FAMILIES OF ELLIPTIC CURVES WITH CONSTANT MOD p REPRESENTATIONS

K. RUBIN AND A. SILVERBERG

Introduction

Suppose E is an elliptic curve over $\mathbf{Q}$ and p is 3 or 5. Then the collection of elliptic curves over $\mathbf{Q}$ having the same mod p representation as E forms an infinite family. In this paper we show how to construct these families explicitly. One reason for the interest in these families is the result announced by Wiles, that if E and E' are elliptic curves over $\mathbf{Q}$ with good reduction at an odd prime p and with the same mod p representation, and E has complex multiplication, then E' is modular.

The proofs of the results in §4 and §5 rely on symbolic computer computations, which were done using the programs Pari and Mathematica.

Note that all the results of this paper remain true with $\mathbf{Q}$ replaced by any number field.

The authors thank Tricia Pacelli and Glenn Stevens for asking a question which led us to simplify the polynomials in Theorems 4.1 and 5.1.

Notation. If N is a positive integer and E is an elliptic curve over a field k with algebraic closure $\bar{k}$, let $E[N]$ denote the kernel of multiplication by N on $E(\bar{k})$. Let $\mathfrak{H}$ denote the complex upper half plane,

$$\Gamma(N) = \{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbf{Z}) : \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \equiv \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right) \pmod{\mathrm{N}}\},$$

and $G_{\mathbf{Q}} = \mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$.

If E is an elliptic curve over $\mathbf{Q}$ and p is a prime, write

$$\rho_{E,p} : G_{\mathbf{Q}} \to \mathrm{Aut}(\mathrm{E[p]}) \cong \mathrm{GL}_2(\mathbf{F}_{\mathrm{p}})$$

for the (isomorphism class of the) mod p representation of E.

1. Modular curves

Suppose p is an odd rational prime. Denote by Y_p the (non-compact) modular curve over $\mathbf{Q}$ which parametrizes isomorphism classes of pairs (E, ϕ) where E is an elliptic curve and

$$\phi : \mathbf{Z}/p\mathbf{Z} \times \boldsymbol{\mu}_p \to E[p]$$

is an isomorphism with the property that

$$\langle \phi(a_1, \zeta_1), \phi(a_2, \zeta_2) \rangle = \zeta_2^{a_1}/\zeta_1^{a_2}$$

where $\langle\ ,\ \rangle$ denotes the Weil pairing on $E[p]$. Equivalently, Y_p parametrizes triples (E, P, C) where E is an elliptic curve, P is a point of exact order p on E, and C is a subgroup of order p on E, not containing P. (Given (E, P, C), define ϕ by $\phi(a, \zeta) = aP + Q$ for the unique $Q \in C$ such that $\langle P, Q \rangle = \zeta$.) Let $Y(N)$ denote the

The authors thank the NSF for financial support.

modular curve which parametrizes elliptic curves with full level N structure (see [5]). Fixing a p-th root of unity ζ, the map

$$(E, \phi) \mapsto (E, \phi(1,1), \phi(0,\zeta)),$$

induces an isomorphism (defined over $\mathbf{Q}(\zeta)$) from Y_p onto one connected component of $Y(p)$. Thus $Y_p(\mathbf{C})$ is isomorphic to $\mathfrak{H}/\Gamma(p)$. Let X_p and $X(N)$ denote the compactifications of Y_p and $Y(N)$, respectively. Then X_p has genus 0 when $p \leq 5$ and genus at least 3 when $p \geq 7$ (see p. 23 of [5]).

From now on we will identify $X(1)$ with $\mathbf{P}^1$ by the map which sends an elliptic curve E to its j-invariant $j(E)$. From the description over $\mathbf{C}$ we see that the forgetful morphism $X_p \to X(1)$ induced by $(E, \phi) \mapsto E$ has degree

$$\frac{1}{2}[\mathrm{SL}_2(\mathbf{Z}) : \Gamma(\mathrm{p})] = \frac{1}{2}\#(\mathrm{SL}_2(\mathbf{F}_\mathrm{p})) = \frac{\mathrm{p}^3 - \mathrm{p}}{2}.$$

Let W_p be a compactification of the elliptic surface associated to the universal elliptic curve over Y_p. Then W_p is a variety over $\mathbf{Q}$, and W_p is an elliptic surface over X_p equipped with a morphism $W_p \to X_p$ and a zero section $\iota_p : X_p \to W_p$, both defined over $\mathbf{Q}$, and $p^2 - 1$ additional sections of order p defined over $\bar{\mathbf{Q}}$. We will denote the $G_\mathbf{Q}$-module of these p^2 sections by $W_p[p]$. The definitions of X_p and W_p imply that $W_p[p]$ is isomorphic to $\mathbf{Z}/p\mathbf{Z} \times \boldsymbol{\mu}_p$ as a $G_\mathbf{Q}$-module. Note that W_p is not uniquely determined, because there is a choice of compactification, but the choice is not important for our purposes. See [4] for the arithmetic of elliptic modular surfaces.

1.1. **Level three.** Let A'_u denote the elliptic curve (the Hesse cubic)

$$X^3 + Y^3 + Z^3 = 3uXYZ$$

over $\mathbf{Q}(u)$, with origin $(0, 1, -1)$. This curve has a Weierstrass model

$$A_u : y^2 = x^3 - 27u(u^3 + 8)x + 54(u^6 - 20u^3 - 8) \tag{1}$$

so in particular

$$j(A'_u) = j(A_u) = 27\frac{u^3(u^3+8)^3}{(u^3-1)^3}. \tag{2}$$

Let $P_u = (-1, 1, 0) \in A'_u[3]$. If ζ is a primitive cube root of unity, then

$$C_u = \{(0, 1, -1), (0, \zeta, -1), (0, \zeta^2, -1)\}$$

is a $\mathrm{Gal}(\overline{\mathbf{Q}(\mathrm{u})}/\mathbf{Q}(\mathrm{u}))$-invariant subgroup of $A'_u[3]$. Thus the map

$$u \mapsto (A'_u, P_u, C_u)$$

induces a morphism $f : \mathbf{P}^1 \to X_3$ defined over $\mathbf{Q}$. To see that f is an isomorphism it suffices to observe that by (2), the degree of the composition $\mathbf{P}^1 \xrightarrow{f} X_3 \to X(1)$ is 12 which is the same as the degree of X_3 over $X(1)$. From now on we will identify X_3 with $\mathbf{P}^1$ using the isomorphism f. With this identification we can take W_3 to be given by (1).

1.2. **Level five.** Following Klein (see [1] and p. 130 of [2]), let B_u denote the elliptic curve

$$y^2 = x^3 - \frac{u^{20} - 228u^{15} + 494u^{10} + 228u^5 + 1}{48}x + \frac{u^{30} + 522u^{25} - 10005u^{20} - 10005u^{10} - 522u^5 + 1}{864} \quad (3)$$

over $\mathbf{Q}(u)$. The j-invariant of B_u is

$$j(B_u) = \frac{-(u^{20} - 228u^{15} + 494u^{10} + 228u^5 + 1)^3}{u^5(u^{10} + 11u^5 - 1)^5}. \quad (4)$$

Let

$$x_0(u) = \frac{u^{10} + 12u^8 - 12u^7 + 24u^6 + 30u^5 + 60u^4 + 36u^3 + 24u^2 + 12u + 1}{12},$$
$$y_0(u) = \frac{u^{13} + u^{12} + 4u^{11} + 5u^9 + 6u^8 + 21u^7 + 29u^6 + 25u^5 + 15u^4 + 9u^3 + 4u^2 + u}{2},$$

and let $Q_u = (x_0(u), y_0(u))$. One can verify that $Q_u \in B_u[5]$. Let ζ denote a primitive fifth root of unity. Since the equation defining B_u is invariant under $u \mapsto \zeta u$, we have $R_u = (x_0(\zeta u), y_0(\zeta u)) \in B_u[5]$ as well. Since $Q_u \in B_u(\mathbf{Q}(u))$ and $R_u \notin B_u(\mathbf{Q}(u))$, these are independent points of order 5. Further, one can verify that for $\sigma \in G_{\mathbf{Q}}$,

$$\sigma R_u = \epsilon(\sigma)R_u + (1 - \epsilon(\sigma))Q_u$$

where $\epsilon : G_{\mathbf{Q}} \to (\mathbf{Z}/5\mathbf{Z})^\times$ is the cyclotomic character. Thus the subgroup C_u of $B_u[5]$ generated by $Q_u - R_u$ is stable under $\mathrm{Gal}(\overline{\mathbf{Q}(\mathrm{u})}/\mathbf{Q}(\mathrm{u}))$. Therefore the map

$$u \mapsto (B_u, Q_u, C_u)$$

induces a morphism $g : \mathbf{P}^1 \to X_5$ defined over $\mathbf{Q}$. To see that g is an isomorphism it is enough to observe that by (4), the degree of the composition $\mathbf{P}^1 \xrightarrow{g} X_5 \to X(1)$ is 60 which is the same as the degree of X_5 over $X(1)$. From now on we will identify X_5 with $\mathbf{P}^1$ using this isomorphism. With this identification we can take W_5 to be given by (3).

2. Twists of modular curves

Proposition 2.1. *Suppose p is a prime and there are commutative diagrams*

$$\begin{array}{ccc} W_p & \xleftarrow{\psi} & W' \\ \downarrow & & \downarrow \\ X_p & \xleftarrow{\psi_0} & X' \\ & \searrow \quad \swarrow & \\ & X(1) & \end{array} \qquad \begin{array}{ccc} W_p & \xleftarrow{\psi} & W' \\ \iota_p \uparrow & & \uparrow \iota' \\ X_p & \xleftarrow{\psi_0} & X' \end{array} \quad (5)$$

where X' is a curve and W' is an elliptic surface over X' with zero-section ι', all defined over $\mathbf{Q}$, ψ and ψ_0 are isomorphisms defined over $\bar{\mathbf{Q}}$, the maps $W_p \to X_p \to X(1)$ are the natural ones (see §1), and the maps $W' \to X' \to X(1)$ are defined over $\mathbf{Q}$. Let $\mathcal{S} \subset X'(\bar{\mathbf{Q}})$ denote the inverse image under ψ_0 of the (finite) set of cusps of X_p. Then there is a $G_{\mathbf{Q}}$-module V such that for every point $t \in X'(\mathbf{C}) - \mathcal{S}$,

the fiber E_t of W' over t is an elliptic curve defined over $\mathbf{Q}(t)$ and $E_t[p] \cong V$ as $\mathrm{Gal}(\overline{\mathbf{Q}(\mathrm{t})}/\mathbf{Q}(\mathrm{t}))$-modules.

Proof. Let V be the group of p^2 sections from X' to W' of order dividing p,

$$V = \{\psi^{-1} \circ s \circ \psi_0 : s \in W_p[p]\}.$$

These sections are defined over $\bar{\mathbf{Q}}$, so V is a $G_{\mathbf{Q}}$-module and the map from V to $E_t[p]$ obtained by restricting the sections in V to t is a $\mathrm{Gal}(\overline{\mathbf{Q}(\mathrm{t})}/\mathbf{Q}(\mathrm{t}))$-isomorphism. □

Corollary 2.2. *With notation as in Proposition 2.1, if E_1, E_2 are the fibers of W' over $t_1, t_2 \in X'(\mathbf{Q}) - \mathcal{S}$, then $E_1[p] \cong E_2[p]$ as $G_{\mathbf{Q}}$-modules.*

Proof. Immediate from Proposition 2.1. □

Remark 2.3. Under the hypotheses of Proposition 2.1, the resulting module V is endowed with a pairing coming from the Weil pairing on $W_p[p]$, and X' is the moduli space for isomorphism classes of pairs (E, ϕ) where E is an elliptic curve and $\phi : V \xrightarrow{\sim} E[p]$ is an isomorphism which takes the pairing on V to the Weil pairing on $E[p]$.

Remark 2.4. Fix an odd prime p, let $V_0 = \mathbf{Z}/p\mathbf{Z} \times \boldsymbol{\mu}_p$, and let η_0 be the $G_{\mathbf{Q}}$-equivariant pairing on V_0

$$\eta_0((a_1, \zeta_1), (a_2, \zeta_2)) = \zeta_2^{a_1}/\zeta_1^{a_2}.$$

There are natural $G_{\mathbf{Q}}$-equivariant maps

$$\mathrm{Aut}(\mathrm{V}_0, \eta_0) \to \mathrm{Aut}(\mathrm{W_p}) \to \mathrm{Aut}(\mathrm{X_p}),$$

where $\mathrm{Aut}(\mathrm{V}_0, \eta_0)$ is the group of automorphisms of V_0 which preserve η_0. Suppose V is a two-dimensional $\mathbf{F}_p$-vector space with an action of $G_{\mathbf{Q}}$ and a non-degenerate skew-symmetic $\boldsymbol{\mu}_p$-valued $G_{\mathbf{Q}}$-equivariant pairing η. Let $\rho : G_{\mathbf{Q}} \to \mathrm{Aut}(\mathrm{V})$ and $\rho_0 : G_{\mathbf{Q}} \to \mathrm{Aut}(\mathrm{V}_0)$ denote the representations induced by the $G_{\mathbf{Q}}$-actions, and fix a group isomorphism $\varphi : V_0 \to V$ which takes the pairing η_0 to the pairing η. Then $\sigma \mapsto \varphi^{-1}\rho(\sigma)\varphi\rho_0(\sigma)^{-1}$ defines a cocycle on $G_{\mathbf{Q}}$ with values in $\mathrm{Aut}(\mathrm{V}_0, \eta_0)$, which induces cohomology classes in $H^1(G_{\mathbf{Q}}, \mathrm{Aut}(\mathrm{W_p}))$ and $H^1(G_{\mathbf{Q}}, \mathrm{Aut}(\mathrm{X_p}))$ that are independent of the choice of φ. The twists of W_p and X_p by these cohomology classes (see [3]) give the varieties W' and X' satisfying Proposition 2.1 for the given $G_{\mathbf{Q}}$-module V.

Suppose E is an elliptic curve defined over $\mathbf{Q}$. Our aim is to explicitly construct W', X', and corresponding morphisms satisfying the hypotheses of Proposition 2.1, so that E is a fiber of W' over some rational point of X'. Then, by Corollary 2.2, the points of $X'(\mathbf{Q}) - \mathcal{S}$ will correspond to elliptic curves E' over $\mathbf{Q}$ with $\rho_{E',p} \cong \rho_{E,p}$.

From now on suppose that $p = 3$ or 5, so that X_p has genus 0. Recall that we have identified both X_p and $X(1)$ with $\mathbf{P}^1$, and with these identifications the morphism from X_p to $X(1)$ is given by the rational function $\mathcal{J}(u) \in \mathbf{Q}(u)$ defined by

$$\mathcal{J}(u) = \begin{cases} j(A_u) & \text{if } p = 3, \\ j(B_u) & \text{if } p = 5 \end{cases}$$

(see (2) and (4)). Let $X' = \mathbf{P}^1$. An isomorphism $\psi_0 : X' \to X_p$ defined over a number field K is given by a linear fractional transformation

$$u = A(t) = \frac{at + b}{ct + d} \qquad \text{where} \qquad A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathrm{K}).$$

The map from X' to $X(1)$ in (5) will be defined over $\mathbf{Q}$ if and only if

$$\mathcal{J}(A(t)) \in \mathbf{Q}(t). \tag{6}$$

3. Algorithm

Fix $p = 3$ or 5 and suppose E is an elliptic curve over $\mathbf{Q}$. We will construct the family of all elliptic curves over $\mathbf{Q}$ with the same mod p representation as E. When applying Wiles' result one is interested in curves E with complex multiplication, but the method works in general.

The construction proceeds as follows. Define polynomials $a_4(u), a_6(u) \in \mathbf{Q}[u]$ so that

$$y^2 = x^3 + a_4(u)x + a_6(u)$$

is the elliptic curve A_u of (1) if $p = 3$, or B_u of (3) if $p = 5$. Also let $n = 1$ if $p = 3$ and $n = 5$ if $p = 5$, so that a_4 has degree $4n$ and a_6 has degree $6n$.

Step 1. Find $u_0 \in \bar{\mathbf{Q}}$ such that

$$\mathcal{J}(u_0) = j(E).$$

Step 2. Find $\mu \in \bar{\mathbf{Q}}^\times$ such that

$$\mu^{-2}a_4(u_0), \mu^{-3}a_6(u_0) \in \mathbf{Q}$$

and

$$y^2 = x^3 + \mu^{-2}a_4(u_0)x + \mu^{-3}a_6(u_0) \quad \text{is isomorphic over } \mathbf{Q} \text{ to } E.$$

Step 3. Find $\alpha, \gamma \in \bar{\mathbf{Q}}$ such that

$$\mu^{-2}(1+\gamma t)^{4n}a_4(A(t)), \quad \mu^{-3}(1+\gamma t)^{6n}a_6(A(t)) \in \mathbf{Q}[t], \tag{7}$$

where

$$A = \begin{pmatrix} \alpha & u_0 \\ \gamma & 1 \end{pmatrix}.$$

Remark 3.1. For Step 1, let u_0 be any root of the numerator of $\mathcal{J}(u) - j(E) \in \mathbf{Q}(t)$. For Step 2, after putting E in Weierstrass form one can solve for μ directly. Step 2 ensures that the constant terms of the polynomials in (7) are rational numbers, and choosing rational values for the coefficients of t gives values for α and γ.

Remark 3.2. The condition in Step 3 implies (6). Conversely, if $\mathrm{Aut(E)} = \{\pm 1\}$, and we have $u_0, \mu, \alpha, \gamma \in \bar{\mathbf{Q}}$ and $A = \left(\begin{smallmatrix} \alpha & u_0 \\ \gamma & 1 \end{smallmatrix}\right)$ which satisfy (6) and the conditions in Steps 1 and 2, then it can be shown that the condition in Step 3 is satisfied.

Theorem 3.3. *Suppose E is an elliptic curve defined over $\mathbf{Q}$, and we have elements $u_0, \mu, \alpha, \gamma \in \bar{\mathbf{Q}}$ and a matrix $A \in \mathrm{GL}_2(\bar{\mathbf{Q}})$ satisfying the conditions in Steps 1, 2, and 3. Let $\mathcal{E}_t$ be the curve*

$$y^2 = x^3 + \mu^{-2}(1+\gamma t)^{4n}a_4(A(t))x + \mu^{-3}(1+\gamma t)^{6n}a_6(A(t)) \tag{8}$$

over $\mathbf{Q}(t)$. Then for every rational number t which is not a pole of $\mathcal{J} \circ A$, $\mathcal{E}_t$ is an elliptic curve over $\mathbf{Q}$ and $\mathcal{E}_t[p] \cong E[p]$ as $G_{\mathbf{Q}}$-modules.

Proof. Let $X' = \mathbf{P}^1$ and let W' be the elliptic surface over X' defined by (8), with W' mapping to X' by $(x, y, t) \mapsto t$. Let $\psi_0 : X' \xrightarrow{\sim} X_p$ be given by A, and $\psi : W' \xrightarrow{\sim} W_p$ by

$$(x, y, t) \mapsto (\mu(1+\gamma t)^{-2n}x, \mu^{3/2}(1+\gamma t)^{-3n}y, A(t)).$$

Then all the hypotheses of Proposition 2.1 are satisfied. By Step 2, the fiber of W' over $t = 0$ is isomorphic over $\mathbf{Q}$ to E. The theorem now follows from Corollary 2.2. □

4. Examples with $p = 3$

4.1. **Generic example.**

Theorem 4.1. *Fix an elliptic curve E over $\mathbf{Q}$,*

$$y^2 = x^3 + ax + b,$$

and let $J = j(E)/1728 = 4a^3/(4a^3 + 27b^2)$. Define

$$\begin{aligned} a(t) &= (-3(J-1)^2t^4 - 8(J-1)^2t^3 + 6(J-1)t^2 + 1)a, \\ b(t) &= (-(J-1)^3(8J+1)t^6 + 6(J-1)^2(2J+1)t^5 + 15(J-1)^2t^4 + \\ &\quad 20(J-1)^2t^3 - 15(J-1)t^2 + 6t + 1)b \end{aligned}$$

and define $\mathcal{E}_t$ by

$$y^2 = x^3 + a(t)x + b(t).$$

Then for every rational number t such that $\mathcal{E}_t$ is nonsingular, $\mathcal{E}_t[3]$ is isomorphic as a $G_{\mathbf{Q}}$-module to $E[3]$.

Proof. If $a = 0$ then $\mathcal{E}_t$ is $y^2 = x^3 + (t+1)^6 b$ and if $b = 0$ then $\mathcal{E}_t$ is $y^2 = x^3 + ax$. In both cases the elliptic surface is isotrivial and the theorem holds. Now assume a and b are both nonzero and let $j = j(E)$. Using (2), a computation shows that

$$\mathcal{J}(u) - j = \frac{27u^{12} + (648 - j)u^9 + 3(1728 + j)u^6 + 3(4608 - j)u^3 + j}{(u^3 - 1)^3}.$$

Let u_0 be a root of the numerator of $\mathcal{J}(u) - j$, so that Step 1 of §3 is satisfied. Let

$$\begin{aligned} \mu &= \frac{a_6(u_0)a}{a_4(u_0)b} = \frac{-2(u_0^6 - 20u_0^3 - 8)a}{(u_0^3 + 8)u_0 b}, \\ \alpha &= \frac{\mu^3 b u_0}{144(u_0^3 - 1)^2}, \\ \gamma &= \frac{-\mu^3 b(u_0^3 + 2)}{864(u_0^3 - 1)^2}. \end{aligned}$$

Since a and b are nonzero, we have $\mu \in \bar{\mathbf{Q}}^\times$. A symbolic computer calculation shows that with these choices, Steps 2 and 3 are satisfied, and the curve $\mathcal{E}_t$ is the same as the curve $\mathcal{E}_t$ of Theorem 3.3. Thus Theorem 3.3 completes the proof. □

Remark 4.2. If a and b are both nonzero, then the elliptic surface $\mathcal{E}_t$ in Theorem 4.1 is not isotrivial and every elliptic curve E' over $\mathbf{Q}$ such that $\rho_{E,3} \cong \rho_{E',3}$ is isomorphic over $\mathbf{Q}$ to $\mathcal{E}_t$ for some $t \in \mathbf{P}^1(\mathbf{Q})$ (see Remark 2.3).

Remark 4.3. The values of α and γ in the proof of Theorem 4.1 were obtained by choosing 0 and $6b$ for the linear coefficients of the polynomials in (7) and then solving for α and γ (see Remark 3.1). This choice gives rise to relatively simple polynomials $a(t)$ and $b(t)$. Choosing other values (not both zero) for the linear coefficients leads to other α, γ, $a(t)$, and $b(t)$, giving rise to an isomorphic elliptic surface.

4.2. $y^2 = x^3 - Dx$: **supersingular at 3, CM by $\sqrt{-1}$.**

Theorem 4.4. *Fix a nonzero integer D and define E_t by*

$$y^2 = x^3 + D(27D^2t^4 - 18Dt^2 - 1)x + 4D^2t(27D^2t^4 + 1).$$

(i) *For every rational number t, E_t is an elliptic curve over $\mathbf{Q}$ and $E_t[3]$ is isomorphic as a $G_{\mathbf{Q}}$-module to $E[3]$, where E is the elliptic curve $y^2 = x^3 - Dx$.*
(ii) *If D is prime to 3 and $t \in \mathbf{Q}$ is integral at 3 then E_t has good reduction at 3.*

Proof. Using (2), a computation shows that

$$\mathcal{J}(u) - j(E) = \frac{27(u^2 - 2u - 2)^2(u^4 + 2u^3 + 6u^2 - 4u + 4)^2}{(u^3 - 1)^3}.$$

Let u_0 be a root of $u^2 - 2u - 2$ and let ν be a fixed square root of $(1 + 2u_0)/D$. Let

$$\mu = 18\nu,$$
$$\alpha = (4 - u_0)\nu D,$$
$$\gamma = (1 - u_0)\nu D.$$

(We can take $u_0 = 1 + \sqrt{3}$, $\mu = \pm 18\sqrt{(3 + 2\sqrt{3})/D}$, $\alpha = \pm\sqrt{6D\sqrt{3}}$, and $\gamma = \pm\sqrt{(9 + 6\sqrt{3})D}$, where the signs of the square roots are taken appropriately and compatibly.) Then Steps 1, 2, and 3 are satisfied, and with these choices E_t is the curve $\mathcal{E}_t$ of Theorem 3.3. The discriminant of E_t is

$$\Delta(E_t) = -2^6D^3(27D^2t^4 + 18Dt^2 - 1)^3,$$

which has no rational roots, so E_t is an elliptic curve for every $t \in \mathbf{P}^1(\mathbf{Q})$. Theorem 3.3 implies (i). Statement (ii) follows immediately from the formula for the discriminant. □

Remark 4.5. The j-invariant of the curve E_t of Theorem 4.4 is

$$j(E_t) = \frac{1728(27D^2t^4 - 18Dt^2 - 1)^3}{(27D^2t^4 + 18Dt^2 - 1)^3}.$$

The result of Wiles mentioned in the introduction, together with Theorem 4.4, implies that if E' is an elliptic curve over $\mathbf{Q}$ whose j-invariant belongs to the set

$$\left\{ \frac{1728(27D^2t^4 - 18Dt^2 - 1)^3}{(27D^2t^4 + 18Dt^2 - 1)^3} : D \in \mathbf{Z} \text{ is prime to 3 and } t \in \mathbf{Q} \text{ is integral at 3} \right\}$$

then E' is modular.

4.3. $y^2 = x^3 - 432D$: **additive at 3, CM by $\sqrt{-3}$.**

Theorem 4.6. *Fix a nonzero integer D and define E_t by*

$$y^2 = x^3 - 27Dt(Dt^3 + 8)x + 54D(D^2t^6 - 20Dt^3 - 8).$$

If $t \in \mathbf{Q}$ and $Dt^3 \neq 1$, then E_t is an elliptic curve over $\mathbf{Q}$ and $E_t[3]$ is isomorphic as a $G_{\mathbf{Q}}$-module to $E[3]$, where E is the elliptic curve $y^2 = x^3 - 432D$.

Note that when $D = 1$, this is the Weierstrass model (1) of the Hesse family. The proof of Theorem 4.6 is the same as that of Theorem 4.4, after letting

$$u_0 = 0, \quad \mu = D^{-1/3}, \quad \alpha = D^{1/3}, \quad \text{and} \quad \gamma = 0.$$

The discriminant and j-invariant of E_t are given by

$$\Delta(E_t) = 2^{12}3^9D^2(Dt^3-1)^3, \qquad j(E_t) = \frac{27Dt^3(Dt^3+8)^3}{(Dt^3-1)^3}.$$

4.4. $y^2 + y = x^3 - x^2 - 7x + 10$**: ordinary at 3, CM by** $\sqrt{-11}$**.**

Theorem 4.7. *Define polynomials*

$$a(t) = -5346t^4 + 2079t^3 - 99t^2 + 77t - 7,$$
$$b(t) = -154366t^6 + 73507t^5 - 26805t^4 - 694t^3 + 1091t^2 - 127t + 10$$

and for each $t \in \mathbf{Q}$ *let* E_t *be the elliptic curve*

$$y^2 + (t^3 + t^2 + t + 1)y = x^3 - x^2 + a(t)x + b(t).$$

For every rational number t, E_t *is an elliptic curve over* $\mathbf{Q}$ *and* $E_t[3]$ *is isomorphic as a* $G_{\mathbf{Q}}$*-module to* $E[3]$*, where* E *is the elliptic curve* $y^2 + y = x^3 - x^2 - 7x + 10$*. If* $t \in \mathbf{Q}$ *is integral at* 3 *and* $t \equiv 0$ *or* $1 \pmod 3$ *then* E_t *has good reduction at* 3*.*

Proof. The elliptic curve E has complex multiplication by $\mathbf{Q}(\sqrt{-11})$ and good reduction at 3. We apply Theorem 4.1 with the Weierstrass model

$$y^2 = x^3 - \frac{22}{3}x + \frac{847}{108}$$

of E. The change of variables

$$(x, y, t) \mapsto \left(\frac{56^2(3x-1)}{3(56-147t)^2}, \frac{56^3(2y+t^3+t^2+t+1)}{2(56-147t)^3}, \frac{27t}{56-147t}\right),$$

transforms the curve $\mathcal{E}_t$ of Theorem 4.1 (with $a = -22/3$ and $b = 847/108$) to the curve E_t. The assertion about good reduction follows by computing that the discriminant of E_t is

$$-11^3(27t^2 - 8t + 1)^3(27t^2 + 36t + 1)^3.$$

□

Remark 4.8. The curve E_t of Theorem 4.7 has been chosen so that it is an integral model which is minimal when $t = 0$. The j-invariant of E_t is

$$\left(\frac{-16(54t^2 - 27t + 2)(27t^2 + 3t + 1)}{(27t^2 - 8t + 1)(27t^2 + 36t + 1)}\right)^3.$$

5. Examples with $p = 5$

5.1. **Generic example.**

Theorem 5.1. *Fix an elliptic curve* E *over* $\mathbf{Q}$*,*

$$y^2 = x^3 + ax + b.$$

Define

$$a(t) = a\sum_{k=0}^{20}\alpha_k t^k, \quad b(t) = b\sum_{k=0}^{30}\beta_k t^k,$$

where $\alpha_k, \beta_k \in \mathbf{Q}[J]$, with $J = j(E)/1728 = 4a^3/(4a^3+27b^2)$, are the polynomials given in the appendix. Define $\mathcal{E}_t$ by

$$y^2 = x^3 + a(t)x + b(t).$$

Then for every rational number t such that $\mathcal{E}_t$ is nonsingular, $\mathcal{E}_t[5]$ is isomorphic as a $G_{\mathbf{Q}}$-module to $E[5]$.

Proof. If $a = 0$ then $\mathcal{E}_t$ is $y^2 = x^3 + (t+1)^{30}b$ and if $b = 0$ then $\mathcal{E}_t$ is $y^2 = x^3 + ax$. In both cases the elliptic surface is isotrivial and the theorem holds. Now assume a and b are both nonzero and let $j = j(E)$. Using (4), a computation shows that the numerator of $\mathcal{J}(u) - j$ is

$$\begin{aligned} &u^{60} + (j-684)u^{55} + (55j+157434)u^{50} + 5(241j-2505492)u^{45} \\ &+ 35(374j+2213157)u^{40} + 3(23195j-43563048)u^{35} + (134761j-33211924)u^{30} \\ &- 3(23195j-43563048)u^{25} + 35(374j+2213157)u^{20} - 5(241j-2505492)u^{15} \\ &+ (55j+157434)u^{10} - (j-684)u^5 + 1. \end{aligned}$$

Let u_0 be a root of this polynomial and let

$$\begin{aligned} \mu &= \frac{a_6(u_0)a}{a_4(u_0)b} = \frac{-(u_0^{30} + 522u_0^{25} - 10005u_0^{20} - 10005u_0^{10} - 522u_0^5 + 1)a}{18(u_0^{20} - 228u_0^{15} + 494u_0^{10} + 228u_0^5 + 1)b}, \\ \alpha &= \frac{6\mu^3 b(57u_0^{15} - 247u_0^{10} - 171u_0^5 - 1)}{u_0^4(u_0^{10} + 11u_0^5 - 1)^4}, \\ \gamma &= \frac{6\mu^3 b(u_0^{15} - 171u_0^{10} + 247u_0^5 + 57)}{(u_0^{10} + 11u_0^5 - 1)^4}. \end{aligned}$$

A symbolic computer calculation shows that with these choices, the polynomials of (7) are $a(t)$ and $b(t)$. Thus the theorem follows from Theorem 3.3. □

Remark 5.2. If $ab \neq 0$, then the elliptic surface $\mathcal{E}_t$ in Theorem 4.1 is not isotrivial and every elliptic curve E' over $\mathbf{Q}$ such that $\rho_{E,5} \cong \rho_{E',5}$ is isomorphic over $\mathbf{Q}$ to $\mathcal{E}_t$ for some $t \in \mathbf{P}^1(\mathbf{Q})$ (see Remark 2.3).

5.2. $y^2 = x^3 - Dx$: ordinary at 5, CM by $\sqrt{-1}$.

Theorem 5.3. *Fix a nonzero integer D and define polynomials*

$$\begin{aligned} a(t) &= D^5t^9 - Dt, \\ b(t) &= -3125D^{11}t^{20} - 39583D^{10}t^{18} + 11875D^9t^{16} - 95000D^8t^{14} + 61750D^7t^{12} + \\ &\quad 41166D^6t^{10} + 12350D^5t^8 - 3800D^4t^6 + 95D^3t^4 - 63D^2t^2 - D, \\ c(t) &= -521875D^{16}t^{29} - 1355787D^{15}t^{27} - 7366875D^{14}t^{25} + 9635000D^{13}t^{23} - \\ &\quad 8315875D^{12}t^{21} - 3678639D^{11}t^{19} - 10560675D^{10}t^{17} + 30400D^9t^{15} + \\ &\quad 2091615D^8t^{13} + 134479D^7t^{11} + 62583D^6t^9 - 14200D^5t^7 + \\ &\quad 2327D^4t^5 + 107D^3t^3 + 7D^2t, \end{aligned}$$

and for each $t \in \mathbf{Q}$ let E_t be the elliptic curve

$$y^2 = x^3 + a(t)x^2 + b(t)x + c(t).$$

For every rational number t, E_t is an elliptic curve over $\mathbf{Q}$ and $E_t[5]$ is isomorphic as a $G_{\mathbf{Q}}$-module to $E[5]$, where E is the elliptic curve $y^2 = x^3 - Dx$. If D is prime to 5, $t \in \mathbf{Q}$ is integral at 5, and $Dt^2 \not\equiv 3 \pmod 5$ then E_t has good reduction at 5.

The elliptic curve E has complex multiplication by $\mathbf{Q}(i)$ and good reduction at 5. Let ν be a fixed square root of $-(1+2i)/D$. The proof of Theorem 5.3 is the same as the proof of Theorem 4.4, using the values

$$u_0 = i, \quad \mu = (1+2i)^2\nu/2, \quad \alpha = -\nu D, \quad \gamma = -i\nu D,$$

and the change of variables $x \mapsto x + (D^5t^9 - Dt)/3$. The discriminant of E_t is

$$4^3D^3(5D^2t^4 - 2Dt^2 + 1)^5(25D^4t^8 - 100D^3t^6 - 210D^2t^4 - 20Dt^2 + 1)^5$$

and the j-invariant is

$$\frac{[4(15D^2t^4 + 10Dt^2 + 3)(25D^4t^8 + 70D^2t^4 + 1)(25D^4t^8 + 300D^3t^6 - 370D^2t^4 + 60Dt^2 + 1)]^3}{[(5D^2t^4 - 2Dt^2 + 1)(25D^4t^8 - 100D^3t^6 - 210D^2t^4 - 20Dt^2 + 1)]^5}.$$

5.3. $y^2 = x^3 + 16D$: supersingular at 5, CM by $\sqrt{-3}$.

Theorem 5.4. *Fix a nonzero integer D and define polynomials*

$$\begin{aligned} a(t) &= -15000D^7t^{19} - 106875D^6t^{16} + 85500D^5t^{13} - 185250D^4t^{10} - \\ &\quad 17100D^3t^7 - 4275D^2t^4 + 120Dt, \\ b(t) &= 50000D^{11}t^{30} + 3625000D^{10}t^{27} + 4893750D^9t^{24} + 25012500D^8t^{21} - \\ &\quad 47523750D^7t^{18} - 9504750D^5t^{12} - 1000500D^4t^9 + 39150D^3t^6 - \\ &\quad 5800D^2t^3 + 16D, \end{aligned}$$

and for each $t \in \mathbf{Q}$ let E_t be the elliptic curve

$$y^2 = x^3 + a(t)x + b(t).$$

For every rational number t, E_t is an elliptic curve over $\mathbf{Q}$ and $E_t[5]$ is isomorphic as a $G_{\mathbf{Q}}$-module to $E[5]$, where E is the elliptic curve $y^2 = x^3 + 16D$. If D is prime to 5, $t \in \mathbf{Q}$ is integral at 5, then E_t has good reduction at 5.

The elliptic curve E has j-invariant 0, complex multiplication by $\mathbf{Q}(\sqrt{-3})$, and good reduction at 5. The proof of Theorem 5.4 is the same as the proof of Theorem 4.4, after letting

$$\begin{aligned} &u_0 \text{ be a root of the polynomial } u^4 - 3u^3 - u^2 + 3u + 1, \\ &\mu = 25(151711644u_0^3 - 6630528u_0^2 - 171313440u_0 - 51318165)^{1/3}/(12D^{1/3}), \\ &\alpha = -((2u_0^3 - 6u_0^2 + 3)D)^{1/3}, \\ &\gamma = ((3u_0^3 - 6u_0 - 2)D)^{1/3}, \end{aligned}$$

using the real cube roots. The discriminant of E_t is

$$-2^{12}3^3D^2(25D^4t^{12} - 275D^3t^9 - 165D^2t^6 + 55Dt^3 + 1)^5$$

and the j-invariant is

$$\frac{-15^3Dt^3(5D^2t^6 + 40Dt^3 - 1)^3(5D^2t^6 - 5Dt^3 + 8)^3(40D^2t^6 + 5Dt^3 + 1)^3}{(25D^4t^{12} - 275D^3t^9 - 165D^2t^6 + 55Dt^3 + 1)^5}.$$

Appendix

Since the polynomials $\alpha_k, \beta_k \in \mathbf{Q}[J]$ which occur in Theorem 5.1 are of marginal interest, we include them in this appendix.

$$
\begin{aligned}
\alpha_0 &= 1,\\
\alpha_1 &= 0,\\
\alpha_2 &= 190(J-1),\\
\alpha_3 &= -2280(J-1)^2,\\
\alpha_4 &= 855(J-1)^2(-17+16J),\\
\alpha_5 &= 3648(J-1)^3(17-9J),\\
\alpha_6 &= 11400(J-1)^3(17-8J),\\
\alpha_7 &= -27360(J-1)^4(17+26J),\\
\alpha_8 &= 7410(J-1)^4(-119-448J+432J^2),\\
\alpha_9 &= 79040(J-1)^5(17+145J-108J^2),\\
\alpha_{10} &= 8892(J-1)^5(187+2640J-5104J^2+1152J^3),\\
\alpha_{11} &= 98800(J-1)^6(-17-388J+864J^2),\\
\alpha_{12} &= 7410(J-1)^6(-187-6160J+24464J^2-24192J^3),\\
\alpha_{13} &= 54720(J-1)^7(17+795J-3944J^2+9072J^3),\\
\alpha_{14} &= 2280(J-1)^7(221+13832J-103792J^2+554112J^3-373248J^4),\\
\alpha_{15} &= 1824(J-1)^8(-119-9842J+92608J^2-911520J^3+373248J^4),\\
\alpha_{16} &= 4275(J-1)^8(-17-1792J+23264J^2-378368J^3+338688J^4),\\
\alpha_{17} &= 18240(J-1)^9(1+133J-2132J^2+54000J^3-15552J^4),\\
\alpha_{18} &= 190(J-1)^9(17+2784J-58080J^2+2116864J^3-946944J^4+2985984J^5),\\
\alpha_{19} &= 360(J-1)^{10}(-1+28J-1152J^2)(1+228J+176J^2+1728J^3),\\
\alpha_{20} &= (J-1)^{10}(-19-4560J+144096J^2-9859328J^3-8798976J^4-\\
&\quad 226934784J^5+429981696J^6),\\
\beta_0 &= 1,\\
\beta_1 &= 30,\\
\beta_2 &= -435(J-1),\\
\beta_3 &= 580(J-1)(-7+9J),\\
\beta_4 &= 3915(J-1)^2(7-8J),\\
\beta_5 &= 1566(J-1)^2(91-78J+48J^2),\\
\beta_6 &= -84825(J-1)^3(7+16J),\\
\beta_7 &= 156600(J-1)^3(-13-91J+92J^2),\\
\beta_8 &= 450225(J-1)^4(13+208J-144J^2),\\
\beta_9 &= 100050(J-1)^4(143+4004J-5632J^2+1728J^3),\\
\beta_{10} &= 30015(J-1)^5(-1001-45760J+44880J^2-6912J^3),\\
\beta_{11} &= 600300(J-1)^5(-91-6175J+9272J^2-2736J^3),\\
\beta_{12} &= 950475(J-1)^6(91+8840J-7824J^2),\\
\beta_{13} &= 17108550(J-1)^6(7+926J-1072J^2+544J^3),\\
\beta_{14} &= 145422675(J-1)^7(-1-176J+48J^2-384J^3),\\
\beta_{15} &= 155117520(J-1)^8(1+228J+176J^2+1728J^3),
\end{aligned}
$$

$$\begin{aligned}
\beta_{16} &= 145422675(J-1)^8(1+288J+288J^2+5120J^3-6912J^4),\\
\beta_{17} &= 17108550(J-1)^8(7+2504J+3584J^2+93184J^3-283392J^4+165888J^5),\\
\beta_{18} &= 950475(J-1)^9(-91-39936J-122976J^2-2960384J^3+11577600J^4-\\
&\quad 5971968J^5),\\
\beta_{19} &= 600300(J-1)^9(-91-48243J-191568J^2-6310304J^3+40515072J^4-\\
&\quad 46455552J^5+11943936J^6),\\
\beta_{20} &= 30015(J-1)^{10}(1001+634920J+3880800J^2+142879744J^3-\\
&\quad 1168475904J^4+1188919296J^5-143327232J^6),\\
\beta_{21} &= 100050(J-1)^{10}(143+107250J+808368J^2+38518336J^3-451953408J^4+\\
&\quad 757651968J^5-367276032J^6),\\
\beta_{22} &= 450225(J-1)^{11}(-13-11440J-117216J^2-6444800J^3+94192384J^4-\\
&\quad 142000128J^5+95551488J^6),\\
\beta_{23} &= 156600(J-1)^{11}(-13-13299J-163284J^2-11171552J^3+217203840J^4-\\
&\quad 474406656J^5+747740160J^6-429981696J^7),\\
\beta_{24} &= 6525(J-1)^{12}(91+107536J+1680624J^2+132912128J^3-3147511552J^4+\\
&\quad 6260502528J^5-21054173184J^6+10319560704J^7),\\
\beta_{25} &= 1566(J-1)^{12}(91+123292J+2261248J^2+216211904J^3-6487793920J^4+\\
&\quad 17369596928J^5-97854234624J^6+96136740864J^7-20639121408J^8),\\
\beta_{26} &= 3915(J-1)^{13}(-7-10816J-242352J^2-26620160J^3+953885440J^4-\\
&\quad 2350596096J^5+26796552192J^6-13329432576J^7),\\
\beta_{27} &= 580(J-1)^{13}(-7-12259J-317176J^2-41205008J^3+1808220160J^4-\\
&\quad 5714806016J^5+93590857728J^6-70131806208J^7-36118462464J^8),\\
\beta_{28} &= 435(J-1)^{14}(1+1976J+60720J^2+8987648J^3-463120640J^4+\\
&\quad 1359157248J^5-40644882432J^6-5016453120J^7+61917364224J^8),\\
\beta_{29} &= 30(J-1)^{14}(1+2218J+77680J^2+13365152J^3-822366976J^4+2990693888J^5-\\
&\quad 118286217216J^6-24514928640J^7+509958291456J^8-743008370688J^9),\\
\beta_{30} &= (J-1)^{15}(-1-2480J-101040J^2-19642496J^3+1399023872J^4-\\
&\quad 4759216128J^5+315623485440J^6+471904911360J^7-2600529297408J^8+\\
&\quad 8916100448256J^9).
\end{aligned}$$

References

[1] F. Klein, Vorlesungen über das Ikosaeder und die Auflösung der Gleichungen fünften Grades, Leipzig (1884) (= Lectures on the icosahedron and the solution of equations of the fifth degree, London (1913)).

[2] F. Klein, Elementary mathematics from an advanced standpoint: Arithmetic, Algebra, Analysis, Dover Publications, New York (1945).

[3] J-P. Serre, *Cohomologie galoisienne*, Lecture Notes in Mathematics **5**, Springer-Verlag, Berlin-New York (1965).

[4] G. Shimura, *Moduli and fibre systems of abelian varieties*, Ann. Math. **83** (1966) 294–338.

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

Department of Mathematics, Ohio State University, Columbus, Ohio 43210, USA
E-mail address: rubin@math.ohio-state.edu

Department of Mathematics, Ohio State University, Columbus, Ohio 43210, USA
E-mail address: silver@math.ohio-state.edu