Acta Mathematica Sinica, English Series
Jan., 2018, Vol. 34, No. 1, pp. 19–28
Published online: February 6, 2017
https://doi.org/10.1007/s10114-017-6414-x
http://www.ActaMath.com

Acta Mathematica Sinica, English Series
© Springer-Verlag GmbH Germany & The Editorial Office of AMS 2018

Iwasawa Theory of Quadratic Twists of $X_0(49)$

Junhwa CHOI
Department of Mathematics, POSTECH, Pohang, 790-784, *Korea*
E-mail: *jhchoi.math@gmail.com*

John COATES
*Emmanuel College, Cambridge University, Cambridge, CB*2 3*AP, United Kingdom*
E-mail: *jhc*13*@dpmms.cam.ac.uk*

Abstract The field $K = \mathbb{Q}(\sqrt{-7})$ is the only imaginary quadratic field with class number 1, in which the prime 2 splits, and we fix one of the primes $\mathfrak{p}$ of K lying above 2. The modular elliptic curve $X_0(49)$ has complex multiplication by the maximal order $\mathcal{O}$ of K, and we let E be the twist of $X_0(49)$ by the quadratic extension $K(\sqrt{M})/K$, where M is any square free element of $\mathcal{O}$ with $M \equiv 1 \bmod 4$ and $(M, 7) = 1$. In the present note, we use surprisingly simple algebraic arguments to prove a sharp estimate for the rank of the Mordell-Weil group modulo torsion of E over the field $F_\infty = K(E_{\mathfrak{p}^\infty})$, where $E_{\mathfrak{p}^\infty}$ denotes the group of $\mathfrak{p}^\infty$-division points on E. Moreover, writing B for the twist of $X_0(49)$ by $K(\sqrt[4]{-7})/K$, our Iwasawa-theoretic arguments also show that the weak form of the conjecture of Birch and Swinnerton-Dyer implies the non-vanishing at $s = 1$ of the complex L-series of B over every finite layer of the unique $\mathbb{Z}_2$-extension of K unramified outside $\mathfrak{p}$. We hope to give a proof of this last non-vanishing assertion in a subsequent paper.

Keywords Birch–Swinnerton-Dyer conjecture, elliptic curves, Iwasawa theory

MR(2010) Subject Classification 11G05, 11G40, 11R23

1 Introduction

Let A be the modular curve $X_0(49)$. It is an elliptic curve defined over $\mathbb{Q}$, with global minimal generalized Weierstrass equation given by

$$y^2 + xy = x^3 - x^2 - 2x - 1, \tag{1.1}$$

having discriminant -7^3 and j-invariant $-3^3 \cdot 5^3$. This curve has complex multiplication by the full ring of integers $\mathcal{O}$ of the field $K = \mathbb{Q}(\sqrt{-7})$. It has good ordinary reduction at the prime 2, Since 2 splits in K, and we put $2\mathcal{O} = \mathfrak{p}\mathfrak{p}^*$. There are many reasons underlying folklore which regards A as the simplest of all elliptic curves defined over $\mathbb{Q}$ from the arithmetic point of view, and the aim of the present note is to provide further evidence for this. Let $\mathfrak{M}$ denote the set of all non-zero square free elements of $\mathcal{O}$ with $M \equiv 1 \bmod 4$, and $(M, 7) = 1$. In this note, we shall be concerned with the Iwasawa theory at the neglected prime $p = 2$ of the family consisting of all elliptic curves $E = A^{(M)}$, which are quadratic twists of A by quadratic extensions of K of the form $K(\sqrt{M})/K$, with $M \in \mathfrak{M}$. Thus the set $\mathcal{B}(E)$ of primes of bad

Received August 26, 2016, accepted December 6, 2016

reduction for E/K consists of $(\sqrt{-7})$ and the primes of K dividing M. We shall show that one can prove, by simple purely algebraic arguments, a surprisingly strong estimate for the rank of $E(K_\infty)$ modulo torsion over the unique $\mathbb{Z}_2$-extension K_∞ of K unramified outside $\mathfrak{p}$, as well as a vanishing theorem for the Iwasawa μ-invariant of the related Selmer group. We feel that results of this kind are of interest, because again traditional folklore includes a feeling that every major arithmetic phenomena occurring in the family of all elliptic curves defined over a number field probably already occurs in the family of all quadratic twists of any fixed elliptic curve defined over the same number field.

Let $E = A^{(M)}$ for any $M \in \mathfrak{M}$, and write $\psi_{E/K}$ for Deuring's Grossencharacter of E/K. If $\mathfrak{a}$ is any non-zero ideal of $\mathcal{O}$, we write $E_\mathfrak{a}$ for the Galois module of $\mathfrak{a}$-division points on E. We fix any of the primes $\mathfrak{p}$ of K lying above 2, and define $E_{\mathfrak{p}^\infty} = \bigcup_{n\geq 1} E_{\mathfrak{p}^n}$. Also, let $\mathcal{O}_\mathfrak{p} = \mathbb{Z}_2$ be the ring of integers of the completion of K at $\mathfrak{p}$. As above, let K_∞ be the unique $\mathbb{Z}_2$-extension of K unramified outside $\mathfrak{p}$, and define

$$F = K(E_{\mathfrak{p}^2}), \quad F_\infty = F(E_{\mathfrak{p}^\infty}) = FK_\infty, \quad \mathcal{G} = \mathrm{Gal}(F_\infty/K).$$

Since E has good reduction at $\mathfrak{p}$, the theory of complex multiplication shows that the formal group of E at $\mathfrak{p}$ is a Lubin–Tate group over $\mathcal{O}_\mathfrak{p}$ for the local parameter $\psi_{E/K}(\mathfrak{p})$, whence it follows immediately that $\mathfrak{p}$ is totally ramified in F_∞, and that the character $\chi_\mathfrak{p} : \mathcal{G} \to \mathcal{O}_\mathfrak{p}^\times$ giving the action of $\mathcal{G}$ on $E_{\mathfrak{p}^\infty}$ is an isomorphism. In particular, we see that there is also a unique prime of K_∞ above $\mathfrak{p}$. Let R_∞ be the maximal abelian 2-extension of F_∞, which is unramified outside the unique prime of F_∞ lying above $\mathfrak{p}$, and write

$$X_\infty = \mathrm{Gal}(R_\infty/F_\infty).$$

In fact, old work of Wiles and the second author [1] shows that the $\mathfrak{p}^\infty$-Selmer group of E over F_∞ is equal to $\mathrm{Hom}(X_\infty, E_{\mathfrak{p}^\infty})$, and that $E(F_\infty)$ modulo torsion is a finitely generated abelian group. It is easily seen that there are only finitely many primes of F_∞ lying above every prime of K, and we now prove the following more precise result by simple algebraic arguments.

Theorem 1.1 *For all $M \in \mathfrak{M}$, the Galois group $X_\infty = \mathrm{Gal}(R_\infty/F_\infty)$ is a free finitely generated $\mathbb{Z}_2$-module, of rank at most equal to the number of primes of K_∞ dividing M. In particular, the $\mathcal{O}$-rank of $E(F_\infty)$ modulo torsion is at most equal to the number of primes of K_∞ dividing M.*

We first remark that this seems to be the only general assertion about $\mu = 0$ which we know in Iwasawa theory at present, whose proof is not analytic. Note also that, when $E = A$, the theorem shows immediately that $X_\infty = 0$, proving that $A(F_\infty)$ is torsion, and also that $Ш(A/F_\infty)(\mathfrak{p}) = 0$ since the torsion subgroup of X_∞ is zero. In fact, it is easy to see that we must then have $A(F_\infty) = A_{\mathfrak{p}^*} \oplus A_{\mathfrak{p}^\infty}$.

Corollary 1.2 *Assume that M is a non-zero square free rational integer $\equiv 1 \bmod 4$, which is such that every prime factor q of M satisfies*

(i) $q \equiv 3, 5, 6 \bmod 7$, *and*

(ii) $q \equiv 3, 5 \bmod 8$.

Then the $\mathcal{O}$-rank of $E(F_\infty)$ modulo torsion is at most equal to the number of rational prime factors of M.

Indeed, it is a simple exercise in algebraic number theory to verify that, under the hypotheses of the corollary, every rational prime q dividing M is in fact inert in the field K_∞.

Example 1.3 The numerical date given in the following examples has been found using MAGMA. Take $M = 57 = 3 \cdot 19$, and $E = A^{(57)}$. We then have $r_{E/K} = 4$. Now a classical 2-descent shows [2] that $E(\mathbb{Q})$ modulo torsion has $\mathbb{Z}$-rank at most 2. A global minimal Weierstrass equation for E is given by

$$y^2 + xy = x^3 - x^2 - 7107x - 281800,$$

and two independent points of infinite order in $E(\mathbb{Q})$ are

$$P_1 = (424, 8320), \quad P_2 = (1975/4, 84335/8).$$

Thus $E(\mathbb{Q})$ has $\mathbb{Z}$-rank 2. Similarly, if we take $M = 681 = 3 \cdot 227$, and $E = A^{(681)}$, we have $r_{E/K} = 4$. Again a classical 2-descent shows [2] that $E(\mathbb{Q})$ modulo torsion has $\mathbb{Z}$-rank at most 2. A global minimal Weierstrass equation for E is given by

$$y^2 + xy = x^3 - x^2 - 1014477x - 483347656,$$

and we find the following two independent points of infinite order in $E(\mathbb{Q})$.

$$P_1 = (15391912/6561, -53883786916/531441), \quad P_2 = (1634764/1369, -163596026/50653).$$

Thus again $E(\mathbb{Q})$ has $\mathbb{Z}$-rank 2. In both of these examples, the $\mathcal{O}$-rank of $E(K)$ is 2, and $Ш(E/K)(2) = 0$. Moreover, the above corollary then shows that $E(F_\infty)$ modulo torsion also has $\mathcal{O}$-rank 2. In addition, since X_∞ has no non-trivial torsion subgroup, we conclude from the above theorem that $Ш(E/F_\infty)(\mathfrak{p}) = 0$. Finally, we take $M = 741 = 3 \cdot 13 \cdot 19$ and $E = A^{(741)}$. Again we have $r_{E/K} = 4$. A classical 2-descent shows [2] that $E(\mathbb{Q})$ modulo torsion has $\mathbb{Z}$-rank at most 2, and that if the rank is 2, then $Ш(E/\mathbb{Q})(2) = 0$. A global minimal Weierstrass equation for E is given by

$$y^2 + xy + y = x^3 - x^2 - 1201115x - 622717910,$$

and two independent point of infinite order are

$$P_1 = (63754/25, 14034448/125), \quad P_2 = (87385/9, 25525813/27).$$

Hence $E(\mathbb{Q})$ has $\mathbb{Z}$-rank 2, and $Ш(E/\mathbb{Q})(2) = 0$, whence $E(K)$ has $\mathcal{O}$-rank 2, and $Ш(E/K)(2) = 0$. However, since M now has three prime factors which are all inert in K_∞, we can only conclude from the above corollary that the $E(F_\infty)$ has $\mathcal{O}$-rank equal to 2 or 3, and that $Ш(E/F_\infty)(\mathfrak{p})$ is either 0 or a single copy of $\mathbb{Q}_2/\mathbb{Z}_2$. It does not seem easy to decide what is the actual arithmetic data for E over F_∞.

For each $n \geq 0$, let $F_n = K(E_{\mathfrak{p}^{n+2}})$, and let K_n be the unique sub-extension of K_∞/K of degree 2^n over K. It is easily seen that $F_n = FK_n$. Let g_{E/F_n} (resp. g_{E/K_n}) be the $\mathbb{Z}$-rank of $E(F_n)$ (resp. $E(K_n)$) modulo torsion.

Theorem 1.4 *For all $M \in \mathfrak{M}$ and all $n \geq 0$, we have $g_{E/F_n} = g_{E/K_n}$.*

Let $L(E/F_n, s)$ (resp. $L(E/K_n, s)$) be the complex L-series of E/F_n (resp. E/K_n). We denote by r_{E/F_n} (resp. r_{E/K_n}) the order of zero at $s = 1$ of $L(E/F_n, s)$ (resp. $L(E/K_n, s)$). In view of the above theorem and the conjecture of Birch and Swinnerton-Dyer, it is natural to conjecture that $r_{E/F_n} = r_{E/K_n}$ for all $n \geq 0$. At present, we can only prove this for $n = 0$.

Theorem 1.5 *For all $M \in \mathfrak{M}$, we have $r_{E/F} = r_{E/K}$.*

We believe that a further analytic study of the 2-adic Iwasawa theory of E/F_∞ should enable to prove that $r_{E/F_n} = r_{E/K_n}$ for all $n \geq 0$. Of course, it is impossible in our present state of knowledge to hope to be able to prove that $r_{E/F_n} = g_{E/F_n}$ for all $n \geq 0$, even though it is predicted by the conjecture of Birch and Swinnerton-Dyer.

Throughout the rest of this paper, $E = A^{(M)}$ will denote any quadratic twist of A with $M \in \mathfrak{M}$. We recall that $\mathcal{G} = \mathrm{Gal}(F_\infty/K)$, and that the character $\chi_\mathfrak{p}$ defines an isomorphism from $\mathcal{G}$ onto $\mathcal{O}_\mathfrak{p}^\times$. Hence

$$\mathcal{G} = \Delta \times \Gamma. \tag{1.2}$$

Here $\Delta = \mathrm{Gal}(F_\infty/K_\infty)$ is cyclic of order 2 and $\Gamma = \mathrm{Gal}(F_\infty/F)$ is isomorphic to $\mathbb{Z}_2$. Finally, α will always denote the unique square root of -7 such that $\mathfrak{p} = \eta\mathcal{O}$, where $\eta = \frac{1-\alpha}{2}$. We also fix an embedding of K into $\mathbb{C}$.

2 Main Arguments

Lemma 2.1 *E has good reduction everywhere over F.*

Proof The proof is best explained using the Serre–Tate homomorphisms, which are defined in [5]. Let $F_\mathbb{A}^\times$ (resp. $K_\mathbb{A}^\times$) be the idele group of F (resp. K), and let $\epsilon_{E/F}$ (resp. $\epsilon_{E/K}$) be the Serre–Tate homomorphism from $F_\mathbb{A}^\times$ to $K^\times$ (resp. $K_\mathbb{A}^\times$ to $K^\times$), so that $\epsilon_{E/F} = \epsilon_{E/K} \circ N_{F/K}$, where $N_{F/K} : F_\mathbb{A}^\times \to K_\mathbb{A}^\times$ is the norm map. By hypothesis, E has good reduction at all places of F above 2. Let w be any place of F not lying above 2, and let U_w be the group of units of the ring of integers of the completion F_w of F at w. As is shown in [5], E will have good reduction at w if and only if $\epsilon_{E/F}(U_w) = 1$. But $\epsilon_{E/F}(U_w) = \epsilon_{E/K}(J_v)$, where v denotes the place of K below w, and J_v denotes the local norm from F_w to K_v of U_w. Let G_K^{ab} denote the Galois group of the maximal abelian extension of K, and let $\xi_K : K_\mathbb{A}^\times \to G_K^{ab}$ be Artin's global reciprocity map. Note that $\xi_K(J_v)$ fixes F. Since E has complex multiplication, it has potential good reduction at all places of K. Hence, since v does not lie above 2, the criterion of Neron–Ogg–Shafarevich tells us that, for each β in the group of local units at v, we must have that $\chi_\mathfrak{p}(\xi_K(\beta))$ is a root of unity. Now assume that β lies in J_v, so that $\xi_K(\beta)$ fixes F, and thus we must have that $\chi_\mathfrak{p}(\xi_K(\beta))$ belongs to $1 + \pi^2\mathcal{O}_\mathfrak{p}$, where π is a local parameter at $\mathfrak{p}$. But $1 + \pi^2\mathcal{O}_\mathfrak{p}$ contains no non-trivial roots of unity, whence necessarily $\chi_\mathfrak{p}(\xi_K(\beta)) = 1$, which in turn implies that $\xi_K(\beta) = 1$, and the proof that E has good reduction at w is now complete. □

Lemma 2.2 *We have $F = K(\sqrt{-\alpha M})$, where, as above, $\mathfrak{p} = (\frac{1-\alpha}{2})\mathcal{O}$.*

Proof A simple computation shows that $K(A[4]) = K(i, \sqrt{\alpha})$, and $K(A_{\mathfrak{p}^2})/K$ is then the unique quadratic sub-extension in which $\mathfrak{p}$ and $\alpha\mathcal{O}$ are the only ramified primes. Since

$$\mathrm{ord}_{\mathfrak{p}^*}(-\alpha - 1) = 2, \quad \mathrm{ord}_\mathfrak{p}(-\alpha - 1) = 1,$$

we see that $\mathfrak{p}^*$ is unramified, but $\mathfrak{p}$ and $\alpha\mathcal{O}$ are both ramified in the extension $K(\sqrt{-\alpha})/K$. Hence $K(A_{\mathfrak{p}^2}) = K(\sqrt{-\alpha})$. We next note that $F(\sqrt{M}) = K(A_{\mathfrak{p}^2}, \sqrt{M})$, because E is isomorphic to A over the field $K(\sqrt{M})$. Now the biquadratic extension $K(\sqrt{-\alpha}, \sqrt{M})/K$ has three quadratic subfields, namely $K(\sqrt{-\alpha}), K(\sqrt{M}), K(\sqrt{-\alpha M})$, and one of these must be equal to F. However, since E has good reduction everywhere over F, all bad primes of E over K, namely

$\alpha\mathcal{O}$ and the primes of K dividing M, must ramify in F. The only one of the three quadratic subfields with this ramification property is the field $K(\sqrt{\alpha M})$, completing the proof. □

Lemma 2.3 *There are only finitely many primes of F_∞ lying above each prime of K.*

Proof The assertion is clear for $\mathfrak{p}$ since it is totally ramified in F_∞. Let w be any place of F_∞ not lying above $\mathfrak{p}$. It suffices to show that the decomposition group of w in F_∞/F is infinite, since all infinite closed subgroups of $\mathcal{G}$ are of finite index. Now, by the previous lemma, E has good reduction at w, and we write $k_{\infty,w}$ for the residue field of w, and $\widetilde{E}^w$ for the reduction of E modulo w. Then, since w does not divide $\mathfrak{p}$, reduction modulo w injects $E_{\mathfrak{p}^\infty}$ into $\widetilde{E}^w(k_{\infty,w})$. Hence $k_{\infty,w}$ must be infinite, and the proof is complete. □

Lemma 2.4 *The field K_∞ has no non-trivial abelian 2-extension, which is unramified outside the unique prime of K_∞ lying above $\mathfrak{p}$.*

Proof Let J_∞ denote the maximal abelian 2-extension of K_∞, which is unramified outside the unique prime above $\mathfrak{p}$, and let J denote the maximal abelian extension of K contained in J_∞. Now J_∞ is clearly Galois over K, and so $\Gamma = \mathrm{Gal}(K_\infty/K)$ acts on $\mathrm{Gal}(J_\infty/K_\infty)$ in the usual fashion by inner automorphisms. We then have

$$\mathrm{Gal}(J_\infty/K_\infty)_\Gamma = \mathrm{Gal}(J/K_\infty),$$

where the module on the left is the Γ coinvariants of $\mathrm{Gal}(J_\infty/K_\infty)$. But, since K has class number one, K_∞ is the union of the ray class fields of K modulo $\mathfrak{p}^n$ for $n \geq 2$, and so J, being an abelian 2-extension of K which is unramified outside $\mathfrak{p}$, must necessarily be equal to K_∞. Hence the Γ-coinvariants of $\mathrm{Gal}(J_\infty/K_\infty)$ are zero, and so by Nakayama's lemma, $J_\infty = K_\infty$. This completes the proof. □

Recall that R_∞ denotes the maximal abelian 2-extension of F_∞, which is unramified outside the unique prime of F_∞ above $\mathfrak{p}$. It is clear that R_∞ must be Galois over K. Hence $\mathcal{G} = \mathrm{Gal}(F_\infty/K)$ operates on X_∞ in the usual fashion by inner automorphisms. In particular, this defines an action of the cyclic group Δ of order 2 on X_∞. Let $\mathfrak{R} = \mathbb{Z}_2[\Delta]$ denote the $\mathbb{Z}_2$-group ring of Δ, and write $(V)_\Delta$ for the Δ-coinvariants of any $\mathfrak{R}$-module V. Finally, let us write $\mathcal{B}_\infty(M)$ for the number of primes of K_∞ dividing M, and $\mathbb{F}_2$ for the field with 2 elements.

Proposition 2.5 *$(X_\infty)_\Delta$ is a vector space over $\mathbb{F}_2$ of dimension at most $\#(\mathcal{B}_\infty(M))$.*

Proof From the definition of the Δ-action, we have

$$(X_\infty)_\Delta = \mathrm{Gal}(L/F_\infty),$$

where L is the maximal abelian extension of K_∞ contained in R_∞. Since K_∞ has no abelian 2-extension unramified outside the unique prime above $\mathfrak{p}$, $\mathrm{Gal}(L/K_\infty)$ must be generated by the inertia subgroups of the primes of bad reduction of E over K_∞. These bad primes consist of the primes of K_∞ above $\alpha\mathcal{O}$, together with the primes in $\mathcal{B}_\infty(M)$, and the ramification index of each of them in the extension L/K_∞ must be equal to their ramification index in F_∞/K_∞, which is 2. Hence each of the inertia subgroups at bad primes of E over K_∞ is a cyclic group of order 2. Next we note that there is just one prime of K_∞ above $\alpha\mathcal{O}$. Indeed, as remarked earlier, we can choose the sign of α so that $\eta = (1-\alpha)/2$ generates $\mathfrak{p}$, whence $\alpha = 1 - 2\eta$. As $\mathrm{ord}_\mathfrak{p}(2\eta) = 2$, we conclude that for all $n \geq 0$, we have $\mathrm{ord}_\mathfrak{p}(\alpha^{2^n} - 1) = n + 2$, proving that $\alpha\mathcal{O}$ is

inert in K_∞, as claimed. Thus, since $\mathrm{Gal}(F_\infty/K_\infty)$ is of order 2, $\mathrm{Gal}(L/F_\infty)$ must be a vector space over $\mathbb{F}_2$ of dimension at most $\#(\mathcal{B}_\infty(M))$, and the proof of the lemma is complete. □

Corollary 2.6 *X_∞ is a finitely generated $\mathfrak{R}$-module, which is generated by at most $\#(\mathcal{B}_\infty(M))$ elements over $\mathfrak{R}$. In particular, X_∞ is a finitely generated $\mathbb{Z}_2$-module.*

Proof Let δ denote the non-trivial element of Δ. Then $\mathfrak{R}$ is a local ring with maximal ideal $\mathfrak{m} = (2, \delta - 1)$. As X_∞ is a compact $\mathfrak{R}$-module, the corollary follows immediately from Proposition 2.5 and the topological Nakayama lemma. □

Theorem 2.7 *X_∞ is a free $\mathbb{Z}_2$-module, and $X_\infty^\Delta = 0$.*

Proof We have the exact sequence of finitely generated $\mathbb{Z}_2$-modules

$$0 \to X_\infty^\Delta \to X_\infty \to X_\infty \to (X_\infty)_\Delta \to 0,$$

where the middle map is multiplication by $\delta - 1$. Since $(X_\infty)_\Delta$ is finite, it follows that X_∞^Δ must also be finite. But X_∞^Δ is clearly stable under the action of Γ, since Γ and Δ commute. However, it is shown in [3] that X_∞ has no non-zero finite Γ-submodule. Thus we must have $X_\infty^\Delta = 0$. Similarly, Greenberg's theorem shows that the torsion subgroup of X_∞ must be zero, and the proof is complete. □

We are grateful to Romyar Sharifi for pointing out the following lemma to us.

Lemma 2.8 *Let Y be a free $\mathbb{Z}_2 -$ module of finite rank, which is also a Δ-module. Assume that $(Y)_\Delta = (\mathbb{Z}/2\mathbb{Z})^r$ for some integer $r \geq 0$. Then Y is necessarily a free $\mathbb{Z}_2$-module of rank r.*

Proof By Nakayama's lemma, we have a surjection $f : \mathfrak{R}^r \to Y$, which induces a surjection $g : \mathbb{Z}_2^r \to Y_\Delta$. Thus we have the commutative diagram with exact rows

$$\begin{array}{ccccccc}
\mathfrak{R}^r & \longrightarrow & \mathfrak{R}^r & \longrightarrow & \mathbb{Z}_2^r & \longrightarrow & 0 \\
\downarrow & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle g} & & \\
Y & \longrightarrow & Y & \longrightarrow & (Y)_\Delta & \longrightarrow & 0,
\end{array}$$

where the two left horizontal maps are given by multiplication by $\delta - 1$. Let e_i denote the i-th basis vector in $\mathfrak{R}^r$ for $1 \leq i \leq r$, and let $\tilde{e_i}$ denote its image under the upper right horizontal map in this diagram. Put $N = \delta + 1$. Then the upper right horizontal map sends Ne_i to $2\tilde{e_i}$ in $\mathbb{Z}_2^r$, and it is then mapped to zero in $(Y)_\Delta = (\mathbb{Z}_2/2\mathbb{Z}_2)^r$ by the homomorphism g. Hence, by the exactness of the bottom row, we must have $f(Ne_i) = (\delta - 1)d_i$ for some d_i in Y. Put $f(Ne_i) = z_i$. Then, since z_i is fixed by Δ, we have

$$2z_i = Nz_i = (\delta^2 - 1)d_i = 0.$$

But Y has no $\mathbb{Z}_2$-torsion, and so $z_i = 0$ for $1 \leq i \leq r$. Hence the kernel of f must contain $N\mathfrak{R}^r$. Since $\mathfrak{R}^r$ has $\mathbb{Z}_2$ -rank $2r$, it follows that Y has $\mathbb{Z}_2$-rank at most r. But Y must have $\mathbb{Z}_2$-rank at least r, since it maps onto $(\mathbb{Z}_2/2\mathbb{Z}_2)^r$. Thus the $\mathbb{Z}_2$-rank of Y must be exactly equal to r, and the proof is complete. □

Noting Proposition 2.5 and Theorem 2.7, we immediately conclude that

Corollary 2.9 *X_∞ has $\mathbb{Z}_2$-rank at most $\#(\mathcal{B}_\infty)$.*

The proof of Theorem 1.1 is now complete.

We recall that, if L is any algebraic extension of K, then we define

$$\mathrm{Sel}(E/L, E_{\mathfrak{p}^\infty}) = \mathrm{Ker}(H^1(L, E_{\mathfrak{p}^\infty}) \to \prod_v H^1(L_v, E)(\mathfrak{p})),$$

and

$$\mathrm{Sel}'(E/L, E_{\mathfrak{p}^\infty}) = \mathrm{Ker}(H^1(L, E_{\mathfrak{p}^\infty}) \to \prod_{v \nmid \mathfrak{p}} H^1(L_v, E)(\mathfrak{p}));$$

here v runs over all finite places of L in the first definition, and all finite places of L not lying above $\mathfrak{p}$ in the second definition, and, as usual, L_v denotes the compositum of the completions at v of the finite extensions of K contained in L. As mentioned earlier, using the fact that E has good reduction everywhere over $F_\infty = K(E_{\mathfrak{p}^\infty})$, Wiles and the second author proved [1] that

$$\mathrm{Sel}(E/F_\infty, E_{\mathfrak{p}^\infty}) = \mathrm{Sel}'(E/F_\infty, E_{\mathfrak{p}^\infty}) = \mathrm{Hom}(X_\infty, E_{\mathfrak{p}^\infty}). \tag{2.1}$$

Proposition 2.10 *We have* $\mathrm{Sel}'(E/F_\infty, E_{\mathfrak{p}^\infty}) = \mathrm{Sel}'(E/F_\infty, E_{\mathfrak{p}^\infty})^\Delta$.

Proof Let δ be the non-trivial element of Δ. If $f \in \mathrm{Hom}(X_\infty, E_{\mathfrak{p}^\infty})$, we have $(\delta f)(x) = -f(\delta x)$ for all x in X_∞. Hence

$$\mathrm{Sel}'(E/F_\infty, E_{\mathfrak{p}^\infty})^\Delta = \mathrm{Hom}(X_\infty/(1+\delta)X_\infty, E_{\mathfrak{p}^\infty}).$$

But $(1+\delta)X_\infty \subset X_\infty^\Delta$, and this latter group is zero by Theorem 2.7, whence the assertion of the proposition follows. □

Proposition 2.11 *For all $n \geq 0$, the restriction map yields an isomorphism*

$$\mathrm{Sel}'(E/F_n, E_{\mathfrak{p}^\infty}) \simeq \mathrm{Sel}'(E/F_\infty, E_{\mathfrak{p}^\infty})^{\Gamma_n},$$

where $\Gamma_n = \mathrm{Gal}(F_\infty/F_n)$.

Proof We have the commutative diagram with exact rows

$$\begin{array}{ccccccc}
0 & \longrightarrow & \mathrm{Sel}'(E/F_\infty, E_{\mathfrak{p}^\infty})^{\Gamma_n} & \longrightarrow & H^1(F_\infty, E_{\mathfrak{p}^\infty})^{\Gamma_n} & \longrightarrow & \left(\prod_{w \nmid \mathfrak{p}} H^1(F_{\infty,w}, E)(\mathfrak{p})\right)^{\Gamma_n} \\
 & & \uparrow{\scriptstyle \alpha_n} & & \uparrow{\scriptstyle \beta_n} & & \uparrow{\scriptstyle \gamma_n = \prod \gamma_{n,v}} \\
0 & \longrightarrow & \mathrm{Sel}'(E/F_n, E_{\mathfrak{p}^\infty}) & \longrightarrow & H^1(F_n, E_{\mathfrak{p}^\infty}) & \longrightarrow & \prod_{v \nmid \mathfrak{p}} H^1(F_{n,v}, E)(\mathfrak{p}).
\end{array}$$

We first claim that β_n is an isomorphism. Indeed, $\Gamma_n = \mathbb{Z}_p$ has p-cohomological dimension 1, and so $H^2(\Gamma_n, E_{\mathfrak{p}^\infty}) = 0$. Moreover, we claim that

$$H^1(\Gamma_n, E_{\mathfrak{p}^\infty}) = 0. \tag{2.2}$$

Indeed, if τ denotes any topological generator of Γ_n, we have

$$H^1(\Gamma_n, E_{\mathfrak{p}^\infty}) = E_{\mathfrak{p}^\infty}/(\tau - 1)E_{\mathfrak{p}^\infty}.$$

Let $T_{\mathfrak{p}} = \varprojlim E_{\mathfrak{p}^n}$, where the transition maps are multiplication by powers of a generator π of $\mathfrak{p}$, and put $V_{\mathfrak{p}}(E) = T_{\mathfrak{p}}(E) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$. Then we have the exact sequence of Γ-modules

$$0 \longrightarrow T_{\mathfrak{p}}(E) \longrightarrow V_{\mathfrak{p}}(E) \longrightarrow E_{\mathfrak{p}^\infty} \longrightarrow 0\,.$$

Now the endomorphism $\tau - 1$ of the 1-dimensional vector space $V_{\mathfrak{p}}(E)$ must be injective, and so it must also be surjective. But then, by the snake lemma, $\tau - 1$ must also be surjective on

the quotient $E_{\mathfrak{p}^\infty}$ of $V_{\mathfrak{p}}(E)$, proving (2.2). Thus by the inflation restriction sequence, β is an isomorphism.

Note that the extension F_∞/F_n is unramified at all other places v of F_n which do not lie above $\mathfrak{p}$, because E has good reduction everywhere over F. Moreover, by the local inflation-restriction sequence,

$$\ker(\gamma_{n,v}) = H^1(\mathrm{Gal}(F_{\infty,w}/F_{n,v}), E(F_{\infty,w}))(\mathfrak{p}),$$

where $v \nmid \mathfrak{p}$, and w denotes any prime of F_∞ above v. But since E has good reduction at v, and the extension $F_{\infty,w}/F_{n,v}$ is unramified, a standard result about the arithmetic of elliptic curves over local fields shows that

$$H^1(\mathrm{Gal}(F_{\infty,w}/F_{n,v}), E(F_{\infty,w})) = 0.$$

It is therefore clear from the above diagram that γ_n is injective, and so α_n must be an isomorphism, as required. □

Corollary 2.12 *For all $n \geq 0$, we have $\mathrm{Sel}'(E/F_n, E_{\mathfrak{p}^\infty})^\Delta = \mathrm{Sel}'(E/F_n, E_{\mathfrak{p}^\infty})$.*

Theorem 2.13 *For all $n \geq 0$, we have $g_{E/F_n} = g_{E/K_n}$, and the $\mathbb{Z}_2$-corank of $Ш(E/F_n)(\mathfrak{p})$ is equal to the $\mathbb{Z}_2$-corank of $Ш(E/K_n)(\mathfrak{p})$.*

Proof Since $\Delta = \mathrm{Gal}(F_n/K_n)$ is of order 2, one sees easily that the kernel and cokernel of the restriction map

$$r_n : \mathrm{Sel}'(E/K_n, E_{\mathfrak{p}^\infty}) \to \mathrm{Sel}'(E/F_n, E_{\mathfrak{p}^\infty})^\Delta$$

are killed by 2, and hence must be finite. In view of the previous corollary, it follows that

$$\mathbb{Z}_2\text{-corank of } \mathrm{Sel}'(E/K_n, E_{\mathfrak{p}^\infty}) = \mathbb{Z}_2\text{-corank of } \mathrm{Sel}'(E/F_n, E_{\mathfrak{p}^\infty}). \tag{2.3}$$

Now we have the exact sequence

$$0 \to E(K_n) \otimes_{\mathcal{O}} K_{\mathfrak{p}}/\mathcal{O}_{\mathfrak{p}} \to \mathrm{Sel}'(E/K_n, E_{\mathfrak{p}^\infty}) \to Ш'(E/K_n)(\mathfrak{p}) \to 0,$$

where the modified Tate-Shafarevich group is defined by the exactness of the sequence

$$0 \to Ш'(E/K_n) \to H^1(K_n, E) \to \prod_{v \nmid \mathfrak{p}} H^1(K_{n,v}, E).$$

Moreover, there are exactly analogous exact sequences for $\mathrm{Sel}'(E/F_n, E_{\mathfrak{p}^\infty})$. Hence, writing h_{E/K_n} (resp. h_{E/F_n}) for the $\mathbb{Z}_2$-corank of $Ш'(E/K_n)(\mathfrak{p})$ (resp. the $\mathbb{Z}_2$-corank of $Ш'(E/F_n)(\mathfrak{p})$), we conclude from (2.3) that

$$g_{E/K_n} + h_{E/K_n} = g_{E/F_n} + h_{E/F_n}. \tag{2.4}$$

But we have $g_{E/K_n} \leq g_{E/F_n}$, and $h_{E/K_n} \leq h_{E/F_n}$, because the natural maps

$$E(K_n) \otimes_{\mathcal{O}} K_{\mathfrak{p}}/\mathcal{O}_{\mathfrak{p}} \to E(F_n) \otimes_{\mathcal{O}} K_{\mathfrak{p}}/\mathcal{O}_{\mathfrak{p}}, \quad Ш'(E/K_n)(\mathfrak{p}) \to Ш'(E/F_n)(\mathfrak{p})$$

have finite kernels. Hence it follows from (2.4) that $g_{E/K_n} = g_{E/F_n}$ and $h_{E/K_n} = h_{E/F_n}$. The proof of the theorem will then be complete once we have shown that

$$h_{E/K_n} = \mathbb{Z}_2\text{-corank of } Ш(E/K_n)(\mathfrak{p}), \quad h_{E/F_n} = \mathbb{Z}_2\text{-corank of } Ш(E/F_n)(\mathfrak{p}).$$

We give the proof for K_n, and an entirely similar argument works for F_n. Let $\mathfrak{p}_n$ be the unique prime of K_n above $\mathfrak{p}$. Then we have the exact sequence

$$0 \to Ш(E/K_n) \to Ш'(E/K_n) \to H^1(K_{n,\mathfrak{p}_n}, E)(\mathfrak{p}),$$

and so it suffice to show that the group on the extreme right is finite. Let $k_\mathfrak{p}$ denote the residue field of $\mathfrak{p}$, and write $\widetilde{E}$ for the reduction of E modulo $\mathfrak{p}$. Then, since $\mathfrak{p}$ is totally ramified in K_n, Tate local duality shows that $H^1(K_{n,\mathfrak{p}_n}, E)(\mathfrak{p})$ is dual to $\widetilde{E}(k_\mathfrak{p})(\mathfrak{p}*)$, which is clearly a finite group. This completes the proof. □

Finally, we give the proof of Theorem 1.5. Since $F = K(\sqrt{-\alpha M})$, it follows immediately that, for all $M \in \mathfrak{M}$, we have

$$L(E/F, s) = L(E/K, s)L(E^{(-\alpha M)}/K, s), \tag{2.5}$$

where $E^{(-\alpha M)}$ is the quadratic twist of E by the quadratic extension F/K. But, as David Rohrlich remarked to us, since $E = A^{(M)}$, we must have

$$E^{(-\alpha M)} = A^{(-\alpha)}. \tag{2.6}$$

Let $B = A^{(-\alpha)}$, so that B is an elliptic curve defined over K with complex multiplication by the ring $\mathcal{O}$ of integers of K. An explicit equation for B/K is given by

$$y^2 = x^3 + 3\alpha x^2 - 16x.$$

Using either MAGMA, or hand calculations with Tate's algorithm [6], one finds that a global minimal equation for B over K is given by

$$y^2 + \eta xy = x^3 + 2(\eta + 1)x^2 + (3\eta - 2)x, \tag{2.7}$$

where, as always, $\eta = (1-\alpha)/2$. The discriminant of this equation is equal to η^{12}, and of course its j-invariant is equal to $-3^3 \cdot 5^3$. Thus B has bad reduction at the prime $\mathfrak{p}$, and good reduction at all other primes of K. It is then easily seen that the conductor of the Grossencharacter ψ_B of E/K must be $\mathfrak{p}^2$, with ψ_B given explicitly by

$$\psi_B(\mathfrak{c}) = c,$$

where $\mathfrak{c}$ is any integral ideal of K prime to $\mathfrak{p}$, and c is the unique generator of $\mathfrak{c}$ with $c \equiv 1 \bmod \mathfrak{p}^2$. Curiously, this elliptic curve B does not seem to have been noted explicitly in the literature before this. However, it has many interesting properties, which are readily verified. For example, for all $n \geq 0$, we have

$$K_n = K(B_{\mathfrak{p}^{n+2}}).$$

As usual, we write $\overline{\psi_B}$ for the complex conjugate Grossencharacter. By the theory of complex multiplication, we have

$$L(B/K, s) = L(\psi_B, s)L(\overline{\psi_B}, s), \tag{2.8}$$

where the L-series on the right hand side of this equation are the Hecke L-functions of the Grossencharacters ψ_B and $\overline{\psi_B}$. We are very grateful to Tim Dokchitser for computing for us the value of these two Hecke L-functions at the point $s = 1$ using MAGMA.

Theorem 2.14 *We have* $L(\overline{\psi_B}, 1) = 0.5066738035484824\cdots + 0.2287207780578165\cdots \mathrm{i}$, *and obviously* $L(\psi_B, 1)$ *is then equal to the complex conjugate of this value. In particular,* $L(B/K, 1) \neq 0$, *and so* $r_{E/F} = r_{E/K}$ *for all* $M \in \mathfrak{M}$.

We believe that it should be possible to prove, for all $n \geq 0$, that $L(B/K_n, 1) \neq 0$, which would in turn imply that $r_{E/F_n} = r_{E/K_n}$ for all $M \in \mathfrak{M}$, by a suitable 2-adic analytic argument related to Iwasawa theory, and we hope to take up this question in a subsequent paper.

Finally, we note that B/K does indeed satisfy the full Birch–Swinnerton-Dyer conjecture. Indeed, let us define the following period of B

$$\Omega(B) = \Gamma(1/7)\Gamma(2/7)\Gamma(4/7)/(7^{1/4}\zeta_8\overline{\eta}\, 2\pi\sqrt{7}), \tag{2.9}$$

where $7^{1/4}$ denotes the positive real 4-th root of 7 and $\zeta_8 = (1+\mathrm{i})/\sqrt{2}$ denotes a primitive 8-th root of unity. Then, as Tim Dokchitser pointed out to us, MAGMA shows that

$$L(\overline{\psi_B}, 1)/\Omega(B) = \overline{\eta}(\sqrt{7} - \mathrm{i})/16. \tag{2.10}$$

In view of (2.8), it follows that

$$L(B/K, 1)/(\Omega(B)\overline{\Omega(B)}) = 1/16. \tag{2.11}$$

Now we know that $B(K)$ and $Ш(B/K)$ are both finite because $L(B/K, 1) \neq 0$, and a classical 2-descent on B/K shows that $Ш(B/K)(2) = 0$. Moreover, the work of Rubin [4], when combined with (2.11), shows that $Ш(B/K)(p) = 0$ for all odd primes p. On the other hand, the conjecture of Birch and Swinnerton-Dyer asserts that, if we define

$$m_\infty(B) = \Omega(B)\overline{\Omega(B)}\sqrt{7}/2,$$

then we should have

$$L(B/K, 1)/m_\infty(B) = \#(Ш(B/K))c_\mathfrak{p}(B)2/(\sqrt{7}\#(B(K))^2),$$

where $c_\mathfrak{p}(B)$ is the usual Tamagawa number for B at $\mathfrak{p}$. Thus, as $B(K) = B_{\mathfrak{p}^*} \oplus B_{\mathfrak{p}^2}$ and $c_\mathfrak{p}(B) = 4$, we conclude that the conjecture of Birch and Swinnerton-Dyer is indeed valid for B/K.

Acknowledgements The results of this paper grew out of some lectures given by the second author at the National Center for Theoretical Sciences in Taipei, Taiwan, in July 2016, and he wishes to thank Ming-Lun Hsieh and Romyar Sharifi for some very helpful comments made during these lectures.

References

[1] Coates, J.: Infinite descent on elliptic curves with complex multiplication. *Progr. Math.*, **35**, 321–350 (1983)
[2] Coates, J., Li, Y., Tian, Y., et al.: Quadratic twists of elliptic curves. *Proc. London Math. Soc.*, **110**, 357–394 (2015)
[3] Greenberg, R.: On the structure of certain Galois groups. *Invent. Math.*, **47**, 85–99 (1978)
[4] Rubin, K.: The "main conjectures" of Iwasawa theory for imaginary quadratic fields. *Invent. Math.*, **103**, 25–68 (1991)
[5] Serre, J. P., Tate, J.: Good reduction of abelian varieties. *Ann. of Math.*, **88**, 492–517 (1968)
[6] Tate, J.: Algorithm for determining the type of a singular fiber in an elliptic pencil. Modular Functions of One Variable IV, Lecture Notes in Math., **476**, 1975, 33–52