ACTA ARITHMETICA
XC.2 (1999)

Elliptic curves with non-trivial 2-adic Iwasawa μ-invariant

by

Kenneth Kramer (Flushing, NY)

1. Introduction. Ralph Greenberg [1] has explained a very general framework for Iwasawa theory which includes as a special case the study of Selmer groups of elliptic curves over cyclotomic towers initiated by Barry Mazur in [3]. Suppose that E is an elliptic curve defined over $\mathbb{Q}$, and let p be a prime at which E has height 1 (i.e. good ordinary, or multiplicative) reduction. Write $\mathbb{Q}_\infty$ for the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$. The p^∞-*Selmer group* $\mathrm{Sel}(\mathbb{Q}_\infty, E[p^\infty])$ is a subgroup of $H^1(\mathbb{Q}_\infty, E[p^\infty])$ defined by imposing certain local conditions at each completion of $\mathbb{Q}_\infty$. Like the classical Selmer group to which it is closely related [1, §2], the p^∞-Selmer group serves to control the Mordell–Weil group $E(\mathbb{Q}_\infty)$ of $\mathbb{Q}_\infty$-rational points on E via the inclusion

$$E(\mathbb{Q}_\infty) \otimes \mathbb{Q}_p/\mathbb{Z}_p \hookrightarrow \mathrm{Sel}(\mathbb{Q}_\infty, E[p^\infty]).$$

The Pontryagin dual $X_E(\mathbb{Q}_\infty) = \mathrm{Hom}(\mathrm{Sel}(\mathbb{Q}_\infty, E[p^\infty]), \mathbb{Q}_p/\mathbb{Z}_p)$ is a module over the Iwasawa algebra $\Lambda = \mathbb{Z}_p[[T]]$, where as usual the action of T is given by the action of $\gamma - 1$ for a choice of topological generator γ of $\mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q})$. A conjecture of Mazur implies that $X_E(\mathbb{Q}_\infty)$ is a finitely generated torsion Λ-module; it is known to hold when E is modular, and in particular when E is semistable ([2, §1]). If so, we have

$$X_E(\mathbb{Q}_\infty) \sim \Lambda/(p^m) \times \prod_{i=1}^{t} \Lambda/(f_i(T)^{a_i}),$$

up to finite kernel and cokernel, where each $f_i(T) \in \Lambda$ is an irreducible polynomial of positive degree, and $\mu_p(E) = m$ defines the p-adic Iwasawa μ-invariant of E.

In the course of preparing the survey article on Iwasawa theory of elliptic curves cited above, Greenberg observed [2, Prop. 5.13] that if E admits a $\mathbb{Q}$-isogeny ϕ_n of degree 2^n whose kernel is cyclic as an abelian group and satisfies certain 2-adic and archimedean conditions, then $\mu_2(E) \geq n$. These

1991 *Mathematics Subject Classification*: 11G05, 11G07.

conditions require that upon extension of the base to $\mathbb{Q}_l$ for $l = 2$ or $l = \infty$, the kernel of ϕ_n be contained in a special subgroup $W_l^{(n)}$ of $E[2^n]$ which we define more precisely in Sections 2 and 3 below. For $n \leq 4$, it is well known that the modular curve $X_0(2^n)$ has genus zero, and therefore gives rise to a family of infinitely many elliptic curves defined over $\mathbb{Q}$, each admitting a cyclic $\mathbb{Q}$-isogeny of degree 2^n. Greenberg found examples of such isogenies satisfying the additional 2-adic and archimedean conditions. There are no cyclic $\mathbb{Q}$-isogenies of degree 32, in view of the fact that the only rational points on $X_0(32)$ are the cusps.

In this note, we modify the standard family of elliptic curves arising from $X_0(2^n)$ for $1 \leq n \leq 4$, to impose the desired 2-adic and archimedean behavior. Thus we obtain (see Section 5) a family of semistable elliptic curves E such that $\mu_2(E) \geq n$. It would follow from [2, Conjecture 1.11] that this family includes all semistable curves with $\mu_2(E) \geq n$, and moreover that $\mu_2(E) \leq 4$. Some elementary observations about the construction of cyclic isogenies make the computational task quite manageable. An amusing consequence of these observations is that for $n = 2, 3, 4$, the relevant isogenies occur in pairs. We have checked our computations with the help of the symbolic algebra program, Maple.

We are indebted to the referee for raising the question of whether or not these families admit additional sections beyond those already imposed. In Section 6, we show that there are essentially no additional sections, thanks to a suggestion by Armand Brumer that the rank formulas of T. Shioda [4, §1, §2] should apply.

It is a pleasure to thank Ralph Greenberg for bringing his criterion for large μ-invariant to our attention, and for generously sharing his ideas about it.

2. The 2-adic condition. Let $G_{\mathbb{Q}} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ be the absolute Galois group of $\mathbb{Q}$, and write $\mathfrak{D}_p = \mathfrak{D}(\mathfrak{P}/p) \subset G_{\mathbb{Q}}$ for the decomposition group at p, depending on the choice of a prime $\mathfrak{P}$ over p in $\overline{\mathbb{Q}}$. We may identify $\mathfrak{D}_p$ with the absolute Galois group of the completion $\mathbb{Q}_p$. Suppose that E is an elliptic curve over $\mathbb{Q}$ having height 1 reduction at p. The kernel of reduction $E_1(\overline{\mathbb{Q}}_{\mathfrak{P}})$ admits an action of $\mathfrak{D}_p$, and its Tate module $\mathbb{T}_p(E_1)$ is a free $\mathbb{Z}_p$-module of rank 1. With respect to a generating set for $\mathbb{T}_p(E)$ created by extension from a generator for $\mathbb{T}_p(E_1)$, the action of the inertia group $\mathfrak{I}(\mathfrak{P}/p)$ takes the form

$$\begin{pmatrix} \chi_p & * \\ 0 & 1 \end{pmatrix}, \tag{1}$$

where χ_p is the cyclotomic character giving the action of Galois on p-power roots of unity. Let W_p denote the $\mathfrak{D}_p$-module $\mathbb{T}_p(E_1)$, and write $W_p^{(n)} =$

$E_1[p^n]$ for the nth layer of W_p. In particular, $W_2^{(n)}$ is the special subgroup of $E[2^n]$ over $\mathbb{Q}_2$ which must contain $\operatorname{Ker}\phi_n$ in Greenberg's criterion for $\mu_2(E) \geq n$.

Consider a minimal model for E over $\mathbb{Z}$ in generalized Weierstrass form,

$$E: \quad y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \tag{2}$$

and let E_1 be the kernel of reduction modulo 2. In order that E have height 1 reduction modulo 2, it is necessary and sufficient that the Hasse invariant $a_1 \pmod 2$ not vanish. Indeed, in terms of a parameter z for the formal group associated with E_1, multiplication by 2 is given by

$$[2]z = 2z - a_1z^2 - 2a_2z^3 + \dots$$

(See [5, Chap. IV] for standard formulas.) If a_1 is odd, there is a non-zero solution to $[2]z = 0$ in $\mathbb{Z}_2$, satisfying $z \in 2a_1^{-1} + 8\mathbb{Z}_2$. Furthermore, the x-coordinate of the corresponding point of order 2 has the form

$$x_0 = \frac{1}{z^2} - \frac{a_1}{z} - a_2 + \dots \in -\frac{b_2}{4} + 2\mathbb{Z}_2,$$

where $b_2 = a_1^2 + 4a_2 \equiv 1 \pmod 4$.

Given that a_1 is odd, we may arrange by suitable translation of variables in (2) that $a_3 = 0$, as we now assume. Then the x-coordinates of the points of order 2 are the roots of the cubic on the right side of the model

$$y^2 = x^3 + \frac{b_2}{4}x^2 + a_4x + a_6. \tag{3}$$

Suppose there is in fact a $\mathbb{Q}$-rational point of order 2 with trivial reduction modulo 2. Its abscissa has the form $x_0 = \alpha/4$, with $\alpha \in \mathbb{Z}$ and $\alpha \equiv -1 \pmod 4$. Matching coefficients in the integral factorization

$$4x^3 + b_2x^2 + 4a_4x + 4a_6 = (4x - \alpha)(x^2 + \beta x + \gamma),$$

we find that $\beta, \gamma \in 4\mathbb{Z}$. It follows that by further translation of x if necessary, the model (3) may be brought to the form

$$E: \quad y^2 = (x - a/4)(x^2 - 4b), \tag{4}$$

with $a, b \in \mathbb{Z}$ and $a \equiv -1 \pmod 4$. Although this last model is not integral, it is easily transformed to an integral model by any substitution of the form $y \mapsto y + sx/2$, with s an odd integer. The resulting integral model is minimal at least over $\mathbb{Z}_2$. For odd primes l this model is semistable if and only if l does not divide both a and b. Then the model is also minimal over $\mathbb{Z}_l$. To save space later on, models are given in the form (4), leaving it to the interested reader to transform them to integral models.

3. The archimedean condition. We conform to the notation at the start of Section 2, but with $p = \infty$ and $\mathfrak{P}$ a place of $\overline{\mathbb{Q}}$ over ∞. Denote by τ a generator for the decomposition group $D_\infty = \mathfrak{D}(\mathfrak{P}/\infty) \approx \operatorname{Gal}(\mathbb{C}/\mathbb{R})$.

Consider a model for E in Weierstrass form $y^2 = f(x)$. Because $\tau^2 = 1$ and $\det\tau = -1$, there is a choice of generating set for $\mathbb{T}_2(E)$ with respect to which τ has a matrix representation of the form

$$\tau \sim \begin{pmatrix} -1 & \beta \\ 0 & 1 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z}_2), \tag{5}$$

analogous to (1). Considering $\mathbb{T}_2(E)$ as a $\mathfrak{D}_\infty$-module, let W_∞ be the submodule belonging to the eigenvalue -1. Its nth layer $W_\infty^{(n)}$ is the special subgroup of $E[2^n]$ over $\mathbb{R}$ which must contain $\operatorname{Ker}\phi_n$ in Greenberg's criterion for $\mu_2(E) \geq n$.

LEMMA 1. *The point of order* 2 *in* $W_\infty^{(1)}$ *corresponds to the smallest real root of* $f(x)$.

Proof. Consider the curve $E^{(-1)} : y^2 = -f(-x)$, obtained from E upon twisting by the quadratic character χ_∞. Because $W_\infty(E) \otimes \chi_\infty$ is fixed by τ, the point of order 2 in its first layer is arbitrarily divisible by 2 in $E^{(-1)}(\mathbb{R})$. It therefore lies on the connected component of the identity, and its x-coordinate is the largest real root of $f(-x)$. (Of course this is the only real root when the discriminant Δ_E is negative.) The result follows by twisting back to E. ∎

REMARK. The matrix in (5) can be diagonalized over $\mathbb{Z}_2$ precisely when β is even; that is, when τ acts trivially on $E[2]$. Equivalent conditions are that $f(x)$ have 3 real roots, or that Δ_E be positive. Thus, $\operatorname{sign}(\Delta_E) = (-1)^\beta$. Using this point of view, one may determine the change in sign of discriminant under an $\mathbb{R}$-isogeny of degree 2, say $\phi : E \to E'$. Indeed, $\Delta_{E'}$ is negative if and only if $\Delta_E > 0$ and the x-coordinate of the point of order 2 in $\operatorname{Ker}\phi$ is the middle root of $f(x)$. However, we do not make any further use of this information.

4. Lifting isogenies. Suppose that F and G are elliptic curves defined over a field K of characteristic 0, related by an isogeny $\phi_F : F \to G$ whose kernel is a cyclic group of order p^n, with $n \geq 1$. Let us say that $\phi_E : E \to G$ is a *lift* of ϕ_F if ϕ_E is a cyclic isogeny of degree p^{n+1} defined over K, and there exists an isogeny $\lambda : E \to F$ such that $\phi_E = \phi_F \circ \lambda$.

LEMMA 2. *There is a one-to-one correspondence between pairs* (E, ϕ_E) *such that* E *admits a cyclic isogeny* ϕ_E *of degree* p^{n+1}, *and triples* (F, ϕ_F, γ) *such that* F *admits cyclic isogenies* ϕ_F *and* γ *of degree* p^n *and* p, *respectively*, *with* $\operatorname{Ker}\phi_F \cap \operatorname{Ker}\gamma = 0$. *Under this correspondence* ϕ_E *is the unique lift of* ϕ_F *determined by* γ.

Proof. We briefly describe the correspondence $(E, \phi_E) \leftrightarrow (F, \phi_F, \gamma)$. Given (E, ϕ_E), the isogeny ϕ_E determines a unique isogeny of degree p, say

$\lambda : E \to F$, whose kernel is the subgroup of order p in $\operatorname{Ker}\phi_E$. Take γ to be the dual of λ and ϕ_F to be the isogeny of F whose kernel is $\lambda(\operatorname{Ker}\phi_E)$. Verify that ϕ_E is a lift of ϕ_F and $\operatorname{Ker}\phi_F \cap \operatorname{Ker}\gamma = 0$. Conversely, given (F, ϕ_F, γ), let $\lambda : F \to E$ be the dual of γ and define ϕ_E by $\phi_E = \phi_F \circ \lambda$. Check that $\operatorname{Ker}\phi_E$ is cyclic, using the fact that $\operatorname{Ker}\phi_F \cap \operatorname{Ker}\gamma = 0$. ∎

COROLLARY 1. *A cyclic isogeny $\phi_F : F \to E$ of degree 2^n admits a lift of degree 2^{n+1} if and only if the discriminant Δ_F of the curve F is a square in K. If so, there are precisely two such lifts.*

Proof. The curve F has at least one K-rational point of order 2, namely the one in $\operatorname{Ker}\phi_F$. In order that F admit an isogeny γ of degree 2 such that $\operatorname{Ker}\phi_F \cap \operatorname{Ker}\gamma = 0$, it is necessary and sufficient that all points of order 2 on F be K-rational. Equivalently, Δ_F is a square in K. If so, there are two choices for γ, each of which gives rise to a lift. ∎

Assume now that E is defined over $\mathbb{Q}$, and write $W_l(E)$ for the special submodule of the Tate module of E defined earlier. That is, if $l = p$ is non-archimedean, then E has height 1 reduction at p and $W_p(E) = \mathbb{T}_p(E_1)$, where E_1 is the kernel of reduction; if $l = \infty$, then $W_\infty(E)$ is the -1-eigenspace for the action of complex conjugation on $\mathbb{T}_2(E)$. We use the notation $P_E = \lim P_E^{(j)}$ for an element of $\mathbb{T}_p(E)$ with $P_E^{(j)} \in E[p^j]$ and $pP_E^{(j+1)} = P_E^{(j)}$.

LEMMA 3. *Let ϕ_E be a cyclic isogeny of degree p^{n+1} which is a lift of the isogeny ϕ_F of degree p^n. In the non-archimedean case*, $\operatorname{Ker}\phi_E = W_p^{(n+1)}(E)$ *if and only if* $\operatorname{Ker}\phi_F = W_p^{(n)}(F)$. *In the archimedean case, suppose also that $p = 2$. Then* $\operatorname{Ker}\phi_E = W_\infty^{(n+1)}(E)$ *if and only if* $\operatorname{Ker}\phi_F = W_\infty^{(n)}(F)$.

Proof. First we consider the non-archimedean case. Let λ be the isogeny of degree p dual to γ in the correspondence of Lemma 2. Suppose that $\operatorname{Ker}\phi_E = W_p^{(n+1)}(E)$, and choose a generator $P_E = \lim P_E^{(j)}$ for $W_p(E)$. Then $\operatorname{Ker}\lambda$ is generated by $P_E^{(1)}$. If we define $P_F^{(j)} = \lambda(P_E^{(j+1)})$, then $P_F^{(j)} \in F[p^j]$. Let $P_F = \lim P_F^{(j)} \in \mathbb{T}_p(F)$. Clearly $P_F \in W_p(F)$ because reduction commutes with λ. Thus $\operatorname{Ker}\phi_F = \lambda(\operatorname{Ker}\phi_E) = W_p^{(n)}(F)$.

Assume, conversely, that $\operatorname{Ker}\phi_F = W_p^{(n)}(F)$ and let $P_F = \lim P_F^{(j)}$ generate $W_p(F)$. Define $P_E^{(j)} = \gamma(P_F^{(j)})$. Under the assumption that $\operatorname{Ker}\gamma \cap \operatorname{Ker}\phi_F = 0$, the point $P_E^{(j)}$ has order p^j. Because γ commutes with reduction, we find that $P_E = \lim P_E^{(j)}$ generates $W_p(E)$, as above. But $\operatorname{Ker}\phi_E = \lambda^{-1}(\operatorname{Ker}\phi_F)$ is generated by $\gamma(P_F^{(n+1)}) = P_E^{(n+1)}$, and therefore equals $W_p^{(n+1)}(E)$.

The argument above is easily modified to treat the archimedean case. Note that W_∞ is a submodule of $\mathbb{T}_2$, and that complex conjugation commutes with the isogenies λ and γ. ∎

5. The families. In this section, we arrive at families of semistable elliptic curves defined over $\mathbb{Q}$ whose Selmer groups have non-trivial Iwasawa μ_2-invariant. Proposition 4 below, giving the family with $\mu_2 \geq 1$, is obtained by applying the archimedean condition of Lemma 1 to the family (4), thereby guaranteeing the existence of a point of order 2 which is in the first layer of W_∞ and which is trivial modulo 2.

PROPOSITION 1. *A family of semistable curves defined over* $\mathbb{Q}$, *such that* $\mu_2 \geq 1$, *has the form*

$$D: \quad y^2 = (x - a/4)(x^2 - 4b), \tag{6}$$

with $a, b \in \mathbb{Z}$, $\gcd(a, b) = 1$, $a \equiv -1 \pmod 4$, *and either* $b < 0$, *or else* $b > 0$ *and* $a < -8\sqrt{b}$. *The discriminant of* D *is* $\Delta_D = b(a^2 - 64b)^2$, *and is minimal.*

To create the families with larger μ_2, we construct successive lifts of the isogeny of degree 2 admitted by (6). Let us describe the strategy for constructing these lifts. Suppose given a curve

$$F: \quad y^2 = (x - a_n/4)(x^2 - 4b_n), \tag{7}$$

which admits a cyclic isogeny ϕ_n of degree 2^n satisfying the desired 2-adic and archimedean conditions; namely, $\operatorname{Ker} \phi_n = W_l^{(n)}$ for $l = 2, \infty$. According to Corollary 1, we may lift ϕ_n to an isogeny of degree 2^{n+1} if and only if the discriminant of F is a square. It is equivalent to make b_n a square, which can be done as long as $n \leq 3$. If so, we choose a suitable parametrization for all cases wherein b_n is a square. By a simple modification of the standard formulae for curves related by an isogeny of degree 2 in [5, Chap. III, ex. 4.5], we find an equation for the lifted curve E, as given by the following lemma.

LEMMA 4. *Suppose that* $b_n = \beta^2$ *in the model* (7) *for* F *and let* $\gamma : F \to E$ *be the isogeny of degree* 2 *whose kernel is generated by the point* $(2\beta, 0)$. *Then* E *has a model of the form* $y^2 = (x - a_{n+1}/4)(x^2 - 4b_{n+1})$, *with* $a_{n+1} = a_n - 24\beta$ *and* $b_{n+1} = \beta(8\beta - a_n)$.

The curve E admits an isogeny ϕ_{n+1} which is a lift of ϕ_n and, under the correspondence of Lemma 2, we have $(E, \phi_{n+1}) \leftrightarrow (F, \phi_n, \gamma)$. Replacing β by $-\beta$ provides the companion lift (E', ϕ'_{n+1}) promised by Corollary 1. According to Lemma 3, both (E, ϕ_{n+1}) and (E', ϕ'_{n+1}) fulfill the desired 2-adic and real conditions.

In each of the following families, we assume without further reminder that the parameters are integers. To lift the curve of Proposition 1, we use the parametrization $a = c + 24d$, $b = d^2$ in (6) and apply Lemma 4 to find the isogenous curve.

PROPOSITION 2. *A family of semistable curves C defined over $\mathbb{Q}$, such that $\Delta_C > 0$ and $\mu_2 \geq 2$, has the form*

$$C: \quad y^2 = (x - c/4)(x^2 + 4d(c + 16d)), \tag{8}$$

with $\gcd(c, d) = 1$, $c \equiv -1 \pmod 4$, $d > 0$ *and* $c+32d < 0$. *The discriminant of* C *is* $\Delta_C = -d(c+16d)(c+32d)^4$, *and is minimal. To obtain the companion curve* C', *such that* $\Delta_{C'} < 0$, *change the sign of* d *and replace* c *by* $c + 48d$ *in the model for* C.

An obvious choice of parametrization to make the discriminant of (8) a square is $c = -S^2 - 16T^2, d = T^2$. Applying Lemma 4 yields the isogenous curve

$$y^2 = \left(x + \frac{S^2 + 24ST + 16T^2}{4}\right)(x^2 - 4ST(S + 4T)^2). \tag{9}$$

Its discriminant is $ST(S+4T)^2(S-4T)^8$. A model which perhaps is simpler may be obtained by the further substitution $S = (s + t)/2$, $T = (s - t)/8$.

PROPOSITION 3. *A family of semistable curves B defined over $\mathbb{Q}$, such that $\Delta_B > 0$ and $\mu_2 \geq 3$, has the form*

$$B: \quad y^2 = \left(x - \frac{t^2 - 2s^2}{4}\right)\left(x^2 - \frac{s^2(s^2 - t^2)}{4}\right),$$

with s, t *odd*, $\gcd(s, t) = 1$, $s \equiv t \pmod 8$, *and* $s > t > 0$. *The discriminant of* B *is* $\Delta_B = s^2t^8(s^2 - t^2)/16$, *and is minimal. To obtain the companion curve* B', *such that* $\Delta_{B'} < 0$, *interchange* s *and* t *in the model for* B.

Necessary and sufficient conditions for the discriminant of (9) to be a square are that S and T be squares. The substitution $S = (m + n)^2/4, T = (m - n)^2/16$ seems to yield a nice model for the isogenous curve resulting from Lemma 4.

PROPOSITION 4. *A family of semistable curves A defined over $\mathbb{Q}$, such that $\Delta_A > 0$ and $\mu_2 \geq 4$, has the form*

$$A: \quad y^2 = \left(x - \frac{n^4 - 2m^4}{4}\right)\left(x^2 - \frac{m^4(m^4 - n^4)}{4}\right),$$

with m, n *odd*, $\gcd(m, n) = 1$, $m \equiv n \pmod 4$, *and* $m > n > 0$. *The discriminant of* A *is* $\Delta_A = m^4n^{16}(m^4 - n^4)/16$, *and is minimal. To obtain the companion curve* A', *such that* $\Delta_{A'} < 0$, *interchange* m *and* n *in the model for* A.

6. Mordell–Weil groups. Let $L_1 = \mathbb{C}(a, b)$ be the field of rational functions in two variables, viewed as a parameter space for the curves in Proposition 1. Similarly denote the parameter spaces $L_2 = \mathbb{C}(c, d)$, $L_3 = \mathbb{C}(s, t)$ and $L_4 = \mathbb{C}(m, n)$ for the curves in Propositions 2, 3 and 4 respectively. By construction, each family may be viewed as a subset of the previous family. We then have containments of the corresponding parameter spaces. Indeed, $L_1 \subset L_2$ via the substitution $a = c$, $b = -4d(c + 16d)$; $L_2 \subset L_3$ via the substitution $c = t^2 - 2s^2$, $d = (s^2 - t^2)/16$; and $L_3 \subset L_4$ via the substitution $s = m^2$, $t = n^2$.

PROPOSITION 5. *The Mordell–Weil groups of these curves over their parameter fields are finite, namely*: $D(L_1) \approx C(L_2) \approx \mathbb{Z}/2$ *and* $B(L_3) \approx A(L_4) \approx \mathbb{Z}/4$.

First we determine the 2-power torsion in each of our families. The 2-division field of C is the quadratic extension $L_2(\theta)$, with $\theta^2 = -4d(c+16d)$. According to the Kummer theory of elliptic curves (see [5, Ch. X, Prop. 1.4]), there is an injection

$$\partial : C(L_2)/2C(L_2) \hookrightarrow L_2(\theta)^\times / L_2(\theta)^{\times 2}$$

induced from the map $(x, y) \mapsto x + \theta$ modulo squares. Applying ∂ to the point of order 2 in $C(L_2)$, we have $\partial(c/4, 0) = c + 4\theta$ modulo squares. But it is easy to check that $c + 4\theta$ is not a square in $L_2(\theta)$. Therefore $C(L_2)[2^\infty] \approx \mathbb{Z}/2$. Because C is a form of D over L_2, it also follows that $D(L_1)[2^\infty] \approx \mathbb{Z}/2$. There is a point of order 4, namely $(-s^2/2, st^2 i/4)$ in $B(L_3)$ which propagates to the point $P = (-m^4/2, m^2 n^4 i/4) \in A(L_4)$. Using Kummer theory as above, one checks that P is not twice a point. Therefore, $B(L_3)[2^\infty]$ and $A(L_4)[2^\infty]$ are cyclic groups of order 4.

Let $\alpha = m/n$ and consider the field of rational functions in one variable $K = \mathbb{C}(\alpha)$. We may descend the field of definition for A from L_4 to K via the model

$$y^2 = \left(x - \frac{1 - 2\alpha^4}{4}\right)\left(x^2 - \frac{\alpha^4(\alpha^4 - 1)}{4}\right). \tag{10}$$

In this form, the discriminant of A is $\Delta_A = \alpha^4(\alpha^4 - 1)/16$ and the j-invariant is

$$j_A = \frac{16(16\alpha^8 - 16\alpha^4 + 1)^3}{\alpha^8 - \alpha^4}.$$

To control the rank of $A(K)$, we restate some results of [4] in a convenient form for our applications.

LEMMA 5. *Suppose more generally that K is the function field of transcendence degree 1 over $\mathbb{C}$ belonging to a Riemann surface S of genus g, and that A is an elliptic curve over K with non-constant j-invariant. De-*

note by $\deg j_A$ *the degree of the map* $j_A : S \to \mathbb{P}^1$. *Let* $\mathcal{B}$ *be the set of bad places of* A, *and assume that each bad place is of multiplicative type. Then* $\operatorname{rank} A(K) \le 2g - 2 + |\mathcal{B}| - \frac{1}{6}\deg j_A$.

P r o o f. Let X denote the Neron model of $A_{/K}$, viewed as an elliptic fibration $X \to S$ with general fiber A. Let p_g be the geometric genus of X. Under the assumption that all places of bad reduction are multiplicative, the inequality of [4, Cor. 2.7] gives $\operatorname{rank} A(K) \le 4g-4+|\mathcal{B}|-2p_g$. According to Kodaira's formula [4, (2.10)], we have $12(p_g - g + 1) = \deg j_A$ when all places of bad reduction are multiplicative. Our form of the rank bound easily follows. ∎

For the model (10) over $K = \mathbb{C}(\alpha)$, we have $g = 0$, and $\deg j_A = 24$. The bad places $\mathcal{B} = \{0, \infty, \pm 1, \pm i\}$ are of multiplicative type. Hence $\operatorname{rank} A(K) = 0$.

To study the torsion of odd order in $A(K)$, let G_s denote the group of components of multiplicity one in the fiber X_s over $s \in S$. As a consequence of [4, Prop. 1.6], the exponent of $\bigoplus_{s\in S} G_s$ annihilates the torsion subgroup of $A(K)$. For the model (10), we have $G_s = 0$ if $s \in \{\pm 1, \pm i\}$, $G_\infty = \mathbb{Z}/16$, and $G_0 = \mathbb{Z}/4$. Therefore $A(K)$ has no torsion of odd order.

From the obvious transformation between the models in Proposition 4 and (10), we may conclude that A has no torsion of odd order and rank 0 over the field L_4. In view of the fact that A is a form of the curves B, C, and D over L_4, the latter curves also have no torsion of odd order and rank 0 over L_4. This completes the proof of Proposition 5.

One might reasonably guess that elliptic curves obtained by specialization of the families of Section 5 using integer values of the parameters exhibit whatever the usual phenomena for the rank of elliptic curves over $\mathbb{Q}$ may be. For example, assume that $A_{m,n}$ is an elliptic curve over $\mathbb{Q}$ obtained by fixing $m, n \in \mathbb{Z}$ in the family of Proposition 4. Write $\nu(n)$ for the number of distinct primes dividing the integer n, and $\nu_+(n)$ for the number of distinct primes congruent to 1 modulo 4 dividing n. The sign in the functional equation for the Hasse–Weil L-function of E is $(-1)^{e(m,n)}$ with

$$e(m,n) = 1 + \nu_+(mn) + \nu((m^4 - n^4)/16).$$

It is easy to arrange for the sign to be -1, so that at least conjecturally the rank of $A_{m,n}(\mathbb{Q})$ is odd. An amusing example involving bad reduction at the first few odd primes is the following curve of conductor $3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17$, which occurs for $m = 21, n = 1$:

$$A_{21,1}: \quad y^2 = (x + 388961/4)(x^2 - 4 \cdot 5 \cdot 11 \cdot 13 \cdot 17 \cdot 21^4).$$

Its Mordell–Weil group over $\mathbb{Q}$ has rank 1, generated by the point of order 2 at $x = -388961/4$ and the point of infinite order at $x = 23331751/36$. The 2-primary part of the Tate–Shafarevich group of $A_{21,1}$ over $\mathbb{Q}$ is $\mathbb{Z}/4 \oplus \mathbb{Z}/4$.

References

[1] R. Greenberg, *Iwasawa theory for p-adic representations*, Adv. Stud. Pure Math. 17 (1989), 97–137.
[2] —, *Iwasawa Theory of Elliptic Curves*, Lecture Notes in Math., Springer, New York, to appear.
[3] B. Mazur, *Rational points of abelian varieties with values in towers of number fields*, Invent. Math. 18 (1972), 183–266.
[4] T. Shioda, *On elliptic modular surfaces*, J. Math. Soc. Japan 106 (1972), 20–59.
[5] J. Silverman, *The Arithmetic of Elliptic Curves*, Grad. Texts in Math. 106, Springer, New York, 1986.

Department of Mathematics
Queens College (CUNY)
Flushing, NY 11367
U.S.A.
E-mail: kramer@qcvaxa.qc.edu

Received on 13.10.1998
and in revised form on 25.1.1999 (3478)