Mathematical Research Letters **3**, 329–342 (1996)

ELLIPTIC MODULARITY FOR OCTAHEDRAL GALOIS REPRESENTATIONS

Joan-C. Lario and Anna Rio

Abstract. Let $\rho : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathrm{GL}_2(\mathbf{F}_3)$ be a residual representation with cyclotomic determinant and splitting field of degree at least 16. First we show that ρ is isomorphic to the Galois representation attached to the 3-torsion points of an elliptic curve which is modular. Then we discuss some facts about minimality of conductors.

1. Introduction

Let $\rho : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathrm{GL}_2(\overline{\mathbf{F}}_p)$ be an odd irreducible representation. As the modular deformation theory of residual representations shows, whenever ρ is modular it can be attained by infinitely many weight 2 newforms lying in the Hecke algebras for $\Gamma_1(N)$, with N being divisible by the primes at which ρ is ramified. To each of these newforms correspond a modular abelian variety which is isogenous to a factor of the jacobian variety $\mathbf{J}_1(N)$.

On the other hand, Serre [S] has conjectured that any such ρ is modular. This is known for Galois representations to $\mathrm{GL}_2(\mathbf{F}_2)$ and $\mathrm{GL}_2(\mathbf{F}_3)$, due to a theorem of Langlands [La] and Tunnell [Tu]; the first case going back essentially to Hecke. Recent results of Shepherd-Barron and Taylor [SB-T] show that this is also true for icosahedral representations to $\mathrm{GL}_2(\mathbf{F}_4)$ and $\mathrm{GL}_2(\mathbf{F}_5)$ with some ramification conditions.

In this paper, we will focus our attention on the octahedral case. More precisely, we will consider residual representations $\rho : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathrm{GL}_2(\mathbf{F}_3)$ with cyclotomic determinant and splitting field of degree at least 16.

In the first sections, our aim is to show that in this case the modularity of ρ can be attained by a modular elliptic curve.

Theorem 1. *Let $\rho : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathrm{GL}_2(\mathbf{F}_3)$ be a Galois representation with cyclotomic determinant and splitting field of degree at least 16. Then there is a modular elliptic curve $E/\mathbf{Q}$ such that ρ is isomorphic to $\rho_{E,3}$.*

The key point is to take advantage of considering the projective Galois representations instead of the linear ones. The proof of the theorem goes

Received November 3, 1995.

Research of the authors was supported in part by DGICYT grants PB93–0815 and PB93–0034, respectively.

as follows. Associated with the projective representation

$$\bar{\rho} : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \xrightarrow{\rho} \mathrm{GL}_2(\mathbf{F}_3) \to \mathrm{PGL}_2(\mathbf{F}_3)\,,$$

we consider the moduli space $\mathbf{PX}(3, \bar{\rho})$ which classifies isomorphism classes of elliptic curves whose projective Galois representation attached to the 3-torsion module is isomorphic to $\bar{\rho}$. An explicit description of this moduli space can be found in [L-R]. Then, we study the behavior of Wiles' hypothesis in [W, Theorem 0.3] over the elliptic curves which correspond to the rational points of $\mathbf{PX}(3, \bar{\rho})$. Finally, we are well placed to show the existence of a *modular point* in $\mathbf{PX}(3, \bar{\rho})$ which, using the fact that two linear liftings differ by a quadratic twist, produces the modular curve E as in the statement.

In the last section, we discuss some facts concerning the minimality of the conductors of the elliptic curves over $\mathbf{Q}$ whose $3-$division points realize the linear liftings of the projective representation $\bar{\rho}$.

To end this introduction we recall that recent results of Wiles [W], Taylor-Wiles [T-W], and Diamond [D] ensure the Shimura-Taniyama-Weil conjecture for a large class of elliptic curves over $\mathbf{Q}$, and that more work and new methods seem to be needed in order to provide a complete proof of the conjecture. In the meanwhile, we have the following corollary which is hoped to be antiquated in a not-too-distant future:

Corollary 1. *Let E be an elliptic curve over $\mathbf{Q}$ such that $\mathrm{Gal}(\mathbf{Q}(E[3])/\mathbf{Q})$ is isomorphic either to $\mathrm{GL}_2(\mathbf{F}_3)$ or to its 2-Sylow subgroup. Then, there is an elliptic curve E_s over $\mathbf{Q}$ such that $E[3] \simeq E_s[3]$ as Galois modules and E_s is modular.*

Note that the hypothesis cover all the cases where $\rho_{E,3}$ is irreducible except for the image being isomorphic to the dihedral group of order 8, which corresponds to the discriminant of the elliptic curve being a cube and the polynomial giving the x-coordinates of the 3-torsion points of E factoring as two irreducible quadratic polynomials over $\mathbf{Q}$.

2. The moduli space $\mathbf{PX}(3, \bar{\rho})$

Let $\bar{\rho} : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathrm{PGL}_2(\mathbf{F}_3)$ be a projective Galois representation as above, i.e. having a linear lifting with cyclotomic determinant and splitting field of degree at least 16. The explicit model of the moduli space $\mathbf{PX}(3, \bar{\rho})$ given in [L-R] for the surjective case works as well under our current hypothesis on $\bar{\rho}$. In particular, we know that all the linear liftings of $\bar{\rho}$ into $\mathrm{GL}_2(\mathbf{F}_3)$ are elliptic. That means that each one of these liftings is isomorphic to the Galois representation $\rho_{E,3}$ attached to the 3-torsion points of some elliptic curve E over $\mathbf{Q}$.

The rational points of $\mathbf{PX}(3,\bar{\rho})$ are in one-to-one correspondence with the elliptic curves over $\mathbf{Q}$ (up to twists) giving the elliptic linear liftings of the fixed $\bar{\rho}$. We recall that $\mathbf{PX}(3,\bar{\rho})$ has two irreducible components of genus zero and a model of $\mathbf{PX}(3,\bar{\rho})$ can be given as follows:

$$C_1 : Q_1(m,n,p) = 2\,a\,m^2 + n^2 - m\,p\,,$$
$$C_2 : Q_2(m,n,p) = (7a^2m^2 + 12\,b\,m\,n + 4\,a\,n^2 - 10\,a\,m\,p + 3\,p^2)/9\,,$$

where $E/\mathbf{Q} : y^2 = x^3 + a\,x + b$ is an elliptic curve producing a linear lifting of $\bar{\rho}$. Finding an explicit Weierstrass equation for E requires only to represent zero by a quadratic form attached to a polynomial describing $\bar{\rho}$.

The conics C_1 and C_2 can be parametrized by:

$$C_1 : q_1(t) = [1 : t : 2\,a + t^2]\ , \text{ and}$$
$$C_2 : q_2(t) = [a(3\,a + 4\,t^2) : -4\,t(a^2 + 3\,b\,t) : a(7a^2 + 12\,b\,t + 4\,a\,t^2)]\,,$$

and the corresponding elliptic curves (up to twists) have Weierstrass equations

$$E_{i,t} : y^2 = x^3 + A_i(t)\,x + B_i(t), \qquad i = 1,\,2,$$

where $A_i(t)$ and $B_i(t)$ are the following polynomials:

$$\begin{aligned}
A_1(t) &= (-a^3 - 9\,b^2 - 6\,a\,b\,t - 6\,a^2t^2 + 18\,b\,t^3 + 3\,a\,t^4)/3\,;\\
B_1(t) &= (-3\,b\,a^3 - 18\,b^3 - 4\,a^4t - 18\,a\,b^2t + 15\,a^2b\,t^2 - 90\,b^2t^3\\
&\qquad - 45\,a\,b\,t^4 - 12\,a^2t^5 + 9\,b\,t^6)/9\,;\\
A_2(t) &= 4\,a\,\Delta(3\,a^3 + 24\,a^2t^2 + 96\,b\,t^3 - 16\,a\,t^4)/3\,;\\
B_2(t) &= 64\,\Delta(9\,a^6b - 24\,a^7t - 180\,a^5b\,t^2 - 720\,a^3b^2t^3 + 240\,a^4b\,t^4\\
&\qquad - 64\,a^2(2\,a^3 + 9\,b^2)t^5 - 192\,b(a^3 + 6\,b^2)t^6)/9\,.
\end{aligned}$$

As for the discriminants, we have

$$\Delta_1(t) = \Delta\,f(t)^3 = 27\,\Delta\,Q_2(q_1(t))^3\,,$$
$$\Delta_2(t) = -\frac{\Delta^2}{27}\,Q_1(q_2(t))^3\,.$$

Here $\Delta = -16(4\,a^3 + 27\,b^2) = \Delta_1(\infty)$ is the discriminant of $E : y^2 = x^3 + a\,x + b$, and $f(x) = x^4 + 2\,a\,x^2 + 4\,b\,x - a^2/3$ is the polynomial giving the x's coordinates of the 3-torsion points of E.

From these formulas, it follows straightforward that the four intersection points of the conics are the cusps of $\mathbf{PX}(3,\bar{\rho})$. Although rational values of t already parametrize all the rational elliptic curves we are interested

in, it is worth noting that nonrational (though algebraic) values of t yield rational values of the corresponding j-invariants:

$$j_i(t) = \frac{c_{4,i}(t)^3}{\Delta_i(t)}\,,$$

for instance one can have $j_1(t_1) = j_2(t_2)$ with t_1 rational, but not t_2. Thus what we have is two forgetful morphisms $j_i : C_i \to \mathbf{P}^1$ of degree 12. The two irreducible components of $\mathbf{PX}(3, \bar{\rho})$ reflect the isometric and anti-isometric isomorphisms (with respect to the Weil pairing) between the 3-torsion modules of the elliptic curves over the two conics. We refer to [Ru-Si] for a slightly different parametrization of the family of elliptic curves with constant mod 3 Galois representation and fixed Weil pairing.

3. Deformations of elliptic type

Let E over $\mathbf{Q}$ be an elliptic curve and consider $\rho : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathrm{Aut}(E[3])$. We shall say that E is of Wiles' type if the following three conditions hold:

W1) E has good or multiplicative reduction at 3,

W2) ρ is absolutely irreducible when restricted to $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}(\sqrt{-3}))$,

W3) For any $q \equiv -1 \pmod 3$, either $\rho \mid D_q$ is absolutely reducible or $\rho \mid I_q$ is absolutely irreducible.

As usual, here D_q denotes a decomposition group at q and I_q its inertia subgroup. By [W, Theorem 0.3], the above conditions ensure the modularity of the elliptic curve E though, as the improvements in [D] show, condition W3 is actually not needed.

Our goal now is to study the behavior of conditions W1, W2, and W3 over the family of elliptic curves attached to

$$\bar{\rho} : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathrm{PGL}_2(\mathbf{F}_3),$$

which is assumed to be as in the previous section. We fix some notation. Let $E : y^2 = x^3 + a\,x + b$ be an elliptic curve over $\mathbf{Q}$ such that $\rho : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathrm{Aut}(E[3])$ is a lifting of $\bar{\rho}$. As before, denote by $f(x)$ the monic quartic polynomial giving the x-coordinates of the 3-torsion points of E. The field obtained by adjoining a root of $f(x)$ will be denoted by K_1.

We are going to begin with the analysis of conditions W2 and W3 since they are projective properties in the sense that they depend only on $\bar{\rho}$. In others words, W2 and W3 are contagious properties over the conics, whereas condition W1 is certainly not.

The condition W2 concerns with how big is the image of the absolute Galois group under the morphism ρ and it can be rephrased in different

ways. Under our assumptions on $\bar{\rho}$, we have two disjoint cases. In the surjective case the restriction of ρ to $\mathrm{Gal}(\mathbf{Q}/\mathbf{Q}(\sqrt{-3}))$ has image isomorphic to $\mathrm{SL}_2(\mathbf{F}_3)$, hence it is absolutely irreducible. In the other case, the image of the linear liftings is the 2-Sylow subgroup of $\mathrm{GL}_2(\mathbf{F}_3)$, and the restriction has image isomorphic to the quaternionic group, being also absolutely irreducible.

Now, let us discuss the condition W3. For the sake of simplicity, we are going to restrict ourselves to the case when $\bar{\rho}$ is surjective.

Proposition 1. *Assume that $\bar{\rho}$ is as above and surjective. Let q be a prime, with $q \equiv -1 \pmod 3$. Then the following statements are equivalent:*
i) *E satisfies W3 at q,*
ii) *q does not decompose in K_1 as $\mathfrak{p}^2\mathfrak{p}'^2$,*
iii) *$\rho(D_q)$ is not isomorphic to the dihedral group of order 8.*

The proof of the proposition rely on the study of all possible chains for the higher ramification groups at different primes q in the splitting field of ρ, which under the assumptions is an extension of $\mathbf{Q}$ with Galois group isomorphic to $\tilde{S}_4 \simeq \mathrm{GL}_2(\mathbf{F}_3)$. Of course, the most intricate case is $q = 2$ where the determination of all the extensions of $\mathbf{Q}_2$ having Galois group a subgroup of $\mathrm{GL}_2(\mathbf{F}_3)$ is needed. All this is accomplished by one of the authors in [R].

Observe that from ii) in the above proposition we get another description of the projective nature of condition W3.

Now we translate this result in terms of the geometry of the elliptic curve E.

Proposition 2. *Assume that $\bar{\rho}$ is surjective, and let $q \equiv -1 \pmod 3$ be a prime. For the elliptic curve E we distinguish:*
i) *If q is odd, then condition W3 fails at q if and only if q-Kodaira$(E) = III$ or III^* and $q \equiv -1 \pmod{12}$.*
ii) *Condition W3 fails at 2 if and only if 2-Kodaira$(E, E_{(2)}) = III$ or III^*, $v_2(j) = 6$, and $j/2^6 \equiv \Delta/2^{v_2(\Delta)} \equiv 1 \pmod 4$.*

Here $E_{(2)}$ stands for the twisted elliptic curve obtained from E by the quadratic character of $\mathbf{Q}(\sqrt{2})$, Δ and j being the discriminant and the modular invariant of E. If q is an odd prime, the claim follows easily along the lines in [R]. We shall sketch the proof for $q = 2$, which is more elaborated. We are going to make use of the following lemma for which we are grateful to Montes [M]; its proof is done case-by-case using the Newton polygon method.

Lemma 1. *Let $f = x^4 + a\,x^2 + b\,x - a^2/12$ be an irreducible polynomial in $\mathbf{Q}[x]$, and let K_1 be the quartic field defined by a root of f. Assume that the coefficients of f are 2-adic integers with $v_2(a) \leq 2$ or $v_2(b) \leq 2$. Then, we have $2 = \mathfrak{p}^2\mathfrak{p}'^2$ in K_1 if and only if*

$$v_2(a) = 2\,, \quad v_2(b) = 5\,, \text{ and } \ \frac{a}{4} \equiv 1 \pmod 4\,.$$

Suppose first the case when E has Kodaira type III and $E_{(2)}$ has type III^* at 2. Just replacing E by the twist $E_{(2)}$, the argument below will provide the proof for the interchanged Kodaira type case.

Since E has Kodaira type III at 2, in particular there is a 2-standard model (in the sense of [N, Chap. III, Sec. 7]) $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ for E with

$$v_2(a_i) \geq 1\,, \quad v_2(a_4) = 1\,, \text{ and } \ v_2(a_6) \geq 2\,.$$

If we add that $E_{(2)}$ has Kodaira type III^* at 2, then we get also

$$v_2(b_6) > 2 \text{ and } \ v_2(b_2) > 2\,.$$

Hereafter the $b's$ and $c's$ are referring to the standard formulae for elliptic curves and the above valuations can be read in [C]. Therefore, $x^4 - 6\,c_4x^2 - 8\,c_6x - 3\,c_4^2$ is a polynomial defining the quartic extension K_1 and we have $v_2(c_4) = 5$ and $v_2(c_6) \geq 7$. The change of the variable x by $4x$ yields the polynomial

$$f = x^4 - 12\,d_4x^2 - 16\,d_6x - 12\,d_4^2$$

with $d_4 = c_4/2^5$ and $d_6 = c_6/2^7$. On the other hand, we have $v_2(\Delta) = 9$ since we also assume that $v_2(j) = 6$. Thus, we can write

$$\frac{j}{2^6} = \frac{(c_4/2^5)^3}{(\Delta/2^9)}\,,$$
$$3^3\frac{\Delta}{2^9} = (\frac{c_4}{2^5})^3 - 2(\frac{c_6}{2^8})^2\,.$$

Moreover, together with the congruences mod 4 we get $c_4/2^5 \equiv 1 \pmod 4$ and $v_2(c_6) = 8$. From this, we have

$$\begin{aligned} v_2(-12\,d_4) &= 2 \\ v_2(-16\,d_6) &= 5 \\ -3\,d_4 &\equiv 1 \pmod 4\,. \end{aligned}$$

Therefore, the lemma applies to the polynomial f and we see that the decomposition of 2 in K_1 is $\mathfrak{p}^2\mathfrak{p}'^2$.

Now we assume the prescribed decomposition for 2 in K_1. Consider a model of $E : y^2 = x^3 + A\,x + B$ with A and B integers. Thus, $x^4 + 2\,A\,x^2 +$

$4\,B\,x - A^2/3$ is a polynomial defining K_1. By performing the change of variable x by $2x$ as many times as needed, we get another polynomial $x^4 + a\,x^2 + b\,x - a^2/12$ which defines the same extension K_1, has 2-adic integer coefficients, and $v_2(a) \leq 2$ or $v_2(b) \leq 2$. By the lemma, we must have $v_2(a) = 2$, $v_2(b) = 5$, and $a/4 \equiv 1 \pmod 4$.

The Weierstrass equation $y^2 = x^3 + a/2\,x + b/4$ is either a model for E or $E_{(2)}$, and $y^2 = x^3 + 2\,a\,x + 2\,b$ for the other. Performing Tate's algorithm it is easy to check that they are 2-minimal models, the first case corresponding to Kodaira type III and the second to III^*. From the first equation, one computes $c_4 = -24\,a$ and $c_6 = -216\,b$. Hence, we also deduce $v_2(j) = 6$ and the congruences in the statement.

Remark 1. *By using Ogg's formula and Tate's algorithm, in* [D-K] *it is proved that if $\rho_{E,2}$ is trivial, then $\rho = \rho_{E,3}$ satisfies W3, the most difficult case being $q = 2$. By combining Proposition 1 and Lemma 1 above, one obtains an elementary Galois-theoretic proof of that result in the surjective case.*

Remark 2. *Under the hypothesis of Lemma 1, but for an odd prime q, the results of Montes give $q = \mathfrak{q}^2\mathfrak{q}'^2$ in K_1 if and only if $v_q(a) = 1$, $v_q(b) \geq 2$ and $\left(\frac{3}{q}\right) = 1$.*

Finally, let us be concerned with condition W1. To this end, we are still denoting by E an elliptic curve over $\mathbf{Q}$ providing a lifting of $\bar{\rho}$. Let $\{E_{i,t}\}$ be the double family of elliptic curves associated with $\bar{\rho}$ as in section 2.

Proposition 3. *There exists at least one $t_0 \in \mathbf{P}^1(\mathbf{Q})$ such that E_{1,t_0} has good or multiplicative reduction at 3.*

The proof is done case-by-case. Since the elliptic curves under consideration are defined up to twist, we can (and do) change $E = E_{1,\infty}$ by its twist by $\mathbf{Q}(\sqrt{-3})$ in order to have a model $y^2 = x^3 + A\,x + B$ with $v_3(A) \leq 1$ or $v_3(B) \leq 2$. Then, by performing Tate's algorithm over the elliptic curves $E_{1,t}$ we check that the values of t given in the following table lead to a curve having a twist semistable at 3:

condition	t	3-Kodaira($E_{1,t}$)
$v_3(A) = 0$	∞	I_0
$v_3(A) = 1$, $v_3(B) \geq 1$	0	I_0^*
$v_3(A) = 1$, $v_3(B) = 0$, $A/3 \equiv 1 \pmod 3$	0	I_0^*
$v_3(A) = 1$, $v_3(B) = 0$, $A/3 \equiv -1 \pmod 3$	0	I_ν^*

condition	t	3-Kodaira$(E_{1,t})$
$v_3(A) \geq 2$, $v_3(B) = 0$	0	I_ν^*
$v_3(A) \geq 2$, $v_3(B) = 1$	0	I_ν
$v_3(A) = 2$, $v_3(B) = 2$, $B/9 \equiv 1 \pmod 3$	3	I_0^*, I_ν^*
$v_3(A) = 2$, $v_3(B) = 2$, $B/9 \equiv -1 \pmod 3$	-3	I_0^*, I_ν^*
$v_3(A) \geq 3$, $v_3(B) = 2$	0	I_ν^*

Alternatively, we can use the following algorithm to find an elliptic curve E_s in the family $\{E_{1,t}\}$ having a twist semistable at 3. Start with $E_s = E$. If E_s does not satisfy the property, then compute $E_{1,0}$ (using E_s as the defining point $E_{1,\infty}$) and reset $E_s = E_{1,0}$. If we repeat this process, after at most two steps we will get the desired elliptic curve. In this way we can restrict ourselves to the values $t = \infty$ and $t = 0$.

Remark 3. *A standard argument which involves Krasner's lemma enables one to show the existence of infinitely many values of t satisfying the claim in the proposition above, just by taking values of t 3-adically close enough to t_0.*

While this paper was in preparation, the authors learned from Diamond that hypothesis W3 in [W, Theorem 0.3] can be removed. Extending Wiles' arguments, Diamond shows that every elliptic curve either semistable at 3 and 5 or semistable at 3 with $[\mathbf{Q}(E[3]) : \mathbf{Q}] \geq 16$ is modular. Therefore, putting together the proposition above and [D, Theorem 5.4] we get the proof of the theorem stated in the introduction.

4. Minimality and ellipticity

In this section, we discuss some facts concerning the minimality of deformations of $\bar\rho$ in the sense of Ash-Stevens, Gross, Ribet, Wiles and others.

We start with a surjective representation $\bar\rho$ having linear liftings ρ with cyclotomic determinant:

$$\begin{array}{ccc} & & \mathrm{GL}_2(\mathbf{F}_3) \\ & \overset{\rho}{\nearrow} & \downarrow \\ \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) & \xrightarrow[\bar\rho]{} & \mathrm{PGL}_2(\mathbf{F}_3). \end{array}$$

To each lifting ρ one attaches three invariants: the level $N(\rho)$, the weight $k(\rho)$, and the character $\epsilon(\rho)$, by means of a general recipe given by Serre in [S]. We refer to the paper of Serre for the precise definition and recall here some facts concerning our situation.

- Level: For any prime $l \neq 3$ and $i \geq 0$, let G_i be the ramification groups of ρ at l and

$$n(l) = \sum_{i=0}^{\infty} \frac{g_i}{g_0} \operatorname{codim} V^{G_i},$$

where $g_i = \#G_i$ and V is the space of the representation ρ. Then the level is defined as the conductor

$$N(\rho) = \prod_{l \neq 3} l^{\,n(l)}.$$

In our case, we have always tame ramification at primes $l \neq 2, 3$.

- Weight and character : Since the determinant of ρ is the cyclotomic character $\chi : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathbf{F}_3^*$, from the formula

$$\det \rho = \epsilon(\rho)\, \chi^{k(\rho)-1}$$

we obtain that the character is trivial and the weight is even.

To the whole family of liftings we can also attach two invariants. Let $N(\bar{\rho})$ be the minimum among the conductors $N(\rho)$ when ρ ranges over all liftings of $\bar{\rho}$ into $\mathrm{GL}_2(\mathbf{F}_3)$, and $k(\bar{\rho})$ the minimum among the weights. Both of them are explicitly computable in terms of a quartic polynomial defining $\bar{\rho}$ as it is shown in [R]. If the minimal weight is $k(\bar{\rho}) = 2$ we will say that $\bar{\rho}$ is flat, otherwise we have $k(\bar{\rho}) = 4$.

Let us now fix a lifting ρ having $N(\rho) = N(\bar{\rho})$ and $k(\rho) = k(\bar{\rho})$. Using again the theorem of Langlands and Tunnell, on one hand we have that ρ is modular. On the other hand, ρ is not induced from a character of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}(\sqrt{-3}))$. Then, Diamond asserts in [D2, Corollary 1] that it satisfies Serre's arrangement of type as predicted by conjecture $(3.2.4_?)$ in [S]. Therefore, associated with ρ, there is a classical cusp form f of weight 2 for the modular group $\Gamma_0(N(\bar{\rho}))$ or $\Gamma_0(3N(\bar{\rho}))$, according to whether $\bar{\rho}$ is flat or not, with the following properties:

- f is an eigenvector for the Hecke operators T_ℓ and U_q,
- the representation $\rho_{f,\mathfrak{p}} : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathrm{GL}_2(\mathcal{O}_\mathfrak{p})$ is a deformation of the residual representation ρ.

Here $\rho_{f,\mathfrak{p}}$ denotes the Galois representation which corresponds to the pair $(f, \mathfrak{p})$, where $\mathfrak{p} \mid 3$ is a prime ideal in the ring of integers $\mathcal{O}$ of the number field generated by the Hecke eigenvalues of f. The existence of this modular deformation can be read, for instance, in [G, Proposition 9.3]. It is worth noting that the weight 2 eigenform f producing a modular deformation of ρ is in general non unique.

At the same time, as we have mentioned before, the lifting ρ comes from the 3-torsion points of some elliptic curve (in fact, from infinitely many). Let E be one of these elliptic curves attached to ρ and denote by N_E its geometric conductor. By the results in [B-L], the possible differences between the conductors N_E and $N(\bar{\rho})$ are controlled. We have

$$v_\ell(N_E/N(\bar{\rho})) = \begin{cases} 1 & \text{if } \ell\text{-Kodaira}(E) = I_{3\nu},\ IV, \text{ or } IV^*\,, \\ 0 & \text{otherwise}\,, \end{cases}$$

where v_ℓ is the standard valuation at primes $\ell \neq 3$.

It would be interesting to relate the results in the previous sections with the above. Namely, we ask whether it is true that a modular elliptic deformation of $\bar{\rho}$ comes from an elliptic curve of conductor $N(\bar{\rho})$ or $3N(\bar{\rho})$, depending on the flatness property.

Numerical experiments seem to indicate that almost always this is true, but as the following example shows this can not be expected in general.

Consider the polynomial $f(x) = x^4 - 12\,x^2 - 21\,x - 12$ which has Galois group isomorphic to $\mathcal{S}_4$ and discriminant $-3^3 \cdot 71^2$. The splitting field of $f(x)$, say K, is of elliptic type in the sense of [L-R]. Therefore we can construct the representation $\bar{\rho} : \mathrm{Gal}(K/\mathbf{Q}) \to \mathrm{PGL}_2(\mathbf{F}_3)$ and consider all its elliptic liftings. The minimal level turns out to be $N(\bar{\rho}) = 71$ and the minimal weight $k(\bar{\rho}) = 2$. But no elliptic curve of conductor 71 exists (see [Br-K]). In this example, there are two newforms for $\Gamma_0(71)$:

$$\begin{aligned} f(q) &= q + \alpha\, q^2 + (3 - \alpha^2)q^3 + (-2 + \alpha^2)q^4 - (1 + \alpha)q^5 + \dots\,, \\ g(q) &= q + (3 - \alpha - \alpha^2)q^2 + (-3 + \alpha + \alpha^2)q^3 + (1 + \alpha)q^4 \\ &\quad + (5 - 2\alpha - \alpha^2)q^5 + \dots\,, \end{aligned}$$

where $\alpha^3 - 5\alpha + 3 = 0$, which yield the minimal deformations of $\bar{\rho}$ when one takes the prime ideal over 3 generated by α. They give rise to two abelian varieties of dimension 3 which are absolutely irreducible factors of the Jacobian variety $\mathbf{J}_0(71)$.

In order to find a "minimal" elliptic deformation of $\bar{\rho}$ one should take the elliptic curve of conductor $2 \cdot 71$ given by the Weierstrass equation $y^2 + xy = x^3 - x^2 - x - 3$, which has 2-Kodaira type I_6.

Nevertheless, in this particular example we can also find an elliptic curve with conductor a power of 3 times 71 which has the desired property. Namely, the elliptic curve $y^2 + y = x^3 - 6\,x + 5$ has conductor $3^3 \cdot 71$ and its projective Galois representation on the 3-torsion module is isomorphic to $\bar{\rho}$.

In general, one can expect the following statement to be true.

Conjecture 1. *Let $\bar{\rho} : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathrm{PGL}_2(\mathbf{F}_3)$ be an irreducible representation with cyclotomic determinant. Assume that $\bar{\rho}$ has linear liftings and let $N(\bar{\rho})$ be as above. Then, there is a linear lifting $\rho_{E,3}$ where $E/\mathbf{Q}$ is an elliptic curve having conductor a power of 3 times $N(\bar{\rho})$.*

Numerical evidence has been collected by computations over all the quartic fields of discriminant (in absolute value) up to 10^6 for which a Galois representation $\rho : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \twoheadrightarrow \mathrm{GL}_2(\mathbf{F}_3)$ with cyclotomic determinant can be constructed. The following table is the beginning of this list of examples. The first two columns display the discriminant and a polynomial for the corresponding quartic field. The third and fourth columns contain the minimal weight and the minimal level, respectively, and the last shows an elliptic curve as predicted by the conjecture.

$-d_{K_1}$	$f(x)$	$k(\bar{\rho})$	$N(\bar{\rho})$	$E/\mathbf{Q}$
3267	$-243 - 40\,x - 54\,x^2 + x^4$	2	11	$11A$
3888	$6 - 2\,x - 6\,x^2 + x^4$	4	8	$24A$
6075	$-3 + 248\,x - 6\,x^2 + x^4$	4	5	$15A$
6912	$3 - 4\,x - 6\,x^2 + x^4$	2	128	$128A$
7803	$-3 - 264\,x - 6\,x^2 + x^4$	2	17	$17A$
10800	$-3 - 72\,x - 6\,x^2 + x^4$	2	40	$40A$
10800	$-51 - 40\,x - 6\,x^2 + x^4$	2	200	$200B$
11907	$-3 - x - 6\,x^2 + x^4$	4	7	$21A$
15552	$-3 - 40\,x - 6\,x^2 + x^4$	4	32	$96A$
15552	$81 - 48\,x - 18\,x^2 + x^4$	4	256	$768B$
18252	$-867 - 456\,x - 102\,x^2 + x^4$	2	26	$26B$
21168	$18 - 6\,x - 6\,x^2 + x^4$	2	56	$56B$
21168	$-3 - 6\,x - 6\,x^2 + x^4$	2	56	$56A$
23763	$-3 - 5\,x + 6\,x^2 + x^4$	2	89	$89A$
24300	$24 - 10\,x - 6\,x^2 + x^4$	4	50	$150A$
25392	$-131 - 24\,x + 10\,x^2 + x^4$	2	184	$184A$
33075	$-2691 + 120\,x - 6\,x^2 + x^4$	2	175	$175A$
36963	$-147 - 360\,x + 42\,x^2 + x^4$	2	37	$37A$
38988	$-27 + 56\,x + 18\,x^2 + x^4$	2	38	$38B$
41067	$-3 - 5\,x - 6\,x^2 + x^4$	4	13	$39A$
41772	$-243 + 728\,x - 54\,x^2 + x^4$	2	118	$118B$
43200	$-183 - 64\,x + 6\,x^2 + x^4$	2	1280	$3840N$
43200	$237 - 104\,x - 54\,x^2 + x^4$	2	160	$160A$
46128	$157 + 120\,x + 10\,x^2 + x^4$	2	248	$248A$
47628	$6189 - 104\,x - 150\,x^2 + x^4$	4	14	$42A$
47628	$-12 - 14\,x - 6\,x^2 + x^4$	4	98	$294F$

$-d_{K_1}$	$f(x)$	$k(\bar{\rho})$	$N(\bar{\rho})$	$E/\mathbf{Q}$
49923	$-243+472\,x-54\,x^2+x^4$	2	43	$43A$
52272	$-171-88\,x-30\,x^2+x^4$	2	968	$968A$
52272	$-75-72\,x-30\,x^2+x^4$	2	88	$88A$
55488	$141-24\,x-22\,x^2+x^4$	2	544	$544B$
57132	$-147+408\,x+42\,x^2+x^4$	2	46	$46A$
59643	$-867-712\,x-102\,x^2+x^4$	2	47	$141B$
62208	$15-4\,x-6\,x^2+x^4$	4	128	$384A$
62208	$6-4\,x-6\,x^2+x^4$	4	256	$768A$
70227	$-3459-136\,x-6\,x^2+x^4$	4	289	$867B$
72075	$4317+312\,x-166\,x^2+x^4$	2	155	$155A$
73008	$-27+40\,x+18\,x^2+x^4$	2	104	$104A$
74892	$-27+136\,x+18\,x^2+x^4$	2	158	$158B$
75843	$-867+312\,x-102\,x^2+x^4$	2	53	$53A$
81675	$-3-3\,x-6\,x^2+x^4$	2	55	$55A$
84672	$-147+56\,x+42\,x^2+x^4$	2	224	$224A$
84672	$-24-8\,x-6\,x^2+x^4$	2	1792	$1792A$

From these computations we have that the most common situation is to find an elliptic curve with conductor $N(\bar{\rho})$ whenever $k(\bar{\rho})=2$ and $3N(\bar{\rho})$ when $k(\bar{\rho})=4$.

However, the computations also provide examples of the situation where the minimal level newforms do not have rational coefficients. We list some of them here:

$-d_{K_1}$	$f(x)$	$k(\bar{\rho})$	$N(\bar{\rho})$	$E/\mathbf{Q}$	N_E
59643	$-867-712\,x-102\,x^2+x^4$	2	47	$141B$	$3\cdot 47$
136107	$-12-21\,x-12\,x^2+x^4$	2	71	$1917A$	$3^3\cdot 71$
147852	$-243-808\,x-54\,x^2+x^4$	2	74	$222C$	$3\cdot 74$
344763	$-147+664\,x+42\,x^2+x^4$	2	113	$339C$	$3\cdot 113$
344763	$-12-25\,x-12\,x^2+x^4$	2	113	$339A$	$3\cdot 113$
401868	$-1875+24\,x-150\,x^2+x^4$	2	122	$3294F$	$3^3\cdot 122$
435483	$-48-63\,x-24\,x^2+x^4$	2	127	$1143A$	$3^2\cdot 127$
477603	$1233+160\,x-66\,x^2+x^4$	2	133	$399B$	$3\cdot 133$
484812	$-867-3016\,x-102\,x^2+x^4$	2	134	$402C$	$3\cdot 134$
615627	$-12-19\,x-12\,x^2+x^4$	2	151	$4077A$	$3^3\cdot 151$
674028	$-147-1128\,x+42\,x^2+x^4$	2	158	$4266V$	$3^3\cdot 158$
984987	$-147-872\,x+42\,x^2+x^4$	2	191	$573C$	$3\cdot 191$
1755675	$-48+89\,x-24\,x^2+x^4$	4	85	$2295J$	$3^3\cdot 85$
4560867	$-48+73\,x-24\,x^2+x^4$	4	137	$3699A$	$3^3\cdot 137$

Finally, some cases that surpass the tables of Cremona are shown in the following table. The corresponding elliptic curves have Weierstrass equation

$$y^2 + y = x^3 + a_4 x + a_6$$

and we give the coefficients $[a_4, a_6]$.

$-d_{K_1}$	$f(x)$	$k(\bar{\rho})$	$N(\bar{\rho})$	$E/\mathbf{Q}$	N_E
599427	$-3267 + 2680\,x - 198\,x^2 + x^4$	2	149	$[-18, -25]$	$3^4 \cdot 149$
604803	$-12 - 31\,x - 12\,x^2 + x^4$	2	449	$[-6, -8]$	$3^3 \cdot 449$
711507	$-12 - 5\,x - 12\,x^2 + x^4$	2	487	$[-6, 1]$	$3^3 \cdot 487$
924075	$16269 - 360\,x - 246\,x^2 + x^4$	2	925	$[-120, 506]$	$3^2 \cdot 925$

Acknowledgement

The authors wish to thank the referee for a careful reading and many valuable comments to an earlier version of the manuscript. And also thank Pilar Bayer for her continuous encouragement and interest on this subject.

References

[B-L] P. Bayer and J. C. Lario, *On Galois representations attached to the p-torsion points of elliptic curves,* Compositio Math. **84** (1992), 71–84.

[Br-K] A. Brumer and K. Kramer, *The rank of elliptic curves,* Duke Math. J. **44** (1977), 715–743.

[C] S. Comalada, *Twists and reduction of an elliptic curve,* J. of Number Theory **49** (1994), 45–62.

[Cr] J. E. Cremona, *Algorithms for Modular Elliptic Curves,* Cambridge University Press, 1992.

[D] F. Diamond, *On deformation rings and Hecke rings,* Ann. of Math., to appear.

[D2] _____, *The refined conjecture of Serre,* Elliptic curves, modular forms & Fermat's Last Theorem (eds. J. Coates and S-T. Yau), Series in Number Theory I, International Press, 1995.

[D-K] F. Diamond and K. Kramer, *Modularity of a family of elliptic curves,* Math. Res. Lett. **2** (1995), 299–304.

[G] B. H. Gross, *A tameness criterion for Galois representations associated to modular forms (mod p),* Duke Math. J. **61** (1990), 445–517.

[La] R. Langlands, *Base Change for* GL(2), Ann. of Math. Studies **96**, Princeton University Press, 1980.

[L-R] J. C. Lario and A. Rio, *An octahedral-elliptic type equality in $Br_2(k)$,* C.R. Acad. Sci. Paris **321** (1995), 39–44.

[M] J. Montes, *Private communication on 16th July, 1995.*

[N] A. Néron, *Modèles minimaux des variétés abéliennes sur les corps locaux et globaux,* Publ. Math. Inst. Htes Ét. scientifiques **21** (1964).

[R] A. Rio, *Representacions de Galois octaèdriques,* Tesi doctoral, Universitat de Barcelona, 1995.

[Ru-Si] K. Rubin and A. Silverberg, *Families of elliptic curves with constant mod p representations,* Elliptic curves, modular forms & Fermat's Last Theorem (eds. J. Coates and S-T. Yau), Series in Number Theory I, International Press, 1995.

[S] J.-P. Serre, *Sur les représentations modulaires de degré 2 de* $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$*,* Duke. Math. J. **54** (1987), 179–230.

[SB-T] N. I. Shepherd-Barron and R. Taylor, *Mod 2 and mod 5 icosahedral representations,* preprint.

[T-W] R. Taylor and A. Wiles, *Ring-theoretic properties of certain Hecke algebras,* Ann. of Math. **141** (1995), 553–572.

[Tu] J. Tunnell, *Artin's conjecture for representations of octahedral type,* Bull. Amer. Math. Soc. **5** (1981), 173–175.

[W] A. Wiles, *Modular elliptic curves and Fermat's Last Theorem,* Ann. of Math. **141** (1995), 443–551.

Departament de Matemàtica Aplicada II, Universitat Politècnica de Catalunya, Barcelona, E–08028

E-mail address: lario@grec.upc.es, rio@grec.upc.es