Mod 6 representations of elliptic curves

K. Rubin and A. Silverberg

Dedicated to Goro Shimura

Abstract. We study the elliptic curves over $\mathbf{Q}$ whose mod 6 representations are symplectically isomorphic to that of a given one E. We show that if the j-invariant of E is not 0, 1728, $4\cdot 1728$, or $-8\cdot 1728$, then there are infinitely many such curves. When $j(E)$ is $4 \cdot 1728$ or $-8 \cdot 1728$, then there are only finitely many. When $j(E)$ is 0 or 1728, then for infinitely many E's the number is finite, and for infinitely many E's the number is infinite.

Introduction

Suppose E is an elliptic curve, N is a positive integer, and $E[N]$ is the kernel of multiplication by N on E. Let $X_{E,N}$ denote the moduli space parametrizing pairs (E', ψ) where E' is an elliptic curve and ψ is an isomorphism between $E[N]$ and $E'[N]$ which is compatible with the Weil pairings. If $N < 6$ then $X_{E,N}$ has genus 0 (and therefore has infinitely many rational points), and if $N > 6$ then $X_{E,N}$ has genus greater than one (and therefore has only finitely many rational points). See (1.6.4) of [**9**] for a formula for the genus.

If $N = 6$, then $X_{E,N}$ has genus one. In "A question" on p. 133 of [**6**], Mazur states that it might be interesting to consider in some detail the problem of determining all elliptic curves over $\mathbf{Q}$ whose mod 6 representation is symplectically isomorphic to that of a given one. This case is more difficult than the cases $N = 3$, 4, or 5 (see [**8**] and [**10**]), since the moduli spaces are no longer of genus 0.

In Theorem 3.1 we show that if E is an elliptic curve over $\mathbf{Q}$ with discriminant D, then $X_{E,6}$ is the elliptic curve $y^2 = x^3 + D$. In the case where $E[6] \cong \mathbf{Z}/6\mathbf{Z} \times \boldsymbol{\mu}_6$, we give a model for the resulting fiber system of elliptic curves (see Theorem 2.1).

In §4 we consider the elliptic curves over $\mathbf{Q}$ whose mod 6 representation is symplectically isomorphic to that of a given one E. We show that if $j(E)$ is not 0, 1728, $4 \cdot 1728$, or $-8 \cdot 1728$, then there are infinitely many such curves. When $j(E)$ is $4 \cdot 1728$ or $-8 \cdot 1728$, then the number is 1 or 2, respectively. When $j(E)$ is 0 or 1728, then for infinitely many E's the number is finite, and for infinitely many E's the number is infinite.

1991 *Mathematics Subject Classification.* Primary: 11G05; Secondary: 11G18, 11F33.
Key words and phrases. elliptic curves, Galois representations, modular curves.
Partially supported by NSF Grant #DMS-9306287 and NSA Grant #MDA904-96-1-0054.

The authors thank the NSF and NSA. The authors also thank the IHES, where this work was carried out.

1. Notation

We review some of the notation from [**8**] and [**10**]. See [**10**] and [**5**] for further details and additional background.

Let $\mathbf{Z}$, $\mathbf{Q}$, and $\mathbf{C}$ denote, respectively, the integers, rational numbers, and complex numbers. If $F \subseteq \bar{\mathbf{Q}}$ is a number field, let $G_F = \mathrm{Gal}(\bar{\mathbf{Q}}/F)$. If E is an elliptic curve, let $j(E)$ denote the j-invariant of E.

Denote by Y_N the (non-compact) modular curve over $\mathbf{Q}$ which parametrizes triples (E, P_N, C_N) where E is an elliptic curve, P_N is a point of exact order N on E, C_N is a cyclic subgroup of order N on E, and C_N and P_N generate $E[N]$. Let X_N denote the compactification of Y_N.

Let W_N denote the universal elliptic curve with level structure as above. Then W_N is a quasi-projective surface defined over $\mathbf{Q}$, with a projection morphism

$$\pi_N : W_N \to Y_N$$

and a zero-section $Y_N \to W_N$, both defined over $\mathbf{Q}$, such that π_N has N^2 sections defined over $\bar{\mathbf{Q}}$ of order dividing N, and such that the fibers of π_N correspond to the triples classified by Y_N.

Definition 1.1. If E and E' are elliptic curves over $\mathbf{Q}$, and $\psi : E[N] \to E'[N]$ is a $G_{\mathbf{Q}}$-equivariant isomorphism which is equivariant with respect to the pairings e_N on E and E', we call ψ a *symplectic isomorphism* and say that $E[N]$ and $E'[N]$ are *symplectically isomorphic*.

If E is an elliptic curve over $\mathbf{Q}$, it was shown in §2 of [**10**] how to obtain a twist

$$W_{E,N} \xrightarrow{\pi_{E,N}} Y_{E,N}$$

of $W_N \xrightarrow{\pi_N} Y_N$, all defined over $\mathbf{Q}$, with the following properties:

- the points of $Y_{E,N}$ correspond to isomorphism classes of pairs (E', ψ) where E' is an elliptic curve and $\psi : E[N] \to E'[N]$ is an isomorphism which respects the Weil pairings,
- the fiber over a point of $Y_{E,N}$ corresponding to (E', ψ) is E'.

If $t \in Y_{E,N}(\mathbf{C})$ and $\mathcal{E}_t$ is the fiber over t in $W_{E,N}$, then $\mathcal{E}_t[N]$ and $E[N]$ are isomorphic as $\mathrm{Gal}(\overline{\mathbf{Q}(t)}/\mathbf{Q}(t))$-modules. In particular, we can view points of $Y_{E,N}(\mathbf{Q})$ as corresponding to $\mathbf{Q}$-isomorphism classes of pairs (E', ψ) where E' is an elliptic curve over $\mathbf{Q}$ and $\psi : E[N] \to E'[N]$ is a symplectic isomorphism.

From now on we will take $N = 6$, and will write Y_E and W_E for $Y_{E,6}$ and $W_{E,6}$, respectively. Let X_E denote the compactification of Y_E.

2. Modular curve and elliptic modular surface of level 6

We give a model for the elliptic modular surface W_6. We can view W_6 as a surface over $\mathbf{Q}$ or as an elliptic curve $\mathcal{E}_t$ over the function field of X_6.

Theorem 2.1. *An affine model for X_6 is*

$$s^2 = t^3 + 1.$$

We have $Y_6 = X_6 - \mathcal{S}$, where $\mathcal{S}$ consists of the point at infinity and the points on $s^2 = t^3 + 1$ satisfying $st(t^3 - 8) = 0$. A model for the fiber in W_6 over $(t, s) \in Y_6$ can be given by

$$\mathcal{E}_t : y^2 = x^3 + a(t)x + b(t)$$

where

$$a(t) = \frac{-(256 + 256t^3 + 960t^6 + 232t^9 + t^{12})}{3},$$

$$b(t) = \frac{2(4096 + 6144t^3 - 30720t^6 - 24640t^9 - 12072t^{12} - 516t^{15} + t^{18})}{27}.$$

The discriminant and j-invariant of $\mathcal{E}_t$ are

$$\Delta(\mathcal{E}_t) = 2^{12}t^6(-8 + t^3)^6(1 + t^3)^3 = (4st(-8 + t^3))^6,$$

$$j(\mathcal{E}_t) = \frac{(4 + t^3)^3(64 + 48t^3 + 228t^6 + t^9)^3}{t^6(-8 + t^3)^6(1 + t^3)^3}.$$

The points $P_1(t) = (2(8-20t^3-t^6)/3, 0)$ and $P_2(t, s) = ((-8-24s^3+20t^3+t^6)/3, 0)$ are points of order 2 on $\mathcal{E}_t$. The points

$$Q_1(t) = (\frac{(4 + 6t^2 + t^3)^2}{3}, 4t^2(1 - t + t^2)(4 + 2t + t^2)^2)$$

and

$$Q_2(t) = (-(4 + t^3)^2, \frac{-4(1 + t^3)(-8 + t^3)^2}{3\sqrt{-3}})$$

are independent points of order 3 on $\mathcal{E}_t$.

Proof. Let X denote the elliptic curve defined by $s^2 = t^3 + 1$, let $\mathcal{S}$ denote the set consisting of the origin of X and the 11 points where $st(t^3 - 8) = 0$, and let Y denote $X - \mathcal{S}$. Note that $X(\mathbf{Q})$ is the cyclic group generated by the point $(2, 3)$, and $X(\mathbf{Q}) \subset \mathcal{S}$. For $(t, s) \in Y$, it is easy to check the formulas for $\Delta(\mathcal{E}_t)$ and $j(\mathcal{E}_t)$, and to check that the points $P_1(t)$, $P_2(t, s)$, $Q_1(t)$, and $Q_2(t)$ are points on $\mathcal{E}_t$ of the given orders. The function field $\mathbf{Q}(X) = \mathbf{Q}(t, s)$ has degree 2 over $\mathbf{Q}(t)$. For $(t, s) \in Y$, the triple

$$(\mathcal{E}_t, P_1(t) + Q_1(t), \langle P_2(t, s) + Q_2(t)\rangle)$$

defines a point in Y_6. We therefore obtain a morphism $f : X \to X_6$. Let $g : X_6 \to \mathbf{P}^1$ be the (degree 72) morphism induced by $(E, P, C) \mapsto j(E)$. By the formula for $j(\mathcal{E}_t)$, we see that the function field $\mathbf{Q}(t)$ has degree 36 over $\mathbf{Q}(j(\mathcal{E}_t))$. Therefore, $\mathbf{Q}(X)$ has degree 72 over $\mathbf{Q}(\mathbf{P}^1)$, and the morphism $g \circ f$ has degree 72. Thus, f is an isomorphism.

That $\mathcal{E}_t$ is a model for W_6 now follows from the universal property of W_6. In the appendix we explain briefly how we obtained this model.

The 12 cusps of X_6 correspond to the 12 points with singular fibers, which are the points of $\mathcal{S}$. □

The model for X_6 is well-known. Fricke and Klein studied models for elliptic modular surfaces (see especially [**4**]).

3. Twists of X_6

THEOREM 3.1. *Suppose $E: y^2 = x^3 + ax + b$ is an elliptic curve, with $a, b \in \mathbf{Q}$. Then a model for the modular curve X_E is given by*

$$s^2 = t^3 + D,$$

where $D = -16(4a^3 + 27b^2)$ is the discriminant of E.

PROOF. Since X_E has a rational point (corresponding to E), and is isomorphic over $\mathbf{C}$ to $y^2 = x^3 + 1$, we know X_E has a model of the form $y^2 = x^3 + \delta$, with $\delta \in \mathbf{Q}$ unique up to sixth powers, where the origin $\mathcal{O}$ corresponds to the pair $(E, \text{identity})$. For $(t, s) \in X_6$, let $\mathcal{E}_t$ denote the fiber of W_6 over (t, s), as in Theorem 2.1. There exists a $\mathbf{C}$-isomorphism $X_E \to X_6$, which sends $\mathcal{O}$ to a point (t_0, s_0) such that $\mathcal{E}_{t_0}$ is $\mathbf{C}$-isomorphic to E, i.e., $j(\mathcal{E}_{t_0}) = j(E)$. Such a map must be of the form

$$(t, s) \mapsto (t', s') = (t\alpha^{-2}, s\alpha^{-3}) + (t_0, s_0),$$

where the addition on the right side is addition on the elliptic curve $X_6 : y^2 = x^3 + 1$ and where $\alpha^6 = \delta$. Let $v = t/s$ and $w = 1/s$. Then v has a simple zero at $\mathcal{O}$ and w has a triple zero at $\mathcal{O}$. Since X_E is defined over $\mathbf{Q}$, we have $j(\mathcal{E}_{t'}) \in \mathbf{Q}(v, w)$.

First, suppose both a and b are non-zero. Using that $w \in v^3 + v^9\mathbf{Q}[[v]]$, one can expand $j(\mathcal{E}_{t'})$ as a power series in v, and see that when $ab \neq 0$, the coefficient of v is

$$\frac{27j(E)\alpha b(t_0)}{s_0 t_0(-8 + t_0^3)a(t_0)},$$

where $a(t)$ and $b(t)$ are as in Theorem 2.1. (The authors used Mathematica and Pari to do this.) From the formula for $\Delta(\mathcal{E}_{t_0})$ in Theorem 2.1, and the relation

$$\frac{D}{\Delta(\mathcal{E}_{t_0})} = \left(\frac{a(t_0)b}{b(t_0)a}\right)^6,$$

we see that α^6/D is the sixth power of a rational number. We can therefore take $\delta = D$.

Now remove the restriction that a and b are non-zero. If we write

$$\mathcal{F}_{t,s} : y^2 = x^3 + a_1(t, s)x + b_1(t, s)$$

for the fiber in W_E above the point $(t, s) \in X_E$, then $\mathcal{F}_{t,s}$ is $\mathbf{C}$-isomorphic to $\mathcal{E}_{t'}$, so there exists a function $\mu(t, s) \in \mathbf{C}(t, s)$ such that

$$a_1(t, s)\mu(t, s)^2 = a(t') \text{ and } b_1(t, s)\mu(t, s)^3 = b(t').$$

Changing variables as above, we can write $a_1(t, s)$ and $b_1(t, s)$ as power series $a_1(v), b_1(v) \in \mathbf{Q}[[v]]$, and we can write $\mu(t, s)$, $a(t')$, and $b(t')$ as power series $\mu(v), A(v), B(v) \in \mathbf{C}[[v]]$.

Now suppose $a = 0$, so $j(E) = 0$. Letting $t_0 = (-4)^{1/3}$, then $j(\mathcal{E}_{t_0}) = 0$ and we can let $s_0 = \sqrt{-3}$. Using these values for t_0 and s_0, a computation shows that

$$a_1'(0) = \mu(0)^{-2}A'(0) = 36b^{2/3}\alpha/(\sqrt{-3}(-4)^{1/3}).$$

Since $a_1'(0) \in \mathbf{Q}$, we see that, up to the sixth power of a rational number, we have

$$\delta = \alpha^6 = -2^4 3^3 b^2 = D.$$

Now suppose $b = 0$, so $j(E) = 1728$. Letting $t_0 = -1 + \sqrt{3}$, then $j(\mathcal{E}_{t_0}) = 1728$ and we can let $s_0 = \sqrt{-9 + 6\sqrt{3}}$. Using these values for t_0 and s_0, a computation shows that

$$b_1'(0) = \mu(0)^{-3} B'(0) = 4a\sqrt{-a}\alpha.$$

Since $b_1'(0) \in \mathbf{Q}$, up to a sixth power of a rational number we have

$$\delta = \alpha^6 = -2^6 a^3 = D.$$

□

4. Elliptic curves with symplectically isomorphic mod 6 representations

If E is an elliptic curve over $\mathbf{Q}$, let

$$S(E) = \{E' : (E', \psi) \in Y_E(\mathbf{Q}) \text{ for some } \psi\},$$

i.e., $S(E)$ is the set of all elliptic curves E' over $\mathbf{Q}$ (up to isomorphism over $\mathbf{Q}$) such that $E[6]$ and $E'[6]$ are symplectically isomorphic. Note that $S(E)$ is infinite if and only if $X_E(\mathbf{Q})$ is infinite.

THEOREM 4.1. *Suppose E is an elliptic curve over $\mathbf{Q}$.*

(a) *If the j-invariant of E is not 0, 1728, $4 \cdot 1728$, or $-8 \cdot 1728$, then $S(E)$ is infinite.*
(b) *If $j(E) = 4 \cdot 1728$, then $S(E) = \{E\}$.*
(c) *If $j(E) = -8 \cdot 1728$, then $S(E) = \{E, E^{(-1)}\}$, where $E^{(-1)}$ is the twist of E by the quadratic character associated to the extension $\mathbf{Q}(i)/\mathbf{Q}$.*

PROOF. Let $y^2 = x^3 + ax + b$ be a model for E, with $a, b \in \mathbf{Q}$, and let $D = -16(4a^3 + 27b^2)$. Let X' denote the elliptic curve $-3s^2 = t^3 + D$. By Theorem 3.1, a model for X_E is $s^2 = t^3 + D$. The rational map

$$(t, s) \mapsto (\frac{t^3 + 4s^2}{t^2}, \frac{-s(3t^3 + 8s^2)}{t^3})$$

defines an isogeny f from X' onto X_E. Clearly, $(4a, 12b)$ is a point on $X'(\mathbf{Q})$. Its image under f is

$$P = (\frac{4(a^3 + 9b^2)}{a^2}, \frac{-36b(a^3 + 6b^2)}{a^3}) \in X_E(\mathbf{Q}).$$

Since X_E is of the form $s^2 = t^3 + D$, the torsion subgroup of $X_E(\mathbf{Q})$ has order dividing 6 (see for example Theorem V of [**1**]). If $j(E) \neq 0$, then $a \neq 0$, so $P \neq \mathcal{O}$.

If P has order 6 then $2P$ has order 3, and it follows that the first coordinate of $2P$ vanishes. However, the first coordinate of $2P$ has numerator

$$4(a^{12} + 18b^2a^9 + 108b^4a^6 + 324b^6a^3 + 729b^8),$$

which vanishes with rational a and b only when $a^3 = -9b^2$, i.e., when P has order 3.

If D is $-2^4 3^3$ (up to a sixth power), then one can show that $a = 0$ and $j(E) = 0$. Otherwise, the point P has order 3 exactly when its first coordinate vanishes, i.e., exactly when $j(E) = 4 \cdot 1728$. In this case, E is of the form $y^2 = x^3 - 9c^2x + 9c^3$ for some $c \in \mathbf{Q}^\times$. It follows from Theorem 3.1 that a model for X_E is $y^2 = x^3 + 16$. There are exactly 3 rational points on this curve (see [**1**]). We have

$$\mathrm{Gal}(\mathbf{Q}(E[2])/\mathbf{Q}) \cong \mathbf{Z}/3\mathbf{Z},$$

since the discriminant of $x^3-9c^2x+9c^3$ is $(3c)^6$, a square. It follows that there are 3 $G_{\mathbf{Q}}$-equivariant automorphisms of $E[2]$, and therefore 3 symplectic automorphisms φ_1, φ_2, and φ_3 of $E[6]$. The (E,φ_i)'s correspond to the 3 points of $X_E(\mathbf{Q})$. We therefore have (b).

The point P has order 2 exactly when its second coordinate vanishes, i.e., exactly when $j(E)=1728$ or $-8\cdot 1728$. Now suppose $j(E)=-8\cdot 1728$. Then E is of the form $y^2=x^3-6c^2x+6c^3$ for some $c\in\mathbf{Q}^\times$, and it follows from Theorem 3.1 that a model for X_E is $y^2=x^3-27$. There are exactly 2 rational points on this curve (see [**1**]). Theorem 4.1 of [**8**] gives an equation for the family $\mathcal{E}_t$ of elliptic curves over $\mathbf{Q}$ whose mod 3 representation is symplectically isomorphic to that of E. When $t=-1/3$, the elliptic curve $\mathcal{E}_t$ is isomorphic over $\mathbf{Q}$ to

$$E^{(-1)}: y^2=x^3-6c^2x-6c^3,$$

the twist of E by -1 (i.e., the twist of E by the quadratic character associated to $\mathbf{Q}(i)/\mathbf{Q}$). Thus, $E[3]$ is symplectically isomorphic to $E^{(-1)}[3]$. For every elliptic curve over $\mathbf{Q}$, its mod 2 representation is symplectically isomorphic to that of any quadratic twist. Therefore, $E^{(-1)}\in S(E)$. Since E and $E^{(-1)}$ are not isomorphic over $\mathbf{Q}$, they correspond to the 2 points of $X_E(\mathbf{Q})$. We therefore have (c).

We can now conclude that if $j(E)$ is not 0, 1728, $4\cdot 1728$, or $-8\cdot 1728$, then P is a point of $X_E(\mathbf{Q})$ of infinite order, giving (a). □

Next, we consider the cases where $j(E)$ is 1728 or 0.

THEOREM 4.2. *For fourth-power-free integers a, let E_a denote the elliptic curve $y^2=x^3+ax$. Then for infinitely many a, $S(E_a)$ is infinite, and for infinitely many a, $S(E_a)$ is finite. If $S(E_a)$ is finite, then $S(E_a)=\{E_a\}$.*

PROOF. By Theorem 3.1, X_{E_a} is isomorphic to $y^2=x^3-a^3$. As shown in [**3**], if a is a prime congruent to 3 (mod 4) then $X_{E_a}(\mathbf{Q})$ has rank one, and if a is a prime congruent to 5 (mod 12) then $X_{E_a}(\mathbf{Q})$ has rank zero. For further results on $X_{E_a}(\mathbf{Q})$, see [**3**].

Suppose that $X_{E_a}(\mathbf{Q})$ is finite. If $-a$ is not a square (in $\mathbf{Q}$), then

$$\mathrm{Gal}(\mathbf{Q}(E_a[2])/\mathbf{Q})\cong\mathbf{Z}/2\mathbf{Z},$$

and there are 2 $G_{\mathbf{Q}}$-equivariant automorphisms of $E_a[2]$, which give rise to the 2 points of $X_{E_a}(\mathbf{Q})$. If $-a$ is a square, then $E_a[2]\subset E_a(\mathbf{Q})$, and there are 6 $G_{\mathbf{Q}}$-equivariant automorphisms of $E_a[2]$, which give rise to the 6 points of $X_{E_a}(\mathbf{Q})$. □

THEOREM 4.3. *For sixth-power-free integers b, let E_b denote the elliptic curve $y^2=x^3+b$. Then for infinitely many b, $S(E_b)$ is infinite, and for infinitely many b, $S(E_b)$ is finite. If $S(E_b)$ is finite, then $S(E_b)=\{E_b,E_b^{(-3)}\}$, where $E_b^{(-3)}$ is the twist of E_b by the quadratic character associated to the extension $\mathbf{Q}(\sqrt{-3})/\mathbf{Q}$, if b is twice a cube, and $S(E_b)=\{E_b\}$ otherwise.*

PROOF. By Theorem 3.1, X_{E_b} is isomorphic to $y^2=x^3-2^43^3b^2$. The X_{E_b}'s are cubic twists of $X_0(27)$ (the Fermat cubic), and X_{E_b} is birationally isomorphic to $x^3+y^3=b$. Lucas and Sylvester (see Chap. XXI of [**2**]) showed that there are infinitely many cube-free integers b such that $X_{E_b}(\mathbf{Q})$ has rank zero.

That there are infinitely many b such that $X_{E_b}(\mathbf{Q})$ has rank at least 3 follows from [**11**], where information is given on the density of such b. Since it is easy to give a short elementary proof that $X_{E_b}(\mathbf{Q})$ is infinite for infinitely many cube-free integers b, we do so here. Define positive integers x_n and b_n recursively by

$$x_1 = 2, \quad b_n = x_n^3 + 1, \quad x_{n+1} = \prod_{i=1}^{n} b_i.$$

Then the cube-free parts of the b_n's are pairwise relatively prime. For every n, the point $(x_n, 1)$ is a point of infinite order on the elliptic curve $x^3 + y^3 = b_n$. In this way, one obtains infinitely many cube-free integers b such that $X_{E_b}(\mathbf{Q})$ is infinite. Note that a similar technique works to show the analogous result in Theorem 4.2.

Suppose that $X_{E_b}(\mathbf{Q})$ is finite. If b is neither a cube nor twice a cube, then $\#X_{E_b}(\mathbf{Q}) = 1$, so $S(E_b) = \{E_b\}$. If $b = 2c^3$ with $c \in \mathbf{Q}^\times$, then $E_b^{(-3)} : y^2 = x^3 - 27b$ occurs in the family $\mathcal{E}_t$ of elliptic curves whose mod 3 representations are symplectically isomorphic to that of E_b, given in Theorem 4.6 of [**8**], with $t = 12/c$. It follows that E_b and $E_b^{(-3)}$ give rise to the 2 points of $X_{E_b}(\mathbf{Q})$. Suppose b is a cube. Using the isomorphism $X_{E_b} \to X_6$ given in the proof of Theorem 3.1, one checks that 1 of the 3 rational points of X_{E_b} is a cusp. Since $\mathrm{Gal}(\mathbf{Q}(E_b[2])/\mathbf{Q}) \cong \mathbf{Z}/2\mathbf{Z}$, the other 2 rational points come from the 2 $G_{\mathbf{Q}}$-equivariant automorphisms of $E_b[2]$. □

Appendix

We now explain how we obtained the model for W_6 given in Theorem 2.1. A Weierstrass model for W_3 is given by

$$A(u) : y^2 = x^3 + a_0(u)x + b_0(u)$$

where

$$a_0(u) = -27u(8 + u^3), \qquad b_0(u) = -54(8 + 20u^3 - u^6)$$

(see (1) of [**8**]). The points

$$q_1(u) = (3(2+u)^2, 36(1 + u + u^2)), \quad q_2(u) = (-9u^2, 12\sqrt{-3}(1 - u^3))$$

have order 3 on $A(u)$. Consider the modular curve that parametrizes quadruples (E, P_2, P_3, C_3) where P_n is a point of order n and C_3 is a subgroup of order 3 not containing P_3. We will denote by $X_0(18)$ the compactification of this modular curve (it is, in fact, isomorphic to the curve usually denoted $X_0(18)$). The map

$$(E, P_2, P_3, C_3) \mapsto (E, P_3, C_3)$$

induces a degree 3 covering $X_0(18) \to X_3$. Therefore, $\mathbf{Q}(X_0(18)) = \mathbf{Q}(u, x)$ where $x^3 + a_0(u)x + b_0(u) = 0$. Let

$$u_0(t) = \frac{4 + t^3}{3t^2} \qquad \text{and} \qquad x_0(t) = \frac{-(16 + t^3)}{t} + 3u_0(t)^2.$$

Then

$$x_0(t)^3 + a_0(u_0(t))x_0(t) + b_0(u_0(t)) = 0,$$

and t is a parameter on $X_0(18)$, i.e., $\mathbf{Q}(X_0(18)) = \mathbf{Q}(t)$. (The functions $u_0(t)$ and $x_0(t)$ were solved for using Mathematica and Pari.) In terms of t, the discriminant Δ of $A(u_0(t))$ is

$$\Delta = \frac{2^{12}(-8 + t^3)^6(1 + t^3)^3}{t^{18}}.$$

Since all the sections of X_6 of order 2 are defined over $\mathbf{Q}$, Δ is a square in $\mathbf{Q}(X_6)$. Therefore, t^3+1 is a square in $\mathbf{Q}(X_6)$. Since the map

$$(E, P_6, C_6) \mapsto (E, 3P_6, 2P_6, 2C_6)$$

induces a degree 2 covering $X_6 \to X_0(18)$, it follows that $\mathbf{Q}(X_6) = \mathbf{Q}(t, s)$ where $s^2 = t^3 + 1$. With $a(t)$ and $b(t)$ as in the statement of Theorem 2.1, we have $a(t) = a_0(u_0(t))t^8$ and $b(t) = b_0(u_0(t))t^{12}$. The point $(x_0(t)t^4, 0) = P_1(t)$ is a point on $\mathcal{E}_t$ of order 2. The other points of order 2 can be solved for using the square root of the discriminant of $\mathcal{E}_t$. The points $q_1(u)$ and $q_2(u)$ on $A(u)$ induce (after multiplying the first coordinate by t^4 and the second by t^6) the points $Q_1(t)$ and $Q_2(t)$.

References

[1] J. W. S. Cassels, *The rational solutions of the diophantine equation* $Y^2 = X^3 - D$, Acta Math. **82** (1950), 244–273.

[2] L. Dickson, History of the theory of numbers II: Diophantine analysis, Chelsea Publishing Co., New York, 1966.

[3] G. Frey, *Der Rang der Lösungen von* $Y^2 = X^3 \pm p^3$ *über* $\mathbf{Q}$, Manuscripta Math. **48** (1984), 71–101.

[4] R. Fricke, Die Elliptischen Funktionen und ihre Anwendungen II, B. G. Teubner, Leipzig-Berlin, 1922; Johnson Reprint Corp., New York, 1972.

[5] A. Kraus, J. Oesterlé, *Sur une question de B. Mazur*, Math. Ann. **293** (1992), 259–275.

[6] B. Mazur, *Rational isogenies of prime degree*, Invent. Math. **44** (1978), 129–162.

[7] K. Rubin, A. Silverberg, *A report on Wiles' Cambridge lectures*, Bull. Amer. Math. Soc. (N. S.) **31**, no. 1 (1994), 15–38.

[8] K. Rubin, A. Silverberg, *Families of elliptic curves with constant mod p representations*, in Conference on Elliptic Curves and Modular Forms, Hong Kong, December 18–21, 1993, Intl. Press, Cambridge, Massachusetts, 1995, pp. 148–161.

[9] G. Shimura, Introduction to the arithmetic theory of automorphic functions, Princeton Univ. Press, Princeton, 1971.

[10] A. Silverberg, *Explicit families of elliptic curves with prescribed mod N representations*, to appear in the Proceedings of the Conference on Number Theory and Fermat's Last Theorem, eds. Gary Cornell, Joseph H. Silverman, Glenn Stevens, Springer-Verlag (1997).

[11] C. L. Stewart, J. Top, *On ranks of elliptic curves and power-free values of binary forms*, J. Amer. Math. Soc. **8** (1995), 943–973.

Note added in proof: Joseph Oesterlé has informed us that J-I. Papadopoulos proved Theorem 3.1 earlier, by different methods, in his thesis *Deux questions relatives à l'arithmétique des courbes elliptiques*, thèse de doctorat de l'Université Paris 6, 16 Juillet 1992.

Department of Mathematics, Ohio State University, 231 W. 18 Avenue, Columbus, Ohio 43210–1174, USA

E-mail address: rubin@math.ohio-state.edu

Department of Mathematics, Ohio State University, 231 W. 18 Avenue, Columbus, Ohio 43210–1174, USA

E-mail address: silver@math.ohio-state.edu