb{Z}[\alpha]$ inside $\mathbb{O}_K$. Moreover the minimal discriminant of the elliptic curve $y^2 = f(x)$ is equal (up to a power of two) to the polynomial discriminant of $f(x)$. If the prime to 2 part of N_E is equal to $N(\bar{\rho})$, then E has good reduction at every odd prime not dividing $N(\bar{\rho})$. Thus necessarily the polynomial discriminant of $f(x)$ is not divisible by any primes other than those already dividing $2\Delta_K$. This is not sufficient, however, since (for example) the cubic $x^3 - 26$ has discriminant $-2^2 \cdot 3^3 \cdot 13^2$, and yet the elliptic curve $y^2 = x^3 - 26$ has conductor $2^6 \cdot 3^2 \cdot 13^2 = 2^6 \cdot 3 \cdot N(\bar{\rho})$. If the index of $\mathbb{Z}[\alpha]$ inside $\mathbb{O}_K$ is an exact power of two, however, then the odd part of the conductor of E is equal to $N(\bar{\rho})$. We prove:

Theorem 2.2. *Let $K/\mathbb{Q}$ be the cubic field determined by the polynomial $u^3 - u^2 - 2u + 27 = 0$. Then $\Delta_K = -2063$. Let L be the Galois closure of K, and $\bar{\rho}$ the* $\mathrm{GL}_2(\mathbb{F}_2)$ *representation that factors through* $\mathrm{Gal}(L/\mathbb{Q})$. *Then $\bar{\rho}$ does not arise from an elliptic curve of conductor* $2^m \cdot 2063$. *Moreover, K is the smallest cubic field* (*with respect to discriminant*) *with this property.*

Let $N = N(\bar{\rho})$. To show that $\bar{\rho}$ does not arise from an elliptic curve, it suffices to prove that there does not exist an element $\alpha \in \mathbb{O}_K$ such that

$$[\mathbb{Z}[\alpha] : \mathbb{O}_K] \in \mathbb{Z}[1/2N]^\times.$$

First, however, we eliminate all cubic fields with smaller discriminant. As we have noted, for such fields it suffices to construct an element $\alpha \in \mathbb{O}_K$ whose index is a power of two. From the Bordeaux Tables [Cohen et al. n.d.], one can determine all cubic fields $K/\mathbb{Q}$ with $|\Delta_K| \leq 2063$. The only such fields listed whose generating element does not already have index 1 or 2 correspond to the discriminants : $\Delta_K = -1356, -1599, -1691, -1751, -1967, -2028$ (all from complex cubic fields). These fields do in fact have elements of index 2, 1, 2, 8, 1 and 2 respectively. Note that for $\Delta_K = -1751$, there is an element of index 17 which also corresponds to an elliptic curve with conductor $2^m \cdot 1751$. The table on the next page gives these examples, where as usual, $[a_1, a_2, a_3, a_4, a_6]$ denotes the elliptic curve

$$y^2 + a_1 yx + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6.$$

Δ_K	E	$[\mathbb{Z}[\alpha]:\mathcal{O}_K]$	$N(\bar{\rho})$	N_E
-1356	$[0,1,0,-9,-21]$	2	$3\cdot 113$	$2^3N(\bar{\rho})$
-1599	$[0,1,0,-14,-27]$	1	$3\cdot 13\cdot 41$	$2^2N(\bar{\rho})$
-1691	$[0,0,0,-13,-24]$	2	$19\cdot 89$	$2^5N(\bar{\rho})$
-1751	$[0,-6,0,-136,-408]$ $[0,0,0,29,-123]$	8 17	$17\cdot 103$ $17\cdot 103$	$2^6N(\bar{\rho})$ $2^5N(\bar{\rho})$
-1967	$[0,-3,0,-16,51]$	1	1967	$2^4N(\bar{\rho})$
-2028	$[0,-1,0,-17,-27]$	2	$3\cdot 13^2$	$2^3N(\bar{\rho})$

Thus it suffices to consider the cubic field of (prime) discriminant $\Delta_K=-2063$. Let $K=\mathbb{Q}(u)$, where u satisfies the polynomial $u^3-u^2-2u+27=0$. A calculation with Pari shows that

$$\mathcal{O}_K=\mathbb{Z}\oplus(\mathbb{Z}\cdot u)\oplus\left(\mathbb{Z}\cdot\frac{u^2+u}{3}\right).$$

If $\theta=xu+y(u^2+u)/3$, then the index $[\mathbb{Z}[\theta]:\mathcal{O}_K]$ is given by the absolute value of the index form, which in this case is equal to

$$f(x,y)=3x^3+5x^2y+2xy^2+3y^3.$$

It now suffices to prove that the equation $f(x,y)=\pm\,2^m2063^n$ has no integral solutions. Without loss of generality we may assume that x and y are coprime. Suppose that $m>0$. Then $f(x,y)$ is even. A simple congruence check implies that $f(x,y)$ is odd whenever at least one of x or y is odd. Thus x and y are both even, which is impossible if they are coprime, and hence $m=0$. Further, for all x and y, $f(x,y)\equiv 0,3,4,5,6 \mod 9$ whereas $\pm 2063^n\equiv 1,2,7,8 \mod 9$ for $3\nmid n$. Thus 3 divides n. We are therefore reduced to finding elements of $\mathcal{O}_K$ of index exactly 2063^{3n}. Given such an element α its minimal polynomial will have discriminant exactly $-2063(2063)^{6n}$. After subtracting perhaps some multiple of $1/3$ from α (which does not affect the discriminant) the minimal polynomial of α is $x^3-27c_4x-54c_6$, where $c_4, c_6\in\mathbb{Z}[\frac{1}{6}]$. Evaluating the discriminant we find that

$$2^23^9(c_4^3-c_6^2)=-2063\cdot(2063)^{6n}.$$

Thus $[324c_4/2063^{2n}, 5832c_6/2063^{3n}]$ is a $\mathbb{Z}[1/(2\cdot 3\cdot 2063)]$ integral point on the elliptic curve

$$Y^2=X^3+2^4\cdot 3^3\cdot 2063=X^3+891216.$$

Using Cremona's program `mwrank` [n.d.], we compute that this curve has no rational points other than ∞, and thus we are done.

Note that $\bar{\rho}$ does of course arise from the 2-torsion of *some* elliptic curve. The examples $E=[0,0,0,-43,-117]$, $F=[0,-1,0,-2,27]$ of conductors $2^3\cdot 5\cdot$

2063 and $2^4 \cdot 3 \cdot 2063$ show that there are no primes other than 2 and 2063 that necessarily divide the conductor of E. Note also that we needed to go to a cubic field of rather large discriminant before we found an S_3-representation that did not come from an elliptic curve of minimal level. We feel this is explained by the "law of small numbers". In particular, cubic fields of small discriminant tend to be quite special, and tend to have integral elements of very small index. This is not a pattern that persists, however, and one would expect the example constructed above is the norm rather than the exception. It is also why we suspected the conjecture in [Lario and Rio 1996] was false, and set about finding a counterexample.

The case $p = 3$**.** This is the case that requires the most computational power, and I am indebted to John Cremona for reinstalling and reconfiguring his programs on a 64-bit machine provided to Harvard by `Sun Microsystems`. For reasons analogous to the situation for $p = 2$, we may expect that mod 3 representations of small Serre level do arise from elliptic curves of small conductor. Unfortunately, one does not have fine control over the set of elliptic curves with fixed mod 3 representation in quite the same way as one does for mod 2 representations. Thus in order to find a candidate mod 3 representation that does not come from an elliptic curve, we use the following algorithm:

(1) Using William Stein's tables [n.d.], find all modular representations of weight 2 and level N and $3N$. By Serre's conjecture, any irreducible mod 3 representation with cyclotomic determinant and Serre level N should arise at these levels.

(2) Using Cremona's tables [1997; 2005], determine if these representations come from an elliptic curve of conductor $3^k N$, for $3^k N$ no greater than 20000 (the current limit of these tables). If $3^5 N < 20000$ and there are no such elliptic curves then one is done, since 3^5 is the largest possible power of 3 dividing the conductor of an elliptic curve.

(3) If the candidate N is larger than $20000/3^5 \simeq 82.3$ and there are no elliptic curves of conductor $3^k N < 20000$ giving rise to $\bar{\rho}$, try and construct elliptic curves of conductor $3^k N$ with large k by computing $\mathbb{Z}[1/6N]$-integral points on the curves $y^2 = x^3 - 3^k \prod_{\ell | N} \ell^{k_i}$. This method sometimes enables one to eliminate $\bar{\rho}$ without having to compute all the elliptic curves of conductor $3^k N$.

(4) Once a representation $\bar{\rho}$ is found that is not eliminated by any of the previous steps, run Cremona's modular symbols algorithm [1997] for *all* $3^k N$ for $k \le 5$, and determine whether or not those elliptic curves give rise to $\bar{\rho}$.

To simplify step 3, one may choose N to be prime, which cuts down markedly the number of elliptic curves to be considered. Note that steps 2 and 3 are ultimately not required for the proof, but are present to narrow down potential examples, since step 4 is very computationally intensive. Using this method we find:

Theorem 2.3. *Let E be the elliptic curve* $[1, 1, 0, -22, -812]$ *of conductor* $2 \cdot 3 \cdot 353$. *Let* $\bar{\rho} : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{F}_3)$ *be the representation induced from the* 3-*torsion of E. The representation $\bar{\rho}$ is surjective, and the Serre level* $N(\bar{\rho}) = 353$. *Then $\bar{\rho}$ does not arise from any elliptic curve of conductor* $3^k \cdot 353$.

Since E is semistable, the mod 3 representation is either reducible or surjective, and a quick check eliminates the first possibility. Since E is semistable at 2, we may check that $E[3]$ is unramified at 2 by considering the 2-adic valuation of the minimal discriminant. The minimal discriminant is $\Delta_E = -2^{18} \cdot 3 \cdot 353$, and since 3 divides 18 we conclude that $N(\bar{\rho}) = 353$. Specifically it arises from a modular form of weight 2 and level $3 \cdot 353 = 1059$ (in this case coming from part of the 3 torsion on a modular abelian variety A_f of dimension 17).

Proof. It suffices to find all elliptic curves of conductor $3^k \cdot 353$ for $k = 0, \dots 5$ and show that none of them give rise to the mod 3 representation associated to $E[3]$. This follows from the two tables below, which give the trace of Frobenius under the image of $\bar{\rho}$, and the first few $\bar{a}_p = a_p \mod 3$ for the elliptic curves. In fact, we see it would have sufficed to consider a_2. Note that there are no elliptic curves of conductor $3^5 \cdot 353$. □

p	2	3	5	7	11	13	17	19	23	29	31	37
Trace($\bar{\rho}$(Frob$_p$))	0		1	2	1	1	0	1	0	0	1	0

N	E	$\bar{a}_2$	$\bar{a}_3$	$\bar{a}_5$	$\bar{a}_7$	$\bar{a}_{11}$	$\bar{a}_{13}$	$\bar{a}_{17}$	$\bar{a}_{19}$
353	$[1, 1, 1, -2, 16]$	2		2	1	1	2	2	0
1059	$[1, 1, 1, -66, -270]$	2		2	1	1	2	2	0
3177	$[1, -1, 0, -594, 6691]$	1		1	1	2	2	1	0
	$[1, -1, 0, -63, -176]$	1		1	1	2	2	1	0
9531	$[0, 0, 1, 3, 4]$	1		1	1	2	2	1	0
	$[0, 0, 1, -87891, -10029164]$	1		1	1	2	2	1	0
	$[0, 0, 1, 27, -115]$	2		2	1	1	2	2	0
	$[0, 0, 1, -791019, 270787421]$	2		2	1	1	2	2	0
28593	$[1, -1, 1, -2162, -38150]$	2		2	1	1	2	2	0
	$[1, -1, 0, -240, 1493]$	1		1	1	2	2	1	0
85779									

The case $p = 5$.

Theorem 2.4. *Let E be the elliptic curve* $[1, 0, 1, -80, -275]$ *of conductor* $7 \cdot 67$. *Let* $\bar{\rho} : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{F}_5)$ *be the representation induced from the* 5*-torsion of* E. *Then $\bar{\rho}$ is surjective,* $N(\bar{\rho}) = 67$, *and $\bar{\rho}$ does not arise from any elliptic curve of conductor* $5^k \cdot 67$.

Since E is semistable, the mod 5 representation is either reducible or surjective, and a quick check eliminates the first possibility. Since E is semistable at 7, we may check that $E[5]$ is unramified at 7 by considering the 7-adic valuation of the minimal discriminant. The minimal discriminant is $\Delta_E = -7^5 \cdot 67$, and since $5|5$ we conclude that $N(\bar{\rho}) = 67$. Specifically it arises from a modular form of weight 2 and level 67, (in this case coming from part of the 5 torsion on a modular abelian variety A_f of dimension two).

Proof. The proof is easier for $p = 5$ than for $p = 3$, since the largest power of 5 dividing the conductor of elliptic curve is two. Thus we simply enumerate the elliptic curves of conductor 67, $67 \cdot 5$, and $67 \cdot 5^2$, and check using mod 5 congruences that none of the mod 5 representations give rise to $\bar{\rho}$, since $\mathrm{Trace}(\bar{\rho}(\mathrm{Frob}_2)) = 1$ mod 5. □

N	E	a_2
67	$[0, 1, 1, -12, -21]$	2
335	$[0, 0, 1, -2, 2]$	0
1675	$[0, 0, 1, -50, 281]$ $[0, -1, 1, -13, 23]$ $[0, -1, 1, -308, -1982]$ $[0, 1, 1, -333, 2244]$	0 0 3 0

3. Large *p*

We conclude with a few remarks about $p \geq 7$. Let $\bar{\rho} : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{F}_p)$ be a modular Galois representation of level $\Gamma_0(N)$ and weight 2. Elliptic curves with Galois representations corresponding to $\bar{\rho}$ are classified by noncuspidal rational points on the twisted modular curves $X(p)(\bar{\rho}, \wedge)$, where $\wedge$ denotes a choice of symplectic structure on the Galois module associated to $\bar{\rho}$; it is determined by $\bar{\rho}$ up to an element of $\mathbb{F}_p^\times/\mathbb{F}_p^{\times 2}$. If $p \geq 7$, then $X(p)$ has genus > 1, and thus there are only finitely many elliptic curves E which give rise to $\bar{\rho}$, and typically one would not necessarily expect there to be any. If f is an eigenform of weight 2 and level $\Gamma_0(N)$ with coefficients *not* in $\mathbb{Q}$, then one would expect the mod ℓ reductions for $p \geq 7$ also to typically not arise from an elliptic curve.

Theorem 3.1. *Let $f \in S_2(\Gamma_0(N))^{new}$, let the coefficients of f generate the ring $\mathbb{O}_f$, and assume that $\mathbb{O}_f \neq \mathbb{Z}$. Then for all but finitely many primes $\mathfrak{p}$ of $\mathbb{O}_f$, the representation*

$$\bar{\rho}_{\mathfrak{p}} : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{O}/\mathfrak{p}) \hookrightarrow \mathrm{GL}_2(\bar{\mathbb{F}}_p).$$

does not come from an elliptic curve.

Proof. Let $f \in S_2(\Gamma_0(N))^{new}$, and let $\mathbb{O}_f$ be the ring generated by coefficients of f.

Lemma 3.2. *If $\mathbb{O}_f \neq \mathbb{Z}$, then there exists a prime ℓ with $(\ell, N) = 1$ and such that $a_\ell(f) \notin \mathbb{Q}$.*

Proof. Let $\mathfrak{p}$ be a prime in $\mathbb{O}_K$ of residue characteristic p such that $\mathbb{O}_K/\mathfrak{p} \neq \mathbb{F}_p$. Suppose moreover that $(p, 2N) = 1$. Then the associated Galois representation

$$\rho_{\mathfrak{p}} : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{O}_K/\mathfrak{p})$$

has image that does not land within $\mathbb{F}_p$. This is because the Hecke eigenvalues a_q for $q|N$ are automatically 0 or 1 since f is a newform, and the eigenvalue a_p for $p > k = 2$ is determined from the mod p representation [Edixhoven 1992]. Now the fact that the trace of $a_\ell \mod \mathfrak{p}$ is the trace of Frobenius for $(\ell, Np) = 1$ and the fact that Frobenius elements are dense guarantees an infinite number of such primes ℓ. □

Note the lemma and theorem are not true for oldforms. Take $N = 33$. Then the old form of level 11 has coefficients in $\mathbb{Q}(x)/(x^2+x+3)$, yet $a_\ell \in \mathbb{Z}$ for all $\ell \neq 3$. Moreover, the mod p representation coming from these old forms is exactly the mod p representation coming from the elliptic curve $X_0(11)$.

Fix such an ℓ as in the lemma above. Now suppose that the mod p representation attached to f comes from an elliptic curve E. Assume that $p \geq 5$. If E has additive reduction at ℓ then since $p \geq 5$, the field $\mathbb{Q}(E[p])$ is ramified at ℓ with ramification index divisible by 2 or 3. This forces the Serre level of $\bar{\rho}$ to be divisible by ℓ^2 which forces a_ℓ to be zero, contradicting our assumption that $\ell \notin \mathbb{Q}$. If E has good reduction, then a_ℓ is determined by the mod ℓ representation, and satisfies the Hasse bound $-2\sqrt{\ell} < a_\ell(E) < 2\sqrt{\ell}$. Moreover $a_\ell \equiv a_\ell(E) \mod \mathfrak{p}$. If E has multiplicative reduction at ℓ, then either $\ell|N$ in which case $a_\ell = \pm 1$ (which is impossible if $a_\ell \notin \mathbb{Q}$), or one can "raise the level" in the sense of Ribet [1990]. This is possible only if $a_\ell^2 \equiv (1+\ell)^2 \mod \mathfrak{p}$. In particular, if

$$A(\ell) = (a_\ell^2 - (1+\ell)^2) \prod_{|i|<2\sqrt{\ell}} (a_\ell - i),$$

then $A(\ell) \equiv 0 \mod \mathfrak{p}$. Yet $A(\ell)$ is independent of $\mathfrak{p}$, and since a_ℓ is not in $\mathbb{Q}$, $A(\ell)$ is nonzero, and thus there are only finitely many such $\mathfrak{p}$. Note in any example we may explicitly rule out all but finitely many primes $\mathfrak{p}$. This concludes the proof of Theorem 3.1. □

Theorem 3.3. *Let* $p \geq 11$. *Then there exists a modular semistable Galois representation* $\bar{\rho} : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{F}_p)$ *of weight* 2 *and level* $\Gamma_0(N)$ *that does not arise from any elliptic curve.*

Proof. We apply explicitly the proof of Theorem 3.1 to three particular forms: the form $f \in S_2(\Gamma_0(23))$ with $\mathbb{O}_f = \mathbb{Z}[(1+\sqrt{5})/2]$, the form $f \in S_2(\Gamma_0(39))$ with $\mathbb{O}_f = \mathbb{Z}[\sqrt{2}]$ and the form $f \in S_2(\Gamma_0(590))$ with $\mathbb{O}_f = \mathbb{Z}[\sqrt{10}]$. For example, for $f \in S_2(\Gamma_0(23))$ we may take $\ell = 2$, since $a_2 = (\sqrt{5}-1)/2$. Then $N_{K/\mathbb{Q}}(A(2))$ is divisible by only the primes 5 and 11. Thus the associated representations for $p > 5$ and $p \neq 11$ do not come from elliptic curves. Moreover, the representation has image inside $\mathrm{GL}_2(\mathbb{F}_p)$ whenever the prime p splits in $\mathbb{O}_f$, or equivalently whenever $(5/p) = 1$. Similar calculations for the other forms show that if $p > 11$, we are done whenever $(2/p) = 1$ or $(10/p) = 1$. Yet since

$$\left(\frac{2}{p}\right)\left(\frac{5}{p}\right) = \left(\frac{10}{p}\right),$$

at least one of these three terms must equal one, and thus we have found a $\mathrm{GL}_2(\mathbb{F}_p)$ representation that does not arise from an elliptic curve for all $p > 11$. For $p = 11$ one can use the same idea, except with a different form, for example $f \in S_2(\Gamma_0(62, \mathbb{F}_{11}))$ with $a_3 \equiv 6 \mod 11$. □

This proof does not apply to $p = 7$, since all possibilities for $\mathrm{Trace}(\bar{\rho}(\mathrm{Frob}_2))$ mod 7 arise from elliptic curves. If $a_2 \equiv \pm 3 \mod 7$, then E must necessarily be semistable at 2 but have a 7-torsion module that is unramified at 7 (and so by Tate's theory necessarily have $a_2 \equiv \pm(1+2) \mod 7$). For example, when $N = 55$, there is a form f with coefficients in $\mathbb{Z}[\sqrt{2}]$ and $a_2 = 1 + \sqrt{2}$. Composing this with the reduction map to $\mathbb{F}_7$ that sends a_2 to $4 \mod 7$ we obtain a candidate $\bar{\rho}$. Raising the level, we see this representation occurs from the mod 7 reduction of a newform of level $2 \cdot 55 = 110$. Indeed, we find that the 7 torsion on the elliptic curve $E := [1, 0, 1, -89, 316]$ gives rise to $\bar{\rho}$. (An easy way to check this is to compute that $\Delta_E = -2^7 \cdot 5 \cdot 11^3$, and so the associated mod 7 representation is unramified at 2 and so comes from a mod 7 representation of level 55.) Nevertheless, we prove:

Theorem 3.4. *There exist irreducible representations* $\bar{\rho} : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{F}_7)$ *with cyclotomic determinant that do not arise from elliptic curves over* $\mathbb{Q}$.

Proof. We construct such representations directly. Let $F = \mathbb{Q}(\sqrt{-7})$, and let p be an inert prime in $\mathbb{O}_F$ such that $p \equiv -1 \mod 16$ (for example, $p = 31$). Inside the ray class field over F of conductor (p) there exists a Galois (over $\mathbb{Q}$) extension K of degree 8 over $\mathbb{Q}$ such that $\mathrm{Gal}(K/\mathbb{Q})$ is dihedral, and K/F is totally ramified at p. Let $L = \mathbb{Q}(\zeta_7)$, and let $H = K.L$. Then $\mathrm{Gal}(H/F)$ is cyclic of degree 24, and

$\mathrm{Gal}(F/\mathbb{Q})$ acts on $\mathrm{Gal}(H/F) \simeq \mathbb{Z}/24\mathbb{Z}$ as multiplication by 7 (fixing the subgroup of order 3, and as inversion on the subgroup of order 8). Thus there is a map

$$\bar{\rho} : \mathrm{Gal}(H/\mathbb{Q}) \hookrightarrow \mathrm{GL}_2(\mathbb{F}_7)$$

with image of index exactly two inside the normalizer of the nonsplit Cartan subgroup (recall the normalizing element acts as conjugation on $\mathbb{F}_{49}^{\times} \simeq \mathbb{Z}/48\mathbb{Z}$, and thus as multiplication by 7). A suitable renormalizing of the nonsplit Cartan ensures that $\bar{\rho}$ has cyclotomic determinant. Another realization of $\bar{\rho}$ is the ω^2-twist of the dihedral representation $\eta : \mathrm{Gal}(K/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{F}_7)$ (in this optic we also observe that $\bar{\rho}$ is modular), where ω is the cyclotomic character. The determinant of η is the quadratic character of conductor 7, which is $\omega^3 \mod 7$. Thus $\omega^2 \otimes \eta$ has determinant $\omega^7 = \omega \mod 7$. Let us now prove that $\bar{\rho}$ does not come from an elliptic curve. Assume that $\bar{\rho}$ arises from the 7-division points of $E/\mathbb{Q}$. All elliptic curves over $\mathbb{Q}$ acquire semistable reduction after an extension of degree at most 6. Moreover, for an elliptic curve with semistable reduction at a prime $p \neq 7$, the action of inertia at p on the 7-torsion is either trivial (in the case of good reduction, by Néron–Ogg–Shafarevich) or factors through a cyclic 7-group (as can be seen from Tate's parameterization). We see that $\#\bar{\rho}|_{I_p} = 8$ is incompatible with either possibility. □

If $(N, p) = 1$ and $p \geq 5$, the curve $X_0(p^2N)$ acquires semistable reduction over an extension of degree $(p^2 - 1)/2$; see [Edixhoven 1990]. Presumably many of the $\mathbb{F}_7$-representations of this level have significant inertia at p, and thus do not arise from elliptic curves for the reasons above. It would be interesting, however, to find an example of an irreducible representation $\bar{\rho}$ such that $X(7)(\bar{\rho})$ has points over *every* local completion of $\mathbb{Q}$ but no rational points. Dieulefait [2004] has also proved Theorems 3.3 and 3.4, the former using similar arguments with a rational form of weight 4, and the latter by finding a representation whose local representation at 2 does not come from an elliptic curve.

Acknowledgements

I thank Akshay Venkatesh and Kiran Kedlaya for an informative discussion about cubic fields, Ken Ribet for bringing to my attention the paper [Lario and Rio 1996], and William Stein for some computational help. I especially thank John Cremona for help with the computation for $p = 3$.

References

[Cohen et al. n.d.] H. Cohen et al., "Tables of data on number fields", Available at ftp://megrez.math.u-bordeaux.fr/pub/numberfields.

[Cremona 1997] J. E. Cremona, *Algorithms for modular elliptic curves*, Cambridge University Press, Cambridge, 1997. MR 99e:11068 Zbl 0872.14041

[Cremona 2005] J. Cremona, “Elliptic curve data”, 2005, Available at http://modular.fas.harvard.edu/cremona/INDEX.html. Online database.

[Cremona n.d.] J. Cremona, “mwrank”, Available at http://www.maths.nott.ac.uk/personal/jec/ftp/progs. Software (requiring NTL or LiDIA).

[Dieulefait 2004] L. Dieulefait, “Existence of non-elliptic mod ℓ Galois representations for every $\ell > 5$”, Preprint, 2004. math.NT/0404025

[Edixhoven 1990] B. Edixhoven, “Minimal resolution and stable reduction of $X_0(N)$”, *Ann. Inst. Fourier* (*Grenoble*) **40**:1 (1990), 31–67. MR 92f:11080 Zbl 0679.14009

[Edixhoven 1992] B. Edixhoven, “The weight in Serre’s conjectures on modular forms”, *Invent. Math.* **109**:3 (1992), 563–594. MR 93h:11124 Zbl 0777.11013

[Lario and Rio 1996] J.-C. Lario and A. Rio, “Elliptic modularity for octahedral Galois representations”, *Math. Res. Lett.* **3**:3 (1996), 329–342. MR 97d:11088 Zbl 0870.11035

[Ribet 1990] K. A. Ribet, “On modular representations of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ arising from modular forms”, *Invent. Math.* **100**:2 (1990), 431–476. MR 91g:11066 Zbl 0773.11039

[Rubin 1997] K. Rubin, “Modularity of mod 5 representations”, pp. 463–474 in *Modular forms and Fermat’s last theorem* (Boston, 1995), edited by G. Cornell et al., Springer, New York, 1997. MR 1638489 Zbl 0914.11030

[Serre 1987] J.-P. Serre, “Sur les représentations modulaires de degré 2 de $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$”, *Duke Math. J.* **54**:1 (1987), 179–230. MR 88g:11022 Zbl 0641.10026

[Silverman 1986] J. H. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics **106**, Springer, New York, 1986. MR 87g:11070

[Stein n.d.] W. A. Stein, “The Modular Forms Database: related data about elliptic curves, abelian varieties, etc.”, Available at http://modular.math.washington.edu/Tables/.

Received August 31, 2004.

FRANK CALEGARI
DEPARTMENT OF MATHEMATICS
HARVARD UNIVERSITY
1 OXFORD STREET
CAMBRIDGE, MA 02138
UNITED STATES

fcale@math.harvard.edu