EXPLICIT FAMILIES OF ELLIPTIC CURVES WITH PRESCRIBED MOD N REPRESENTATIONS

A. SILVERBERG

Introduction

In Part 1 we explain how to construct families of elliptic curves with the same mod 3, 4, or 5 representation as that of a given elliptic curve over $\mathbf{Q}$. In §4 we give equations for the families in the mod 4 case. The mod 3 and mod 5 cases were given in [9] (see also [8]). The results remain true (with the same proofs) with the field of rational numbers replaced by any field whose characteristic does not divide the level.

In Part 2 we use the work of Wiles, Taylor-Wiles, and Diamond to give explicit equations for infinite families of modular elliptic curves. In §7 (see Theorem 7.3) we show how to find infinite families of modular elliptic curves with the same mod 4 representation. In §8 we prove that if E is an elliptic curve over $\mathbf{Q}$, and the torsion subgroup of $E(\mathbf{Q})$ is not cyclic of order 1, 2, 3, 6, or 9 (i.e., the torsion subgroup is cyclic of order 4, 5, 7, 8, 10, or 12 or is of the form $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2N\mathbf{Z}$ for $N = 1$, 2, 3 or 4), then E is modular (see Theorem 8.1 and Corollary 8.10).

The proofs of the results in §4 use symbolic computer computations, which were done using the programs Pari and Mathematica. I would like to thank Ken Ribet and Karl Rubin for useful conversations, and the IHES for its hospitality.

Notation. Let $\mathbf{Z}$, $\mathbf{Q}$, and $\mathbf{C}$ denote, respectively, the integers, rational numbers, and complex numbers.

We will suppose that N is a positive integer, and $N \geq 3$. If 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 $E(\bar{k})$, and let $j(E)$ denote the j-invariant of E. If $F \subseteq \bar{\mathbf{Q}}$ is a number field, let $G_F = \mathrm{Gal}(\bar{\mathbf{Q}}/F)$. Let $\boldsymbol{\mu}_N$ be the $G_{\mathbf{Q}}$-module of N-th roots of unity, and let

$$e_N : E[N] \times E[N] \to \boldsymbol{\mu}_N$$

denote the Weil pairing. Let $\mathfrak{H}$ denote the complex upper half plane, and let

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

Let I denote the 2×2 identity matrix.

Part 1. Elliptic curves with the same mod N representation

1. Modular curves and elliptic modular surfaces of level N

Let

$$V_N = \mathbf{Z}/N\mathbf{Z} \times \boldsymbol{\mu}_N,$$

a $G_{\mathbf{Q}}$-module, and define a $G_{\mathbf{Q}}$-equivariant pairing

$$\eta_N : V_N \times V_N \to \boldsymbol{\mu}_N$$

by

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

Denote by Y_N the (non-compact) modular curve over $\mathbf{Q}$ which parametrizes triples (E,P,C) where E is an elliptic curve, P is a point of exact order N on E, C is a cyclic subgroup of order N on E, and C and P generate $E[N]$. Let $Y(N)$ denote the modular curve which parametrizes elliptic curves with full level N structure (see [12]). If ζ is a fixed primitive N-th root of unity in $\bar{\mathbf{Q}}$, then the map

$$(E,P,C) \mapsto (E,P,Q),$$

where Q is the unique point in C such that $e_N(P,Q) = \zeta$, induces an isomorphism (defined over $\mathbf{Q}(\zeta)$) from Y_N onto one connected component of $Y(N)$. Thus $Y_N(\mathbf{C})$ is isomorphic to $\mathfrak{H}/\Gamma(N)$. Let X_N denote the compactification of Y_N. Then X_N has genus 0 if and only if $N \leq 5$ (see p. 23 of [12]).

Lemma 1.1. *The curve Y_N parametrizes isomorphism classes of pairs (E,ϕ), where E is an elliptic curve and*

$$\phi : V_N \to E[N]$$

is a group isomorphism with the property that for all u, $v \in V_N$,

$$\eta_N(u,v) = e_N(\phi(u),\phi(v)).$$

Proof. Given (E,P,C), define ϕ by $\phi(a,\zeta) = aP+Q$ for the unique $Q \in C$ such that $e_N(P,Q) = \zeta$. Conversely, given (E,ϕ), let $P = \phi(1,1)$ and let $C = \phi(0 \times \boldsymbol{\mu}_N)$. □

There is a quasi-projective surface W_N 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 $\mathbf{Q}$, with N^2 sections defined over $\bar{\mathbf{Q}}$ of order dividing N, and such that the fibers of π_N correspond to the triples (E,P,C) classified by Y_N. (Note that this notation differs from that of [9], where W_N denoted a compactification.) The variety W_N can be viewed as the universal elliptic curve with level structure as above. See [13] for the theory of elliptic modular surfaces of level N. Analytically, we have

$$W_N(\mathbf{C}) \cong (\mathfrak{H} \times \mathbf{C})/(\Gamma(N) \ltimes \mathbf{Z}^2).$$

If $\tau \in \mathfrak{H}$, then the equivalence class of τ in $\mathfrak{H}/\Gamma(N)$ corresponds to the $\mathbf{C}$-isomorphism class of the triple $(\mathbf{C}/\mathbf{Z}\tau + \mathbf{Z}, \tau/N, \langle 1/N\rangle)$. Let $W_N[N]$ denote the N^2 sections of π_N of order dividing N, viewed as a $G_{\mathbf{Q}}$-module.

2. Twists of modular curves and elliptic modular surfaces

Let $\mathrm{Aut}(V_N,\eta_N)$ denote the group of automorphisms of V_N which preserve η_N. Suppose V is a free rank-2 module over $\mathbf{Z}/N\mathbf{Z}$ with a continuous and linear $G_{\mathbf{Q}}$-action and suppose

$$\eta : V \times V \to \boldsymbol{\mu}_N$$

is a non-degenerate alternating $G_{\mathbf{Q}}$-equivariant pairing. Fix a group isomorphism $\varphi : V_N \to V$ under which the pairing η_N corresponds to the pairing η. Then $\tau \mapsto \varphi^{-1} \circ \tau(\varphi)$ defines a cocycle on $G_{\mathbf{Q}}$ with values in $\mathrm{Aut}(V_N,\eta_N)$. By the universal property of W_N, there is a natural injective $G_{\mathbf{Q}}$-equivariant homomorphism

$$\mathrm{Aut}(V_N,\eta_N) \hookrightarrow \mathrm{Aut}(W_N).$$

There is also a natural $G_{\mathbf{Q}}$-equivariant homomorphism

$$\mathrm{Aut}(W_N) \to \mathrm{Aut}(Y_N).$$

Therefore, the above cocycle induces cocycles c and c_0 on $G_{\mathbf{Q}}$ with values in $\mathrm{Aut}(W_N)$ and in $\mathrm{Aut}(Y_N)$, respectively. Let W (respectively, Y) denote the twist of W_N (respectively, Y_N) by the cocycle c (respectively, c_0) (see [10]). Then W and Y are quasi-projective varieties defined over $\mathbf{Q}$. Up to isomorphism, W and Y are independent of the choice of φ. We obtain isomorphisms

$$\psi : W \to W_N \qquad \text{and} \qquad \psi_0 : Y \to Y_N$$

defined over $\bar{\mathbf{Q}}$, and a projection morphism $\pi : W \to Y$ defined over $\mathbf{Q}$, such that the diagram

$$\begin{array}{ccc} W & \xrightarrow{\psi} & W_N \\ \downarrow \pi & & \downarrow \pi_N \\ Y & \xrightarrow{\psi_0} & Y_N \end{array}$$

commutes, and such that for every $\tau \in G_{\mathbf{Q}}$,

$$c(\tau) = \psi \circ \tau(\psi)^{-1} \quad \text{and} \quad c_0(\tau) = \psi_0 \circ \tau(\psi_0)^{-1}.$$

It follows from the definition of W that if $t \in Y(\mathbf{C})$ and E_t is the elliptic curve $\pi^{-1}(t)$, then $E_t[N]$ and V are isomorphic as $\mathrm{Gal}(\overline{\mathbf{Q}(t)}/\mathbf{Q}(t))$-modules.

Theorem 2.1. *Suppose $N = 3$, 4, or 5, and E is an elliptic curve over $\mathbf{Q}$. Then there are infinitely many elliptic curves E' over $\mathbf{Q}$ such that $E[N]$ and $E'[N]$ are isomorphic as $G_{\mathbf{Q}}$-modules.*

Proof. Let $V = E[N]$ and let $\eta = e_N$, the Weil pairing on $E[N]$. Let W and Y be the varieties constructed as above, for V and η, and let X denote the compactification of Y. Since E is defined over $\mathbf{Q}$, $Y(\mathbf{Q})$ is nonempty. Since $N \leq 5$, X has genus 0. Therefore, X is isomorphic to $\mathbf{P}^1$, and $X(\mathbf{Q})$ and $Y(\mathbf{Q})$ are infinite. The points of $Y(\mathbf{Q})$ correspond to the desired elliptic curves E'. □

3. Models

Suppose now that $N = 3$, 4, or 5 and E is an elliptic curve over $\mathbf{Q}$ with Weierstrass model $y^2 = x^3 + ax + b$, with $a, b \in \mathbf{Q}$. We will construct a model for W, where Y and W are the twists of Y_N and W_N as in §2, with $V = E[N]$ and $\eta = e_N$. For $N = 3$, 4, and 5, let $m = 1$, 2, and 5, respectively. Then $12m = \#\mathrm{PSL}_2(\mathbf{Z}/N\mathbf{Z})$.

We can find a model for W_N (see (1) and (3) of [9] for $N = 3$ and $N = 5$, respectively, and (5) below for $N = 4$) such that for $u \in Y_N$, the fiber $E_u = \pi_N^{-1}(u)$ is of the form

$$E_u : y^2 = x^3 + a_4(u)x + a_6(u) \tag{1}$$

where $a_4(u), a_6(u) \in \mathbf{Q}[u]$ and $\deg(a_j) = jm$ for $j = 4, 6$. Let u_0 be an algebraic number such that E_{u_0} is isomorphic (over $\bar{\mathbf{Q}}$) to E. The isomorphism $\psi_0 : Y \to Y_N$ extends to an isomorphism $\psi_0 : X \to X_N$ on the compactifications. Since X and X_N are isomorphic to $\mathbf{P}^1$, the isomorphism ψ_0 can be given by a linear fractional transformation, which can be normalized so that 0 is sent to u_0. Let

$$A = \begin{pmatrix} \alpha & u_0 \\ \gamma & 1 \end{pmatrix} \in \mathrm{GL}_2(\bar{\mathbf{Q}})$$

be such a transformation. Since ψ takes a fiber $\mathcal{E}_t = \pi^{-1}(t)$ in W isomorphically onto a fiber $E_u = \pi_N^{-1}(u)$ in W_N, the isomorphism ψ takes a point $(t, x, y) \in W \subseteq \mathbf{P}^1 \times \mathbf{P}^2$ to a point of the form $(A(t), h(t)^{-2}x, h(t)^{-3}y) \in W_N \subseteq \mathbf{P}^1 \times \mathbf{P}^2$, for appropriate $h(t)$. Therefore, $(h(t)^{-2}x, h(t)^{-3}y)$ lies on $E_{A(t)}$. Using (1), it follows that (t, x, y) satisfies

$$y^2 = x^3 + h(t)^4 a_4(A(t))x + h(t)^6 a_6(A(t)). \tag{2}$$

When $t = 0$, we would like (2) to be an equation for the elliptic curve E. We will solve for $h(t)^2$, α, and γ so that

$$h(t)^4 a_4(A(t)) \quad \text{and} \quad h(t)^6 a_6(A(t)) \tag{3}$$

are in $\mathbf{Q}[t]$ (i.e., so that (2) is a model over $\mathbf{Q}$ for W) and take on the values a and b, respectively, when $t = 0$. From

$$h(0)^4 a_4(A(0)) = a \qquad \text{and} \qquad h(0)^6 a_6(A(0)) = b, \tag{4}$$

we can solve for $h(0)^2$. Write $h(t)^2 = h(0)^2(\gamma t + 1)^{2m}$ and substitute into (3). Then the expressions in (3) become polynomials in $\bar{\mathbf{Q}}[t]$, and have constant terms a and b, respectively. In particular, (2) is E when $t = 0$. Take any ordered pair of rational numbers (r, s) which is not a rational multiple of $(4a, 6b)$, set the coefficients of t in the polynomials in (3) equal to r and s, respectively, and solve for α and γ. With these values, (2) is a model over $\mathbf{Q}$ for W. Different choices of the pair (r, s) give rise to $\mathbf{Q}$-isomorphic elliptic surfaces.

Let $J = j(E)/1728$. The resulting model for W is of the form

$$y^2 = x^3 + a f_4(J, t)x + b f_6(J, t)$$

where $f_4, f_6 \in \mathbf{Z}[J, t]$, f_4 and f_6 depend only on N, and $\deg_t(f_j) = jm$ for $j = 4, 6$.

4. Level 4

We begin by writing down a model for the elliptic modular surface W_4, following [14]. We can view W_4 as a surface over $\mathbf{Q}$ or as an elliptic curve A_u over a function field in one variable. Define

$$A_u : y^2 = x(x-1)(x - \frac{(u + u^{-1})^2}{4}).$$

If $u \in \mathbf{C}$ and $u \notin \{0, 1, -1, i, -i\}$, then A_u is an elliptic curve over $\mathbf{Q}(u)$, and a Weierstrass model for A_u is given by

$$E_u : y^2 = x^3 - 27(u^8 + 14u^4 + 1)x - 54(u^{12} - 33u^8 - 33u^4 + 1). \tag{5}$$

We have

$$j(A_u) = j(E_u) = \frac{16(u^8 + 14u^4 + 1)^3}{u^4(u^4 - 1)^4}. \tag{6}$$

Let

$$P_u = (\frac{u^2 + 1}{2u^2}, \frac{1 - u^4}{4u^3}) \in A_u[4].$$

Let C_u be the $\mathrm{Gal}(\overline{\mathbf{Q}(u)}/\mathbf{Q}(u))$-invariant cyclic subgroup of $A_u[4]$ generated by the point (of order 4)

$$(\frac{u^2 + 1}{2u}, \frac{i(u^2 + 1)(u - 1)^2}{4u^2}).$$

The map $u \mapsto (A_u, P_u, C_u)$ induces a morphism $f : \mathbf{P}^1 \to X_4$ defined over $\mathbf{Q}$. The morphism $j : X_4 \to \mathbf{P}^1$ induced by $(E, P, C) \mapsto j(E)$ has degree $\#\mathrm{PSL}_2(\mathbf{Z}/4\mathbf{Z}) =$

24. By (6), the degree of the composition $j \circ f$ is 24, which is the same as the degree of j. Therefore, f is an isomorphism. Identify X_4 with $\mathbf{P}^1$ via f.

Next, we give models for the twisted surfaces W.

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

$$E: \quad y^2 = x^3 + ax + b,$$

with $a, b \in \mathbf{Q}$*, and let* $J = j(E)/1728 = 4a^3/(4a^3 + 27b^2)$*. Let* $\mathcal{E}_t$ *be*

$$\mathcal{E}_t: \quad y^2 = x^3 + a(t)x + b(t), \tag{7}$$

where

$$\begin{aligned} a(t) \;=\; & ((J-1)^4(144J^2 - 56J - 7)t^8 - 48(J-1)^4(4J+1)t^7 + \\ & 28(J-1)^3(4J+5)t^6 + 224(J-1)^3t^5 + 42(J-1)^2(4J-5)t^4 - \\ & 112(J-1)^2t^3 + 28(J-1)t^2 + 1)a, \\ b(t) \;=\; & ((J-1)^6(1728J^3 - 144J^2 + 116J + 1)t^{12} - \\ & 12(J-1)^5(288J^3 - 128J^2 + 82J + 1)t^{11} + \\ & 66(J-1)^5(48J^2 - 56J - 1)t^{10} - 44(J-1)^4(208J^2 - 176J - 5)t^9 - \\ & 99(J-1)^4(48J^2 - 104J - 5)t^8 + 792(J-1)^3(8J^2 - 10J - 1)t^7 - \\ & 924(J-1)^3(4J+1)t^6 + 792(J-1)^2t^5 - 99(4J-5)(J-1)^2t^4 + \\ & 44(J-1)(6J-5)t^3 - 66(J-1)t^2 + 12t + 1)b. \end{aligned}$$

Then for every rational number t *such that* $\mathcal{E}_t$ *is nonsingular,* $\mathcal{E}_t[4]$ *is isomorphic as a* $G_{\mathbf{Q}}$*-module to* $E[4]$*. If* $ab \neq 0$*, then (7) is a model for* W *over* $\mathbf{Q}$*, where* W *is constructed as in §2 from* $V = E[4]$*,* $\eta = e_4$*.*

Proof. If $a = 0$ then $\mathcal{E}_t$ is $y^2 = x^3 + (t+1)^{12}b$ and if $b = 0$ then $\mathcal{E}_t$ is $y^2 = x^3 + ax$. In both cases the elliptic surface is isotrivial, and $\mathcal{E}_t[4]$ is isomorphic as a $G_{\mathbf{Q}}$-module to $E[4]$. Now assume $ab \neq 0$. Let $j = j(E)$. Using (6), a computation shows that

$$j(E_u) - j(E) = \frac{16(u^{24}+1) + (672-j)(u^{20}+u^4) + (9456+4j)(u^{16}+u^8) + (45248-6j)u^{12}}{u^4(u^4-1)^4}.$$

Let u_0 be a root of the numerator. Then $j(E_{u_0}) = j(E)$. Following the algorithm in §3, we deduce from (4) that

$$h(0)^2 = \frac{a_4(u_0)b}{a_6(u_0)a} = \frac{b(u_0^8 + 14u_0^4 + 1)}{2a(u_0^{12} - 33u_0^8 - 33u_0^4 + 1)} \in \bar{\mathbf{Q}}^\times.$$

Now solve for α and γ so that the coefficients of t in the polynomials in (3) are 0 and $12b$, respectively. (This choice $(r, s) = (0, 12b)$ leads to the relatively simple polynomials $a(t)$ and $b(t)$ in the statement of the theorem.) We obtain

$$\alpha = \frac{(7u_0^4 + 1)b}{2^2 3^5 u_0^3 (1 - u_0^4)^3 h(0)^6}, \qquad \gamma = \frac{(u_0^4 + 7)b}{2^2 3^5 (u_0^4 - 1)^3 h(0)^6}.$$

With these values, (2) is a model over $\mathbf{Q}$ for W, and (2) is (7) with the stated $a(t)$ and $b(t)$. This elliptic surface is not isotrivial. □

Theorem 4.2. *Fix a nonzero integer* D *and define* $\mathcal{E}_t$ *by*

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

where

$$a(t) = D(81D^2t^4 + 6Dt^2 + 1)(81D^2t^4 - 90Dt^2 + 1),$$
$$b(t) = 8D^2t(9Dt^2 + 1)(9D^2t^4 - 2Dt^2 + 1)(729D^2t^4 - 18Dt^2 + 1).$$

If $t \in \mathbf{Q}$ and $9Dt^2 \neq 1$, then $\mathcal{E}_t$ is an elliptic curve over $\mathbf{Q}$ and $\mathcal{E}_t[4]$ is isomorphic as a $G_{\mathbf{Q}}$-module to $E[4]$, where E is the elliptic curve

$$y^2 = x^3 + Dx.$$

Proof. Using (6), a computation shows that

$$j(E_u) - j(E) = \frac{2^4(u^2 - 2u - 1)^2(u^2 + 2u - 1)^2(u^4 + 1)^2(u^4 + 6u^2 + 1)^2}{u^4(u^4 - 1)^4}.$$

Let $u_0 = 1 + \sqrt{2}$, a root of $u^2 - 2u - 1$. Now follow the algorithm in §3. We obtain

$$h(0)^4 = \frac{D}{a_4(u_0)} = \frac{(12\sqrt{2} - 17)D}{2^4 3^4}.$$

Let

$$h(0)^2 = \frac{(2\sqrt{2} - 3)\sqrt{-D}}{36}, \quad r = 0, \quad \text{and} \quad s = 8D^2.$$

Then

$$\alpha = 3\sqrt{-D}, \qquad \gamma = -3(1 + \sqrt{2})\sqrt{-D},$$

and we obtain $\mathcal{E}_t$ as in the statement of the theorem. The discriminant of $\mathcal{E}_t$ is

$$\Delta(\mathcal{E}_t) = -2^6D^3(9Dt^2 - 1)^4(81D^2t^4 + 54Dt^2 + 1)^4.$$

Thus if $t \in \mathbf{P}^1(\mathbf{Q})$ and $9Dt^2 \neq 1$, then $\mathcal{E}_t$ is an elliptic curve. The j-invariant of $\mathcal{E}_t$ is

$$j(\mathcal{E}_t) = \frac{1728(81D^2t^4 + 6Dt^2 + 1)^3(81D^2t^4 - 90Dt^2 + 1)^3}{(9Dt^2 - 1)^4(81D^2t^4 + 54Dt^2 + 1)^4}.$$

□

Theorem 4.3. *Fix a nonzero integer D and define $\mathcal{E}_t$ by*

$$y^2 = x^3 - 12Dt(8Dt^3 - 1)(Dt^3 + 1)x - D(8D^2t^6 + 88Dt^3 - 1)(8D^2t^6 + 1).$$

For every rational number t, $\mathcal{E}_t$ is an elliptic curve over $\mathbf{Q}$ and $\mathcal{E}_t[4]$ is isomorphic as a $G_{\mathbf{Q}}$-module to $E[4]$, where E is the elliptic curve

$$y^2 = x^3 + D.$$

Proof. We have $j(E) = 0$ and

$$j(E_u) = \frac{2^4(u^4 - 2u^3 + 2u^2 + 2u + 1)^3(u^4 + 2u^3 + 2u^2 - 2u + 1)^3}{u^4(u^4 - 1)^4}.$$

Let u_0 be a root of $u^4 - 2u^3 + 2u^2 + 2u + 1$. Let

$$\beta = u_0(1 + u_0 - u_0^2) \qquad \text{and} \qquad \lambda = \frac{(39\beta + 18)^{2/3}D^{1/3}}{6}.$$

Applying the algorithm of §3, we have

$$h(0)^6 = \frac{D(13\beta - 84)}{2^6 3^5}.$$

Let

$$h(0)^2 = \frac{[3D(13\beta - 84)]^{1/3}}{36}, \quad r = 12D, \quad \text{and} \quad s = 0.$$

Then

$$\alpha = (11u_0^3 - 33u_0^2 + 49u_0 - 11)\lambda, \quad \gamma = (3\beta - 19)\lambda,$$

and we obtain $\mathcal{E}_t$ as in the statement of the theorem. The discriminant and j-invariant of $\mathcal{E}_t$ are given by

$$\Delta(\mathcal{E}_t) = -2^4 3^3 D^2 (8D^2t^6 - 20Dt^3 - 1)^4,$$
$$j(\mathcal{E}_t) = \frac{-2^{14}3^3 Dt^3(8Dt^3 - 1)^3(Dt^3 + 1)^3}{(8D^2t^6 - 20Dt^3 - 1)^4}.$$

Since $\Delta(\mathcal{E}_t)$ has no rational roots, the theorem follows. □

Part 2. Explicit families of modular elliptic curves

5. Modular j-invariants

If E and E' are elliptic curves over $\mathbf{Q}$, and E and E' are isomorphic over $\mathbf{C}$, then E is modular if and only if E' is modular. It therefore makes sense to talk about modular j-invariants, i.e., the rational numbers which are j-invariants of modular elliptic curves. Before the work of Wiles, it was not known that there are infinitely many modular j-invariants. Using the results of Wiles [19], Taylor-Wiles [18], and Diamond [2], it is now very easy to write down infinite families of modular j-invariants.

We begin by stating Diamond's improvement of the results of Wiles and Taylor-Wiles. While Theorems 7.3 and 8.1 below follow easily from this statement, in fact such results generally follow from the theorems stated in [19], with some additional work.

Theorem 5.1. *If E is an elliptic curve over $\mathbf{Q}$ which has semistable reduction at 3 and at 5, then E is modular.*

Proof. See Theorem 1.2 of [2]. □

6. Semistable reduction

We next state some results which will be used in the proofs of Propositions 7.1 and 8.4. If F is a number field, and v is a prime ideal of F, let $\mathcal{I}_v$ denote the inertia subgroup of G_F corresponding to an extension to $\bar{\mathbf{Q}}$ of the v-adic valuation on F.

Theorem 6.1. *If E is an elliptic curve over $\mathbf{Q}$, then there is a number field over which E has everywhere semistable reduction.*

Proof. See Proposition 3.6 of [4]. See also Proposition 5.4 on p. 181 of [17]. □

Theorem 6.2. *If E is an elliptic curve over $\mathbf{Q}$, p and ℓ are distinct prime numbers, $\rho_p : G_{\mathbf{Q}} \to \mathrm{GL}_2(\mathbf{Z}_p)$ is the p-adic representation associated to E, and $\tau \in \mathcal{I}_\ell$, then the characteristic polynomial of $\rho_p(\tau)$ has integer coefficients which are independent of p.*

Proof. See Theorem 4.3 of [4]. □

Theorem 6.3. *Suppose E is an elliptic curve over a number field F, p and ℓ are distinct prime numbers, v is a prime ideal of F dividing ℓ, and $\rho_p : G_F \to \mathrm{GL}_2(\mathbf{Z}_p)$ is the p-adic representation associated to E. Then E has good reduction at v if and only if $\rho_p(\mathcal{I}_v)$ is trivial.*

Proof. See Theorem 1 of [11]. □

Theorem 6.4. *Suppose E is an elliptic curve over a number field F, p and ℓ are distinct prime numbers, v is a prime ideal of F dividing ℓ, and $\rho_p : G_F \to \mathrm{GL}_2(\mathbf{Z}_p)$ is the p-adic representation associated to E. Then the following are equivalent:*

(i) *E has semistable reduction at v,*
(ii) *for every $\tau \in \mathcal{I}_v$, all the eigenvalues of $\rho_p(\tau)$ are 1 (i.e., $\mathcal{I}_v$ acts unipotently on the p-adic Tate module of E),*
(iii) *for every $\tau \in \mathcal{I}_v$, $(\rho_p(\tau) - I)^2 = 0$.*

Proof. See Proposition 3.5 and Corollaire 3.8 of [4]. □

Let $\bar{\mathbf{Z}}$ denote the ring of algebraic integers.

Theorem 6.5. *If α is a root of unity in $\bar{\mathbf{Z}}$, and either*

(a) *$5 \leq N \in \mathbf{Z}$ and $(\alpha - 1)^2 \in N\bar{\mathbf{Z}}$, or*
(b) *$3 \leq N \in \mathbf{Z}$ and $\alpha - 1 \in N\bar{\mathbf{Z}}$,*

then $\alpha = 1$.

Proof. Part (b) is well-known. See Theorem 3.1 of [16] for proofs of (a) and (b). □

Lemma 6.6. *Suppose that N is a positive integer, and for each prime divisor p of N we have a matrix $A_p \in M_2(\mathbf{Z}_p)$ such that the characteristic polynomials of the A_p have integral coefficients independent of p, and such that $(A_p - I)^2 \in NM_2(\mathbf{Z}_p)$. Then for every eigenvalue α of A_p, $(\alpha - 1)/\sqrt{N}$ satisfies a monic polynomial with integer coefficients.*

Proof. See Lemma 5.2 of [15]. □

7. Mod 4 representations

Proposition 7.1. *Suppose E and E' are elliptic curves over $\mathbf{Q}$, N is a positive integer, $E[N]$ and $E'[N]$ are isomorphic as $G_{\mathbf{Q}}$-modules, and ℓ is a prime number which does not divide N. If*

(a) *$N \geq 5$ and E has semistable reduction at ℓ, or*
(b) *$N = 3$ or 4 and E has good reduction at ℓ,*

then E' has semistable reduction at ℓ.

Proof. We give a proof in the spirit of [15]. Let $\mathcal{I}_\ell$ denote the inertia subgroup of $G_{\mathbf{Q}}$ corresponding to an extension $\bar{\lambda}$ to $\bar{\mathbf{Q}}$ of the ℓ-adic valuation on $\mathbf{Q}$. Suppose $\tau \in \mathcal{I}_\ell$, p is a prime divisor of N, and $\rho_{E,p}$ and $\rho_{E',p}$ are the p-adic representations of $G_{\mathbf{Q}}$ associated to E and E', respectively. Suppose α is an eigenvalue of $\rho_{E',p}(\tau)$. There is a number field F such that E has semistable reduction at the restriction λ of $\bar{\lambda}$ to F (by Theorem 6.1). Therefore, $\tau^m \in \mathcal{I}_\lambda$ for some positive integer m. By Theorem 6.4,

$$(\rho_{E',p}(\tau)^m - I)^2 = 0.$$

Thus, $(\alpha^m - 1)^2 = 0$, so $\alpha^m = 1$.

Since E has semistable reduction at ℓ,

$$(\rho_{E,p}(\tau) - I)^2 = 0$$

by Theorem 6.4. Since $E[N] \cong E'[N]$, we have

$$\rho_{E,p}(\tau) - \rho_{E',p}(\tau) \in N\mathrm{M}_2(\mathbf{Z}_p)$$

for appropriate choices of bases for the p-adic Tate modules of E and of E'. Therefore,

$$(\rho_{E',p}(\tau) - I)^2 \in N\mathrm{M}_2(\mathbf{Z}_p).$$

The characteristic polynomial of $\rho_{E',p}(\tau)$ is independent of the choice of prime divisor p of N (by Theorem 6.2). By Lemma 6.6, $(\alpha - 1)^2 \in N\bar{\mathbf{Z}}$. Suppose $N \geq 5$. By Theorem 6.5a, $\alpha = 1$. Therefore, $\mathcal{I}_\ell$ acts on the Tate module of E' by unipotent operators. By Theorem 6.4, E' has semistable reduction at ℓ. Now suppose $N = 3$ or 4 and E has good reduction at ℓ. By Theorem 6.3, $\rho_{E,p}(\tau) = I$. Therefore, $\rho_{E',p}(\tau) - I \in N\mathrm{M}_2(\mathbf{Z}_p)$, $\alpha - 1 \in N\bar{\mathbf{Z}}$, and $\alpha = 1$ (using Lemma 6.6 and Theorem 6.5b). By Theorem 6.4, E' has semistable reduction at ℓ. □

Examples 7.2. To see that Proposition 7.1a fails for $N = 3$ or 4, let E be the elliptic curve $y^2 = x^3 + x + 1$. The conductor of E is $2^4 31$, so E has multiplicative reduction at 31. Consider Theorem 4.1 with $a = b = 1$ and let E' be the elliptic curve obtained by letting $t = 1$ (letting $t = 0$ gives E). Then $E[4] \cong E'[4]$, and it is easy to check that E' has additive reduction at 31. Theorem 4.1 of [9] is the analogue of Theorem 4.1 of this paper, with $N = 3$ instead of $N = 4$. Consider Theorem 4.1 of [9] with $a = b = 1$, and let E'' be the elliptic curve obtained by letting $t = 1$ (again, $t = 0$ gives E). Then $E[3] \cong E''[3]$, and it is easy to check that E'' has additive reduction at 31.

To see that Proposition 7.1b fails for $N = 2$, let ℓ be an odd prime, let E be the elliptic curve $y^2 = x^3 - x$, and let E' be the elliptic curve $y^2 = x^3 - \ell^2 x$. Then E has good reduction at ℓ (the conductor of E is 2^5), E' has additive reduction at ℓ (the conductor of E' is $2^5\ell^2$), and $E[2] \cong E'[2] \cong \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$.

Theorem 7.3. *If E is an elliptic curve over $\mathbf{Q}$ which has good reduction at 3 and at 5, and E' is an elliptic curve over $\mathbf{Q}$ such that $E[4]$ and $E'[4]$ are isomorphic as $G_{\mathbf{Q}}$-modules, then E' is modular.*

Proof. By Proposition 7.1b with $N = 4$, E' has semistable reduction at 3 and at 5. Therefore E' is modular by Theorem 5.1. □

Therefore, the explicit families of §4 give infinite families of modular elliptic curves, as long as one of the elliptic curves in the family has good reduction at 3 and at 5.

8. Torsion subgroups

Theorem 8.1. *If E is an elliptic curve over $\mathbf{Q}$ which has:*

1. *all its points of order 2,*
2. *a cyclic subgroup of order 4,*
3. *a point of order 5, or*
4. *a point of order 7,*

defined over $\mathbf{Q}$, then E is modular.

We prove Theorem 8.1 in a series of lemmas.

Lemma 8.2. *If E is an elliptic curve over $\mathbf{Q}$, and $E(\mathbf{Q}) \supseteq \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$, then E is modular.*

Proof. It is easy to see that E is isomorphic over $\mathbf{C}$ to an elliptic curve E' of the form

$$y^2 = x(x - A)(x - B)$$

where A and B are relatively prime integers. Suppose p is an odd prime. Since the right hand side does not have a triple root modulo p, E' has semistable reduction at p. In other words, one can twist away any additive reduction on E at odd primes. The lemma now follows from Theorem 5.1. □

Lemma 8.2 was an observation made with K. Rubin. The main theorem of [3] shows that Lemma 8.2 follows from the results of [19] and [18], without using [2].

Lemma 8.3. *If E is an elliptic curve over $\mathbf{Q}$, and E has a cyclic subgroup of order 4 defined over $\mathbf{Q}$, then E is modular.*

Proof. Suppose C is a rational cyclic subgroup of E of order 4. Let $D = C \cap E[2]$. Then D is a subgroup of E of order 2, and D is defined over $\mathbf{Q}$. Let $E' = E/D$, an elliptic curve over $\mathbf{Q}$. The quotient map $\varphi : E \to E'$ is an isogeny defined over $\mathbf{Q}$. Therefore to show that E is modular, it suffices to show that E' is modular. Fix a generator x of C and fix $y \in E[2] - D$. Then $\varphi(x)$ generates C/D, which is a rational subgroup of E' of order 2. Therefore, $\varphi(x)$ is defined over $\mathbf{Q}$. Similarly, $\varphi(y)$ generates $E[2]/D$, a rational subgroup of E' of order 2, so $\varphi(y)$ is defined over $\mathbf{Q}$. Since $x - y \notin C$, we have $x - y \notin D$, so $\varphi(x) \neq \varphi(y)$. Therefore, E' has all its points of order 2 defined over $\mathbf{Q}$. By Lemma 8.2, E' is modular. □

Proposition 8.4. *If E is an elliptic curve over $\mathbf{Q}$, $5 \leq N \in \mathbf{Z}$, and $E(\mathbf{Q}) \supseteq \mathbf{Z}/N\mathbf{Z}$, then E has semistable reduction at every prime which does not divide N.*

Proof. We give a proof from [15] (see Theorem 6.2). Suppose ℓ is a prime which does not divide N. Let $\mathcal{I}_\ell$ denote the inertia subgroup of $G_{\mathbf{Q}}$ corresponding to an extension $\bar{\lambda}$ to $\bar{\mathbf{Q}}$ of the ℓ-adic valuation on $\mathbf{Q}$. Suppose $\tau \in \mathcal{I}_\ell$. Since ℓ does not divide N, $\mathbf{Q}(\zeta_N)$ is unramified at ℓ, so $\mathcal{I}_\ell$ acts as the identity on the N-th roots of unity. Suppose p is a prime divisor of N, and let $\rho_p : G_{\mathbf{Q}} \to \mathrm{GL}_2(\mathbf{Z}_p)$ denote the p-adic representation associated to E. Since $E(\mathbf{Q})$ has a point of order N,

$$\rho_p(\tau) \equiv \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \pmod{N\mathrm{M}_2(\mathbf{Z}_p)},$$

for an appropriate choice of basis for the p-adic Tate module of E. Therefore, $(\rho_p(\tau) - I)^2 \in N\mathrm{M}_2(\mathbf{Z}_p)$. There is a number field F such that E has semistable reduction at the restriction λ of $\bar{\lambda}$ to F (by Theorem 6.1). Then $\tau^m \in \mathcal{I}_\lambda$ for some positive integer m. By Theorem 6.4, $(\rho_p(\tau)^m - I)^2 = 0$. Let α be an eigenvalue of $\rho_p(\tau)$. Then $(\alpha^m - 1)^2 = 0$, so $\alpha^m = 1$. By Lemma 6.6 and Theorem 6.2, $(\alpha - 1)^2 \in N\mathrm{M}_2(\bar{\mathbf{Z}})$. By Theorem 6.5a, $\alpha = 1$. Therefore, $\mathcal{I}_\ell$ acts on the Tate module of E by unipotent operators. By Theorem 6.4, E has semistable reduction at ℓ. □

Examples 8.5. Proposition 8.4 fails for $N < 5$. The point $(48, -15)$ is a point of order 4 on the elliptic curve $y^2 + xy = x^3 - x^2 - 7056x + 229905$, and this curve has additive reduction at 3 (it is the curve 63A5 in Cremona's tables [1]). The point $(1, 1)$ is a point of order 3 on the elliptic curve $y^2 = x^3 + x^2 - x$, and this curve has additive reduction at 2 (it is 20A2 in [1]).

Lemma 8.6. *If E is an elliptic curve over $\mathbf{Q}$, and $E(\mathbf{Q}) \supseteq \mathbf{Z}/7\mathbf{Z}$, then E is modular.*

Proof. By Proposition 8.4 with $N = 7$, E has semistable reduction at 3 and at 5. By Theorem 5.1, E is modular. □

Theorem 8.7. *If E is an elliptic curve over $\mathbf{Q}$, p is an odd prime number, E has semistable reduction at p, the mod p representation $\bar{\rho}_{E,p}$ for E is modular, and the restriction of $\bar{\rho}_{E,p}$ to $G_{\mathbf{Q}(\sqrt{-1^{(p-1)/2}p})}$ is absolutely irreducible, then E is modular.*

Proof. This is Theorem 5.3 of [2], applied to the p-adic representation associated to the elliptic curve E. □

Proposition 8.8. *If E is an elliptic curve over $\mathbf{Q}$, the mod 5 representation for E is reducible, and the restriction to $G_{\mathbf{Q}(\sqrt{-3})}$ of the mod 3 representation for E is not absolutely irreducible, then E is modular.*

Proof. See Proposition 13 of [7] (by work of J. E. Cremona, the elliptic curves over $\mathbf{Q}$ whose j-invariants are given in Proposition 13 of [7] are all modular), p. 544 of [19], or the proof of Theorem 5.4 of [2]. □

Lemma 8.9. *If E is an elliptic curve over $\mathbf{Q}$, and $E(\mathbf{Q}) \supseteq \mathbf{Z}/5\mathbf{Z}$, then E is modular.*

Proof. Since $E(\mathbf{Q}) \supseteq \mathbf{Z}/5\mathbf{Z}$, the mod 5 representation for E is reducible. By Proposition 8.8, we may assume that the restriction to $G_{\mathbf{Q}(\sqrt{-3})}$ of the mod 3 representation for E is absolutely irreducible. The mod 3 representation for E is modular by the Langlands-Tunnell Theorem. By Proposition 8.4, E has semistable reduction at 3. By Theorem 8.7, E is modular. □

Theorem 8.1 follows from Lemmas 8.2, 8.3, 8.6, and 8.9.

By [6], if E is an elliptic curve over $\mathbf{Q}$, then the torsion subgroup of $E(\mathbf{Q})$ is isomorphic to one of the following 15 groups:

$$\begin{array}{ll} \mathbf{Z}/N\mathbf{Z} & \text{for } N = 1, \ldots, 10 \text{ or } 12, \\ \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2N\mathbf{Z} & \text{for } N = 1, 2, 3, \text{ or } 4. \end{array}$$

This and Theorem 8.1 immediately imply the following result.

Corollary 8.10. *If E is an elliptic curve over $\mathbf{Q}$, and the torsion subgroup of $E(\mathbf{Q})$ is not a cyclic group of order 1, 2, 3, 6, or 9, then E is modular.*

Given a model for an elliptic curve E over $\mathbf{Q}$, the Nagell-Lutz Theorem (see Corollary 7.2 of Chapter VIII of [17]) provides an algorithm for computing the torsion subgroup of $E(\mathbf{Q})$.

9. Explicit families of modular elliptic curves

By Theorem 8.1, the elliptic curves below are modular. See Table 3 on p. 217 of [5] for such parametrizations of elliptic curves over $\mathbf{Q}$ with points of finite order.

Example 9.1 (rational 2-torsion)**.** Elliptic curves over $\mathbf{Q}$ with all points of order 2 defined over $\mathbf{Q}$ are given by

$$Dy^2 = x(x-1)(x-\lambda)$$

with $D, \lambda \in \mathbf{Q}^\times, \lambda \neq 1$. The corresponding (modular) j-invariants are all the numbers of the form

$$\frac{2^8(\lambda^2-\lambda+1)^3}{\lambda^2(\lambda-1)^2} \quad \text{with} \quad \lambda \in \mathbf{Q} - \{0, 1\}.$$

Example 9.2 (rational cyclic subgroup of order 4)**.** The family of elliptic curves with a rational cyclic subgroup of order 4 is given by

$$y^2 = x^3 + D(1-4b)x^2 - 8D^2bx + 16D^3b^2$$

with $b, D \in \mathbf{Q}^\times, b \neq \frac{1}{16}$. The rational cyclic subgroup of order 4 is

$$\{0, (4bD, 0), (0, \pm 4bD\sqrt{D})\}$$

and the j-invariant is

$$\frac{(16b^2+16b+1)^3}{(16b+1)b^4}.$$

Example 9.3 (rational points of order 5)**.** The family of elliptic curves over $\mathbf{Q}$ with a rational point of order 5 is given by

$$y^2 + (1-b)xy - by = x^3 - bx^2$$

with $b \in \mathbf{Q}^\times$. The point $(0,0)$ has order 5.

Example 9.4 (rational points of order 7)**.** The family of elliptic curves over $\mathbf{Q}$ with a rational point of order 7 is given by

$$y^2 + (1-d(d-1))xy - d^2(d-1)y = x^3 - d^2(d-1)x^2$$

with $d \in \mathbf{Q} - \{0, 1\}$. The point $(0,0)$ has order 7.

References

[1] J. E. Cremona, Algorithms for modular elliptic curves, Cambridge Univ. Press, Cambridge, 1992.

[2] F. Diamond, *On deformation rings and Hecke rings*, preprint.

[3] F. Diamond, K. Kramer, *Modularity of a family of elliptic curves*, Math. Research Letters **2** (1995), 299–305.

[4] A. Grothendieck, *Modèles de Néron et monodromie*, in Groupes de monodromie en géometrie algébrique, SGA7 I, A. Grothendieck, ed., Lecture Notes in Math. **288**, Springer, Berlin-Heidelberg-New York, 1972, pp. 313–523.

[5] D. S. Kubert, *Universal bounds on the torsion of elliptic curves*, Proc. London Math. Soc. **33** (1976), 193–237.

[6] B. Mazur, *Modular curves and the Eisenstein ideal*, Publ. Math. IHES **47** (1977), 133–186.

[7] K. Rubin, *Modularity of mod* 5 *representations*, this volume.

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

[9] 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.

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

[11] J-P. Serre, J. Tate, *Good reduction of abelian varieties*, Ann. of Math. **88** (1968), 492–517.

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

[13] T. Shioda, *On elliptic modular surfaces*, J. Math. Soc. Japan **24** (1972), 20–59.

[14] T. Shioda, *On rational points of the generic elliptic curve with level N structure over the field of modular functions of level N*, J. Math. Soc. Japan **25** (1973), 144–157.

[15] A. Silverberg, Yu. G. Zarhin, *Semistable reduction and torsion subgroups of abelian varieties*, Ann. Inst. Fourier **45** (1995), 403–420.

[16] A. Silverberg, Yu. G. Zarhin, *Variations on a theme of Minkowski and Serre*, to appear in J. Pure and Applied Algebra.

[17] J. Silverman, The Arithmetic of Elliptic Curves, Springer-Verlag, New York-Berlin-Heidelberg-Tokyo, 1986.

[18] R. Taylor, A. Wiles, *Ring-theoretic properties of certain Hecke algebras*, Ann. Math. **141** (1995), 553–572.
[19] A. Wiles, *Modular elliptic curves and Fermat's Last Theorem*, Ann. Math. **141** (1995), 443–551.

Department of Mathematics, Ohio State University, 231 W. 18 Avenue, Columbus, Ohio 43210–1174, USA
E-mail address: silver@math.ohio-state.edu