Münster J. of Math. **7** (2014), 83–103
urn:nbn:de:hbz:6-22359594522

Münster Journal of Mathematics

On the 2-part of the Birch–Swinnerton-Dyer conjecture for elliptic curves with complex multiplication

John Coates, Minhyong Kim, Zhibin Liang, and Chunlai Zhao

(Communicated by Christopher Deninger)

To Peter Schneider for his 60th birthday

Abstract. Given an elliptic curve E over $\mathbb{Q}$ with complex multiplication having good reduction at 2, we investigate the 2-adic valuation of the algebraic part of the L-value at 1 for a family of quadratic twists. In particular, we prove a lower bound for this valuation in terms of the Tamagawa number in a form predicted by the conjecture of Birch and Swinnerton-Dyer.

1. Introduction

Let E be an elliptic curve defined over $\mathbb{Q}$, with complex multiplication by the ring of integers of an imaginary quadratic field K. Thus, by the theory of complex multiplication, K must be either $\mathbb{Q}(\sqrt{-1}), \mathbb{Q}(\sqrt{-2}), \mathbb{Q}(\sqrt{-3})$, or one of the fields

$$\mathbb{Q}(\sqrt{-q}) \quad (q = 7, 11, 19, 43, 67, 163). \tag{1}$$

Recently, Y. Tian [7], [8] made the remarkable discovery that one could prove deep results about the arithmetic of certain quadratic twists of E with root number -1, by combining formulae of Gross–Zagier type for these twists, with a weak form of the 2-part of the conjecture of Birch and Swinnerton-Dyer for certain other quadratic twists of E, where the root number is $+1$. We recall that, when the complex L-series of an elliptic curve with complex multiplication does not vanish at $s = 1$, the p-part of the conjecture of Birch and Swinnerton-Dyer has been established, by the methods of Iwasawa theory, for all primes p which do not divide the order of the group of roots of unity of K (see [5]). However, at present we do not know how to extend such methods to cover the case of the prime $p = 2$. Nevertheless, when $K = \mathbb{Q}(\sqrt{-1})$, one of us [10], [11], [12], [13] did establish a weaker result in this direction for the prime $p = 2$, by combining the classical expression for the value of the complex L-series as a sum of Eisenstein series (see Corollary 2.2), with an averaging argument over quadratic twists, and happily this weaker result has sufficed for Tian's work in [7], [8]. The aim of the present note is to show that the rather elementary method developed in the papers [10], [11], [12], [13] works even more simply for quadratic twists of those elliptic curves E having good reduction at the prime 2, and with complex multiplication by the ring of integers of the fields K given by (1). We hope that the results established here will be a first step towards extending the deep results of [7], [8], [9], to certain infinite families of quadratic twists of our curves E, having root number equal to -1. For the curve $E = X_0(49)$, this has now been done in [1] . It is also interesting to note that, in [9], Tian and his collaborators introduce a new and completely different method for establishing weak forms of the 2-part part of the conjecture of Birch and Swinnerton-Dyer for curves with $K = \mathbb{Q}(\sqrt{-1})$, by using a celebrated formula of Waldspurger, and they believe that this new method can eventually be applied to a much wider class of elliptic curves, including those without complex multiplication. Needless to say, the rather elementary methods used here seem to be special to elliptic curves with complex multiplication. Finally, we wish to thank Y. Tian for his ever helpful comments on our work.

2. The averaging argument

Let K be an imaginary quadratic field of class number 1, which we assume is embedded in $\mathbb{C}$, and let $\mathcal{O}_K$ its ring of integers. Let E be any elliptic curve defined over K, whose endomorphism ring is isomorphic to $\mathcal{O}_K$. Fix once and for all a global minimal generalized Weierstrass equation for E over $\mathcal{O}_K$

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \quad (a_i \in \mathcal{O}_K). \tag{2}$$

Let $\mathfrak{L}$ be the period lattice of the Neron differential $dx/(2y + a_1x + a_3)$. Then $\mathfrak{L}$ is a free $\mathcal{O}_K$-module of rank 1, and we fix $\Omega_\infty \in \mathbb{C}^\times$ such that $\mathfrak{L} = \Omega_\infty \mathcal{O}_K$. Denote by ψ_E the Grossencharacter of E/K in the sense of Deuring–Weil, and write $\mathfrak{f}$ for the conductor of ψ_E (thus the prime divisors of $\mathfrak{f}$ are precisely the primes of K where E has bad reduction). Now let $\mathfrak{g}$ be any integral multiple of $\mathfrak{f}$, and fix $g \in \mathcal{O}_K$ such that $\mathfrak{g} = g\mathcal{O}_K$. Let S be the set of primes ideals of K dividing $\mathfrak{g}$, and denote by

$$L_S(\bar{\psi}_E, s) = \sum_{(\mathfrak{a},\mathfrak{g})=1} \frac{\bar{\psi}_E(\mathfrak{a})}{(N\mathfrak{a})^s}$$

the imprimitive Hecke L-function of the complex conjugate Grossencharacter of ψ_E. Our subsequent induction argument is based on the following expression for $L_S(\bar{\psi}_E, s)$, which goes back to the 19th century. Let z and s be complex variables. For any lattice L in the complex plane $\mathbb{C}$, define the Kronecker–Eisenstein series by

$$H_1(z, s, L) := \sum_{w \in L} \frac{\bar{z} + \bar{w}}{|z + w|^{2s}},$$

where the sum is taken over all $w \in L$, except $-z$ if $z \in L$. This series converges to define a holomorphic function of s in the half plane $Re(s) > 3/2$, and it has an analytic continuation to the whole s-plane. Let $\mathfrak{R}$ denote the ray class field of K modulo $\mathfrak{g}$, and let $\mathcal{B}$ be any set of integral ideals of K, prime to $\mathfrak{g}$, whose Artin symbols give precisely the Galois group of $\mathfrak{R}$ over K (in other words, $\mathcal{B}$ is a set of integral ideals of K representing the ray class group of K modulo $\mathfrak{g}$). Since the conductor of ψ_E divides $\mathfrak{g}$, it is well-known that $\mathfrak{R}$ is equal to the field $K(E_g)$, which is obtained by adjoining to K the coordinates of the g-division points on E.

Proposition 2.1. *We have*

$$L_S(\bar{\psi}_E, s) = \frac{|\Omega_\infty/g|^{2s}}{\overline{(\Omega_\infty/g)}} \sum_{\mathfrak{b}\in\mathcal{B}} H_1(\psi_E(\mathfrak{b})\Omega_\infty/g, s, \mathfrak{L}).$$

Proof. As mentioned above $\mathcal{B}$ is a set of integral representatives of the ray class group of K modulo $\mathfrak{g}$, and so it follows that, fixing any generator of each $\mathfrak{b}$ in $\mathcal{B}$, we obtain a set of representatives of $(\mathcal{O}/\mathfrak{g})^*/\tilde{\mu}_K$, where $\tilde{\mu}_K$ denotes the image under reduction modulo $\mathfrak{g}$ of the group μ_K of roots of unity of K. Moreover, the very existence of ψ_E shows that the reduction map from μ_K to $\tilde{\mu}_K$ must be an isomorphism of groups. For each $\mathfrak{b}$ in $\mathcal{B}$, we choose the generator of $\mathfrak{b}$ given by $\psi_E(\mathfrak{b})$. It follows that, as $\mathfrak{b}$ runs over $\mathcal{B}$ and c runs over $\mathfrak{g}$, the principal ideals $(\psi_E(\mathfrak{b}) + c)$ run over all integral ideals of K, prime to $\mathfrak{g}$, precisely once. Thus

$$L_S(\bar{\psi}_E, s) = \sum_{\mathfrak{b}\in\mathcal{B}} \sum_{c\in\mathfrak{g}} \frac{\bar{\psi}_E((\psi_E(\mathfrak{b}) + c))}{|\psi_E(\mathfrak{b}) + c|^{2s}}.$$

Note that, since $c \in \mathfrak{g}$, we have

$$(\psi_E(\mathfrak{b}) + c) = (\psi_E(\mathfrak{b}))(1 + c/\psi_E(\mathfrak{b})) = \mathfrak{b}(1 + c/\psi_E(\mathfrak{b})),$$

so that

$$\psi_E((\psi_E(\mathfrak{b}) + c)) = \psi_E(\mathfrak{b})(1 + c/\psi_E(\mathfrak{b})) = \psi_E(\mathfrak{b}) + c.$$

Hence

$$L_S(\bar{\psi}_E, s) = \sum_{\mathfrak{b}\in\mathcal{B}} \sum_{c\in\mathfrak{g}} \frac{\overline{\psi_E(\mathfrak{b}) + c}}{|\psi_E(\mathfrak{b}) + c|^{2s}},$$

which can easily be rewritten as

$$\frac{|\Omega_\infty/g|^{2s}}{\overline{(\Omega_\infty/g)}} \sum_{\mathfrak{b}\in\mathcal{B}} \sum_{w\in\mathfrak{L}} \frac{\overline{\psi_E \mathfrak{b})\Omega_\infty/g + w}}{|\psi_E(\mathfrak{b})\Omega_\infty/g + w|^{2s}},$$

completing the proof of the proposition. □

We recall that, for any lattice L, the nonholomorphic Eisenstein series $\mathcal{E}_1^*(z, L)$ is defined by

$$\mathcal{E}_1^*(z, L) = H_1(z, 1, L).$$

Then the above proposition immediately implies that

$$L_S(\bar{\psi}_E, 1)/\Omega_\infty = g^{-1} \sum_{\mathfrak{b} \in \mathcal{B}} \mathcal{E}_1^*(\psi_E(\mathfrak{b})\Omega_\infty/g, \mathfrak{L}).$$

Also, it is well-known (see, for example, [3]) that $\mathcal{E}_1^*(\psi_E(\mathfrak{b})\Omega_\infty/g, \mathfrak{L})$ belongs to the field $\mathfrak{R}$, and satisfies

$$\mathcal{E}_1^*(\psi_E(\mathfrak{b})\Omega_\infty/g, \mathfrak{L}) = \mathcal{E}_1^*(\Omega_\infty/g, \mathfrak{L})^{\sigma_{\mathfrak{b}}},$$

where $\sigma_{\mathfrak{b}}$ denotes the Artin symbol of $\mathfrak{b}$ in the Galois group of $\mathfrak{R}$ over K. Thus the above proposition has the following immediate corollary, where $\mathrm{Tr}_{\mathfrak{R}/K}$ denotes the trace map from $\mathfrak{R}$ to K.

Corollary 2.2. *We have*

$$L_S(\bar{\psi}_E, 1)/\Omega_\infty = \mathrm{Tr}_{\mathfrak{R}/K}(g^{-1}\mathcal{E}_1^*(\Omega_\infty/g, \mathfrak{L})).$$

We next consider the twisting of E by certain quadratic extensions of K. A nonzero element M of $\mathcal{O}_K$ is said to be squarefree if it is not divisible by the square of any nonunit element of this ring.

Lemma 2.3. *Let M be any nonzero and nonunit element of $\mathcal{O}_K$, which satisfies (i) M is squarefree, (ii) M is prime to the discriminant of K, and (iii) $M \equiv 1$ mod 4. Then the extension $K(\sqrt{M})/K$ has conductor equal to $M\mathcal{O}_K$.*

Proof. Since M is squarefree and $M \equiv 1$ mod 4, the extension $K(\sqrt{M})/K$ is totally and tamely ramified at all primes dividing M. Thus the assertion of the lemma will follow once we have shown that the primes of K above 2 are not ramified in this extension. Let v be any place of K above 2. Let w be such that $w^2 = M$, and put $z = (w-1)/2$. Then z is a root of the polynomial $f(X) = X^2 - X - (M-1)/4$, so that z is an algebraic integer. But $f'(z) = 2z - 1$ is then clearly a unit at v, and so v is unramified in our extension $K(\sqrt{M})/K$, completing the proof. □

Let M be as in the above lemma, and assume in addition that $(M, \mathfrak{f}) = 1$. We write χ_M for the abelian character of K defining the quadratic extension $K(\sqrt{M})/K$, and let $E^{(M)}$ denote the twist of E by χ_M. Thus $E^{(M)}$ is the unique elliptic curve defined over K, which is isomorphic to E over $K(\sqrt{M})$, and which is such that

$$E^{(M)}(K) = \{P \in E(K(\sqrt{M})) \mid \sigma(P) = \chi_M(\sigma)(P),\ \sigma \in \mathrm{Gal}(K(\sqrt{M})/K)\}.$$

The curve $E^{(M)}$ also has endomorphism ring isomorphic to $\mathcal{O}_K$, and its Grossencharacter, which we denote by $\psi_{E^{(M)}}$, is equal to the product $\psi_E\chi_M$. We write $\mathfrak{f}_M$ for the conductor of $\psi_{E^{(M)}}$. In view of the above lemma, we have $\mathfrak{f}_M = M\mathfrak{f}$, because $(\mathfrak{f}, M) = 1$ and χ_M has conductor $M\mathcal{O}_K$. Finally, putting

$$\mathfrak{p}(z, \mathfrak{L}) = x + (a_1^2 + 4a_2)/12,\ \mathfrak{p}'(z, \mathfrak{L}) = 2y + a_1x + a_3,$$

we obtain a classical Weierstrass equation for E over $\mathbb{C}$ of the form

$$Y^2 = 4X^3 - g_2(\mathfrak{L})X - g_3(\mathfrak{L}),$$

with $X = \mathfrak{p}(z, \mathfrak{L})$, $Y = \mathfrak{p}'(z, \mathfrak{L})$. The corresponding classical Weierstrass equation for $E^{(M)}$ over $\mathbb{C}$ is then given by

$$Y^2 = 4X^3 - M^2 g_2(\mathfrak{L})X - M^3 g_3(\mathfrak{L}).$$

Hence the period lattice for the curve $E^{(M)}$ over $\mathbb{C}$ is given by

$$\mathfrak{L}_M = \frac{\Omega_\infty}{\sqrt{M}} \mathcal{O}_K. \tag{3}$$

We now suppose that we are given a sequence

$$\pi_1, \pi_2, \ldots, \pi_n$$

of $n \geq 0$ distinct prime elements of $\mathcal{O}_K$ (if $n = 0$, we take the empty sequence). We shall say that this sequence is *admissible* for E/K if, for all $1 \leq j \leq n$, we have that π_j is prime to the discriminant of K, and

$$\pi_j \equiv 1 \bmod 4, \quad (\pi_j, \mathfrak{f}) = 1. \tag{4}$$

For each integer $n \geq 0$, define

$$\mathfrak{M}_0 = 1, \ \mathfrak{M}_n = \pi_1 \cdots \pi_n, \ \mathfrak{g}_n = \mathfrak{M}_n \mathfrak{f}. \tag{5}$$

We now take $\mathfrak{R}_n$ to be the ray class field of K modulo $\mathfrak{g}_n$. Since $\pi_j \equiv 1 \bmod 4$, the above lemma shows that the extension $K(\sqrt{\pi_j})/K$ has conductor $\pi_j \mathcal{O}_K$, and so is contained in $\mathfrak{R}_n$, for all j with $1 \leq j \leq n$. Hence the field $\mathfrak{J}_n$ defined by

$$\mathfrak{J}_0 = K, \ \mathfrak{J}_n = K(\sqrt{\pi_1}, \ldots, \sqrt{\pi_n}) \tag{6}$$

is always a subfield of $\mathfrak{R}_n$. Let S_n be the set of prime ideals of K dividing $\mathfrak{g}_n$. Also, writing f for any $\mathcal{O}_K$ generator of the ideal $\mathfrak{f}$, we put $g_n = f\mathfrak{M}_n$, so that $\mathfrak{g}_n = g_n \mathcal{O}_K$. Finally, we define $\mathcal{D}_n$ to be the set of all divisors of $\mathfrak{M}_n$ which are given by the product of any subset of $\{\pi_1, \ldots, \pi_n\}$. The averaging theorem which follows is essentially contained in the earlier paper of one of us [10], and is the basis of all of our subsequent arguments. For simplicity, we write just ψ_M for the Grossencharacter of the curve $E^{(M)}$ for any $M \in \mathcal{D}_n$.

Theorem 2.4. *Let $\{\pi_1, \ldots, \pi_n\}$ be any admissible sequence of $n \geq 0$ elements for E/K. Then we have*

$$\sum_{M \in \mathcal{D}_n} L_{S_n}(\bar{\psi}_M, 1)/\Omega_\infty = 2^n \operatorname{Tr}_{\mathfrak{R}_n/\mathfrak{J}_n}({g_n}^{-1} \mathcal{E}_1^*(\Omega_\infty/g_n, \mathfrak{L})), \tag{7}$$

where $\operatorname{Tr}_{\mathfrak{R}_n/\mathfrak{J}_n}$ denotes the trace map from $\mathfrak{R}_n$ to $\mathfrak{J}_n$.

Proof. When $n = 0$, this is just the formula of Corollary 2.2 with $\mathfrak{g} = \mathfrak{f}$. Thus, assuming $n \geq 1$, let M be any element of $\mathcal{D}_n$. Applying Corollary 2.2 to the curve $E^{(M)}$ with $\mathfrak{g} = \mathfrak{g}_n$, and using (3), we conclude that

$$L_{S_n}(\bar{\psi}_M, 1)\sqrt{M}/\Omega_\infty = \operatorname{Tr}_{\mathfrak{R}_n/K}\left({g_n}^{-1} \mathcal{E}_1^*\Big(\frac{\Omega_\infty}{\sqrt{M} g_n}, \mathfrak{L}_M\Big)\right).$$

Now, for any nonzero complex number λ, we have

$$\mathcal{E}_1^*(z, \mathfrak{L}_M) = \lambda \mathcal{E}_1^*(\lambda z, \lambda \mathfrak{L}_M).$$

Hence, taking $\lambda = \sqrt{M}$, and writing G_n for the Galois group of $\mathfrak{R}_n/K$, we conclude that

$$L_{S_n}(\bar{\psi}_M, 1)/\Omega_\infty = \sum_{\sigma \in G_n} (\sqrt{M})^{\sigma - 1} {g_n}^{-1} (\mathcal{E}_1^*(\Omega_\infty/g_n, \mathfrak{L}))^\sigma. \tag{8}$$

It is now clear that the assertion of the theorem is an immediate consequence of the following lemma. □

Lemma 2.5. *Let* $H_n = \mathrm{Gal}(\mathfrak{R}_n/\mathfrak{J}_n)$. *If* σ *is any element of* G_n, *then* $\sum_{M \in \mathcal{D}_n} (\sqrt{M})^{\sigma - 1}$ *is equal to* 2^n *if* σ *belongs to* H_n, *and is equal to* 0 *otherwise.*

Proof. The first assertion of the lemma is clear. To prove the second assertion, suppose that σ maps $k \geq 1$ elements of the set $\{\sqrt{\pi_1}, \ldots, \sqrt{\pi_n}\}$ to minus themselves, and write $V(\sigma)$ for the subset consisting of all such elements. If M be any element of $\mathcal{D}_n$, it is clear that σ will fix $\sqrt{M}$ if and only if M is a product of an even number of elements of $V(\sigma)$, with an arbitrary number of elements of the complement of $V(\sigma)$ in $\{\sqrt{\pi_1}, \ldots, \sqrt{\pi_n}\}$. Hence the total number of M in $\mathcal{D}_n$ such that σ fixes $\sqrt{M}$ is equal to

$$2^{n-k}((k,0) + (k,2) + (k,4) + \ldots) = 2^{n-1},$$

where (n, r) denotes the number of ways of choosing r objects from a set of n objects. Similarly, the total number of M in $\mathcal{D}_n$ such that σ maps $\sqrt{M}$ to $-\sqrt{M}$ is equal to

$$2^{n-k}((k,1) + (k,3) + (k,5) + \ldots) = 2^{n-1}.$$

Since these last two expressions are equal, the second assertion of the lemma is now clear. □

3. Integrality at 2

We use the notation and hypotheses introduced in the last section. Our aim in this section is to prove the following result.

Theorem 3.1. *Assume that* E *has good reduction at the primes of* K *above 2, and that* $n \geq 0$. *Let* $\{\pi_1, ..., \pi_n\}$ *be any admissible sequence for* E/K. *Define*

$$\Psi_n = \mathrm{Tr}_{\mathfrak{R}_n/\mathfrak{J}_n}\left({g_n}^{-1} \mathcal{E}_1^*\left(\frac{\Omega_\infty}{g_n}, \mathfrak{L}\right)\right).$$

Then $2\Psi_n$ *is always integral at all places of* $\mathfrak{J}_n$ *above 2. Moreover, if the coefficient* a_1 *in* (2) *is divisible by 2 in* $\mathcal{O}_K$, *then* Ψ_n *is integral at all places of* $\mathfrak{J}_n$ *above 2.*

We remark that it is shown in [1] by an additional argument that, provided $n \geq 1$, we always have that Ψ_n is integral at all places of $\mathfrak{J}_n$ above 2, irrespective of whether the coefficient a_1 in (2) is divisible by 2 in $\mathcal{O}_K$ or not.

Before giving the proof of the theorem, we recall some classical identities involving elliptic functions (see for example, [2]). Let L be any lattice in the complex plane, and write $\mathfrak{p}(z, L)$ for the Weierstrass $\mathfrak{p}$-function attached to L. For each integer $m \geq 2$, we define the elliptic function $B_m(z, L)$ by

$$2B_m(z, L) = \frac{\mathfrak{p}''(z, L)}{\mathfrak{p}'(z, L)} + \sum_{k=2}^{k=m-1} \frac{\mathfrak{p}'(kz, L) - \mathfrak{p}'(z, L)}{\mathfrak{p}(kz, L) - \mathfrak{p}(z, L)}.$$

Lemma 3.2. *For all integers $m \geq 2$, we have*

$$B_m(z, L) = \mathcal{E}_1^*(mz, L) - m\mathcal{E}_1^*(z, L).$$

Proof. Let $\zeta(z, L)$ denote the Weierstrass zeta function of L. The following identity is classical

$$\mathcal{E}_1^*(z, L) = \zeta(z, L) - zs_2(L) - \bar{z}A(L)^{-1},$$

(see, for example, Prop. 1.5 of [3], where the definitions of the constants $s_2(L)$ and $A(L)$ are also given). It follows immediately that

$$\mathcal{E}_1^*(mz, L) - m\mathcal{E}_1^*(z, L) = \zeta(mz, L) - m\zeta(z, L).$$

But now we have the addition formula

$$\zeta(z_1 + z_2, L) = \zeta(z_1, L) + \zeta(z_2, L) + \frac{1}{2}\frac{\mathfrak{p}'(z_1, L) - \mathfrak{p}'(z_2, L)}{\mathfrak{p}(z_1, L) - \mathfrak{p}(z_2, L)}.$$

Taking the limit as z_1 tends to z_2, we obtain the statement of the lemma for $m = 2$. For any $m \geq 2$, the above addition formula also shows that

$$\begin{aligned} &\zeta((m+1)z, L) - (m+1)\zeta(z, L) \\ &\qquad\qquad = \zeta(mz, L) - m\zeta(z, L) + \frac{1}{2}\frac{\mathfrak{p}'(mz, L) - \mathfrak{p}'(z, L)}{\mathfrak{p}(mz, L) - \mathfrak{p}(z, L)}, \end{aligned}$$

whence the assertion of the lemma follows by induction on m. □

The next lemma is attributed in [2] to unpublished notes of Swinnerton-Dyer.

Lemma 3.3. *Let w be any complex number such that $w + L$ has exact finite order $m \geq 3$ in $\mathbb{C}/L$. Then $\mathcal{E}_1^*(w, L) = -B_{m-1}(w, L)/m$.*

Proof. By the previous lemma, we have

$$B_{m-1}(w, L) = \mathcal{E}_1^*((m-1)w, L) - (m-1)\mathcal{E}_1^*(w, L).$$

But, as a function of z, $\mathcal{E}_1^*(z, L)$ is periodic with respect to L and odd, whence it follows that $\mathcal{E}_1^*((m-1)w, L) = -\mathcal{E}_1^*(w, L)$. This completes the proof. □

Now we have the addition formula

$$\begin{aligned} &\mathfrak{p}(z_1 + z_2, L) + \mathfrak{p}(z_1, L) + \mathfrak{p}(z_2, L) \\ &\qquad\qquad = \frac{1}{4}((\mathfrak{p}'(z_1, L) - \mathfrak{p}'(z_2, L))/(\mathfrak{p}(z_1, L) - \mathfrak{p}(z_2, L)))^2, \end{aligned}$$

whence we immediately obtain the following corollary.

Corollary 3.4. *Let w be any complex number such that $w+L$ has exact finite order $m \geq 3$ in $\mathbb{C}/L$. Then we have*

$$m\mathcal{E}_1^*(w,L) = \sum_{k=1}^{k=m-2} (\mathfrak{p}((k+1)w,L) + \mathfrak{p}(kw,L) + \mathfrak{p}(w,L))^{1/2},$$

for an appropriate choice of the square root in each case.

We can now give the proof of Theorem 3.1. Recall that the period lattice of the Neron differential of our fixed global minimal Weierstrass equation (2) is $\mathfrak{L} = \Omega_\infty \mathcal{O}_K$. Take $w = \psi(\mathfrak{b})\Omega_\infty/g_n$, where $\mathfrak{b}$ is any fixed integral ideal of K prime to $\mathfrak{g}_n$. Thus $\mathcal{E}_1^*(w,\mathfrak{L})$ is any one of the conjugates of $\mathcal{E}_1^*(\Omega_\infty/g_n,\mathfrak{L})$ over K. Let m be the smallest positive rational integer lying in the ideal $\mathfrak{g}_n$, so that m is also the smallest positive rational integer with the property that mw lies in $\mathfrak{L}$. Moreover, since E has good reduction at the primes of K above 2, the ideal $\mathfrak{f}$ is not divisible by any prime of K above 2. This means that the smallest positive rational integer in the ideal $\mathfrak{g}_n$ must be odd. It follows that m is odd, and it must then be > 2. Let P be the point on E defined by w. Then we have

$$\mathfrak{p}(rw,\mathfrak{L}) = x(rP) + (a_1^2 + 4a_2)/12, \ (r = 1, ..., m-1). \tag{9}$$

But, as E has good reduction at all primes of K above 2 and the point rP has odd order, it follows that $x(rP)$ is integral at each prime of $\mathfrak{R}_n$ above 2. Thus we can immediately conclude from Corollary 3.4 and (9) that the following two assertions. Firstly, if $a_1/2$ lies in $\mathcal{O}_K$, then every conjugate of $\mathcal{E}_1^*(\Omega_\infty/g_n,\mathfrak{L})$ over K is integral at all places of $\mathfrak{R}_n$ above 2. In general, if we drop the assumption that $a_1/2$ lies in $\mathcal{O}_K$, all we can say with the above argument is that every conjugate of $2\mathcal{E}_1^*(\Omega_\infty/g_n,\mathfrak{L})$ over K is integral at every place of $\mathfrak{R}_n$ above 2. Taken together, these two assertions clearly imply Theorem 3.1. □.

If v denotes any place of the algebraic closure of $\mathbb{Q}$ above 2, we denote the associated order valuation by ord_v, and we always normalize it so that $\mathrm{ord}_v(2) = 1$. Applying the above theorem in the special case $n = 0$, we immediately obtain:

Corollary 3.5. *Assume that E has good reduction at the primes of K above 2. Then, for all places v of K above 2, we have*

$$\mathrm{ord}_v(L(\bar{\psi}_E, 1)/\Omega_\infty) \geq -1.$$

Moreover, if 2 divides a_1 in $\mathcal{O}_K$, then

$$\mathrm{ord}_v(L(\bar{\psi}_E, 1)/\Omega_\infty) \geq 0.$$

4. The induction argument

Let E be an elliptic curve defined over K, with complex multiplication by the ring of integers of K, and global minimal Weierstrass equation given by (2). We always assume that E has good reduction at the primes of K above 2. We fix once and for all any place v of the algebraic closure of $\mathbb{Q}$ above 2, and write ord_v for the order valuation at this place, normalized so that $\mathrm{ord}_v(2) = 1$. Define ϕ_E to be 0 or 1, according as 2 does or does not divide a_1 in $\mathcal{O}_K$, where we recall that a_1 is the coefficient of xy in the equation (2). We assume now that $n \geq 1$, and let any admissible sequence $\{\pi_1, ..., \pi_n\}$ for E/K. As before, we define $\mathfrak{M}_n = \pi_1 \dots \pi_n$, and write

$$L^{(\mathrm{alg})}(\bar{\psi}_{\mathfrak{M}_n}, 1) = L(\bar{\psi}_{\mathfrak{M}_n}, 1)\sqrt{\mathfrak{M}_n}/\Omega_\infty, \tag{10}$$

which is an element of K. Our goal in this section is to prove the following theorem.

Theorem 4.1. *Assume that $K \neq \mathbb{Q}(\sqrt{-1})$, $\mathbb{Q}(\sqrt{-3})$, and that E has good reduction at all places of K above 2. Then, for all $n \geq 1$, and all admissible sequences $\{\pi_1, ..., \pi_n\}$ for E/K, we have*

$$\mathrm{ord}_v(L^{(alg)}(\bar{\psi}_{\mathfrak{M}_n}, 1)) \geq n - \phi_E. \tag{11}$$

Proof. We shall prove the theorem by induction on n, and we begin with an obvious remark. Let r be any integer ≥ 0, and recall that $\psi_{\mathfrak{M}_r}$ denotes the Grossencharacter of the twisted curve $E^{(\mathfrak{M}_r)}$. For each $n > r$, write $\mathfrak{p}_n = \pi_n \mathcal{O}_K$. Then $\mathfrak{p}_n$ is prime to the conductor of $\psi_{\mathfrak{M}_r}$, and we have

$$\mathrm{ord}_v(1 - \bar{\psi}_{\mathfrak{M}_r}(\mathfrak{p}_n)/N\mathfrak{p}_n) \geq 1. \tag{12}$$

Indeed, we have $\psi_{\mathfrak{M}_r}(\mathfrak{p}_n) = \zeta\pi_n$, where $\zeta = 1$ or -1 because $K \neq \mathbb{Q}(\sqrt{-1})$, $\mathbb{Q}(\sqrt{-3})$. Thus $\zeta \equiv 1 \bmod 2$, and (12) then follows easily because $\pi_n \equiv 1 \bmod 4$ and $N\mathfrak{p}_n = \psi_{\mathfrak{M}_r}(\mathfrak{p}_n)\bar{\psi}_{\mathfrak{M}_r}(\mathfrak{p}_n)$. Note also that, on combining Theorems 3.1 and 2.4, we conclude that, for all integers $n \geq 1$, we have

$$\mathrm{ord}_v\left(\sum_{M \in \mathcal{D}_n} L_{S_n}(\bar{\psi}_M, 1)/\Omega_\infty\right) \geq n - \phi_E. \tag{13}$$

It is clear that, on combining (12) for $r = 0$ and (13) for $n = 1$, we immediately obtain (11) for $n = 1$. Suppose now that $n > 1$, and that (11) has been proven for all integers strictly less than n. Combining this inductive hypothesis with assertion (12), we conclude that for all proper divisors M of $\mathfrak{M}_n$, we have

$$\mathrm{ord}_v(L_{S_n}(\bar{\psi}_M, 1)/\Omega_\infty) \geq n - \phi_E,$$

whence (13) again shows that (11) holds for the integer n. This completes the proof of the theorem. □

We next investigate which rational primes p split in K, and have the additional property that they can be written as $p = \pi\pi^*$, with π in $\mathcal{O}_K$ satisfying $\pi \equiv 1 \bmod 4$ (and thus automatically also satisfying $\pi^* \equiv 1 \bmod 4$). We call primes p with this property *special* split primes for K. Obviously, a necessary condition for p to be a special split prime for K is that $p \equiv 1 \bmod 4$. We remark that it is clear from the Chebotarev density theorem that there are always infinitely many special split primes for K.

Lemma 4.2. *Assume that $K \neq \mathbb{Q}(\sqrt{-1})$, $\mathbb{Q}(\sqrt{-2})$, $\mathbb{Q}(\sqrt{-3})$. Let p be any rational prime which splits in K, and which satisfies $p \equiv 1 \bmod 4$. If $K = \mathbb{Q}(\sqrt{-7})$, then p is always a special split prime for K. If $K = \mathbb{Q}(\sqrt{-q})$, where $q = 11, 19, 43, 67, 163$, then such a p is a special split prime for K if and only if we can write $p = \pi\pi^*$ in $\mathcal{O}_K$ with $\pi + \pi^* \equiv 0 \bmod 2$.*

Proof. Let $K = \mathbb{Q}(\sqrt{-q})$, and put $\tau = (1+\sqrt{-q})/2$, so that $1, \tau$ form an integral basis of $\mathcal{O}_K$. Assume first that $K = \mathbb{Q}(\sqrt{-7})$. Then $p = a^2 + ab + 2b^2$, with a an odd integer, whose sign can be chosen so that $a \equiv 1 \bmod 4$, and with b an even integer, which has necessarily to be divisible by 4 since $p \equiv 1 \bmod 4$. We then clearly have that $\pi = a + b\tau$ satisfies $\pi \equiv 1 \bmod 4$. Finally, assume that $K = \mathbb{Q}(\sqrt{-q})$, where q is any of $11, 19, 43, 67, 163$. Then $p = a^2+ab+mb^2$, where a and b are integers, and $m = (q+1)/4$ is now an odd integer. Since $p \equiv 1 \bmod 4$, we see that $\pi = a + b\tau$ satisfies $\pi \equiv 1 \bmod 4$ if and only if $a \equiv 1 \bmod 4$ and b is even. But $\pi + \pi^* = 2a + b$, and so $\pi + \pi^*$ will be even if and only if b is even. By if b is even, then a is odd, and then we can always choose the sign of a so that $a \equiv 1 \bmod 4$. This completes the proof. □

Now assume that our elliptic curve E is in fact defined over $\mathbb{Q}$, and take (2) to be a global minimal Weierstrass equation for E over $\mathbb{Q}$. Then the conductor $N(E)$ of E is given by

$$N(E) = d_K N\mathfrak{f},$$

where d_K denotes the absolute value of the discriminant of K. Moreover, the complex L-series $L(E,s)$ of E over $\mathbb{Q}$ coincides with the Hecke L-series $L(\bar{\psi}_E, s)$. If R is a nonzero squarefree integer, $E^{(R)}$ will now denote the twist of E by the extension $\mathbb{Q}(\sqrt{R})/\mathbb{Q}$. Write

$$L^{(\mathrm{alg})}(E^{(R)}, 1) = L(E^{(R)}, 1)\sqrt{R}/\Omega_\infty. \tag{14}$$

Finally, ϕ_E has the same definition as earlier.

Lemma 4.3. *Assume that E is defined over $\mathbb{Q}$, and has complex multiplication by the ring of integers of any of the fields $K = \mathbb{Q}(\sqrt{-q})$, where $q = 7, 11, 19, 43, 67, 163$. Suppose further that E has good reduction at 2. Then the conductor $N(E)$ of E is a square.*

Proof. Let p be any prime dividing $N(E)$. Since E has potential good reduction at p, we must have that p^2 exactly divides $N(E)$ whenever $p > 3$. Also $p \neq 2$, because E has good reduction at 2. Thus we only have to check that an even power of 3 must divide $N(E)$. But, since $q > 3$, it is well-known (see [4]) that E is the quadratic twist of an elliptic curve of conductor q^2, whence it follows immediately that either 3 does not divide $N(E)$, or 3^2 exactly divides $N(E)$, according as 3 does not, or does, divide the discriminant of the twisting quadratic extension. This completes the proof. □

We now introduce a definition which for the moment is motivated by what is needed to deduce the next theorem from our earlier induction argument (but see also the connexion with Tamagawa factors discussed in the next section).

Write w for the sign in the functional equation of $L(E,s)$. We continue to assume that E is defined over $\mathbb{Q}$, and satisfies the hypotheses of Lemma 4.3. If D is any squarefree integer which is prime to $N(E)$, it is well-known that the root number of the twist $E^{(D)}$ of E by the quadratic extension $\mathbb{Q}(\sqrt{D})/\mathbb{Q}$ is given by $\chi_D(-N(E))w$, where χ_D denotes the Dirichlet character of this quadratic extension. Thus, in view of Lemma 4.3, we are led to make the following definition.

Definition 4.4. Assume that E satisfies the hypotheses of Lemma 4.3. A squarefree positive integer M is said to be *admissible* for E if it satisfies (i) $(M, N(E)) = 1$, (ii) $M \equiv 1 \bmod 4$ or $M \equiv 3 \bmod 4$, according as $w = +1$ or $w = -1$, and (iii) every prime factor of M which splits in K is a special split prime for K.

Theorem 4.5. *Assume that E is defined over $\mathbb{Q}$, has complex multiplication by the ring of integers of $K = \mathbb{Q}(\sqrt{-q})$, where $q = 7, 11, 19, 43, 67, 163$, and has good reduction at 2. Let M be a squarefree positive integer, which is admissible for E, and let $r(M)$ denote the number of primes of K dividing M. Then we have*

$$\operatorname{ord}_2(L^{(alg)}(E^{(wM)},1)) \geq r(M) - \phi_E, \tag{15}$$

where w denotes the sign in the functional equation of $L(E,s)$.

Proof. Let M be any squarefree integer which is admissible for E, and let p be any prime dividing M. If p is inert in K, define π to be p or $-p$, according as p is congruent to 1 or 3 mod 4. If p splits in K, then Lemma 4.2 shows that we can then write $p = \pi\pi^*$, where π and π^* are elements of $\mathcal{O}_K$, which are both congruent to 1 mod 4. Since every p with $p \equiv 3 \bmod 4$, and p dividing M, is inert in K, it is now clear that we can write

$$wM = \pi_1 \ldots \pi_{r(M)},$$

where the π_i are distinct prime elements of $\mathcal{O}_K$, which are all congruent to 1 mod 4, and which are also prime to $\mathfrak{f}$ and the discriminant of K. Hence the above theorem is an immediate consequence of Theorem 4.1. □

The following is an immediate corollary of the above theorem. Of course, the hypothesis made in the corollary that $L(E,1) \neq 0$ implies that the root number $w = 1$, and so the admissible M in this case are $\equiv 1 \bmod 4$.

Corollary 4.6. *Assume that E is defined over $\mathbb{Q}$, has complex multiplication by the ring of integers of K, and has good reduction at 2. Suppose further that we have (i) $K \neq \mathbb{Q}(\sqrt{-3})$, and (ii) $\operatorname{ord}_2(L^{(alg)}(E,1)) = -1$. Let M be any squarefree positive integer which is admissible for E, and which is divisible only by rational primes which split in K. Then*

$$\operatorname{ord}_2\left(\frac{L^{(alg)}(E^{(M)},1)}{L^{(alg)}(E,1)}\right) \geq 2k(M),$$

where $k(M)$ denotes the number of rational primes dividing M.

We now discuss some numerical examples of this theorem. For basic information about the curves discussed below, see, for example, [4]. As a first example, let E be the elliptic curve defined by

$$y^2 + xy = x^3 - x^2 - 2x - 1. \tag{16}$$

It has conductor 49, and complex multiplication by the ring of integers of $K = \mathbb{Q}(\sqrt{-7})$. In fact, this curve is isomorphic to the modular curve $X_0(49)$. By the Chowla–Selberg formula, the period lattice $\mathfrak{L}$ of the Neron differential on E is given by $\mathfrak{L} = \Omega_\infty \mathcal{O}_K$, where

$$\Omega_\infty = \frac{\Gamma(\frac{1}{7})\Gamma(\frac{2}{7})\Gamma(\frac{4}{7})}{2\pi i\sqrt{-7}}.$$

Moreover, $\phi_E = 1$ because $a_1 = 1$, and $L^{(\mathrm{alg})}(E, 1) = 1/2$. We remark that this elliptic curve, and the three other elliptic curves defined over $\mathbb{Q}$ of conductor 49, seem to be the only examples of such curves with complex multiplication, good reduction at 2, and $\mathrm{ord}_2(L^{(\mathrm{alg})}(E, 1)) < 0$. Note that any positive squarefree integer M with $(M, 7) = 1$ and $M \equiv 1 \bmod 4$, will be admissible for E, provided each of its prime factors which splits in K (thus a prime factor which is congruent to any of 1, 2, or 4 mod 7) is congruent to 1 mod 4. Theorem 4.5 therefore implies that, for such admissible integers M, we have

$$\mathrm{ord}_2(L^{(\mathrm{alg})}(E^{(M)}, 1)) \geq r(M) - 1. \tag{17}$$

We see from Table I at the end of this paper that this estimate is in general best possible.

As a second example, take for E the elliptic curve defined by

$$y^2 + y = x^3 - x^2 - 7x + 10. \tag{18}$$

It has conductor 121, and complex multiplication by the ring of integers of $K = \mathbb{Q}(\sqrt{-11})$. Again by the Chowla–Selberg formula, the period lattice $\mathfrak{L}$ of the Neron differential on E is given by $\mathfrak{L} = \Omega_\infty \mathcal{O}_K$, where

$$\Omega_\infty = \frac{\Gamma(\frac{1}{11})\Gamma(\frac{3}{11})\Gamma(\frac{4}{11})\Gamma(\frac{5}{11})\Gamma(\frac{9}{11})}{2\pi i\sqrt{-11}}.$$

Moreover, $\phi_E = 0$ because $a_1 = 0$, and $w = -1$. The split primes for K are those which are congruent to $1, 3, 4, 5, 9 \bmod 11$. The special split primes for K are much rarer. For example, all special split primes < 1000 for this curve are:

$$53, 257, 269, 397, 401, 421, 617, 757, 773, 929.$$

Let now M be any squarefree positive integer which is admissible for E (in particular, since we are only interested in twists $E^{(-M)}$ having root number equal to $+1$, we assume that $M \equiv 3 \bmod 4$ and $(M, 11) = 1$). Then Theorem 4.5 implies that

$$\mathrm{ord}_2(L^{(\mathrm{alg})}(E^{(-M)}, 1)) \geq r(M). \tag{19}$$

However, in this example, Table II at the end of this paper suggests that this estimate is not, in general, best possible. It seems plausible to speculate from Table II that the lower bound of (19) could be improved to $r(M) + 1$.

5. Tamagawa factors

Our goal in this last section is to relate the estimate given by Theorem 4.5 to the Tamagawa factors which arise in the Birch–Swinnerton-Dyer conjecture for the twists of our given elliptic curve with complex multiplication. We assume at first that E is any elliptic curve defined over $\mathbb{Q}$ and that p is any prime of bad reduction for E. Let $E(\mathbb{Q}_p)$ denote the group of points on E with coordinates in the field of p-adic numbers $\mathbb{Q}_p$, and $E_0(\mathbb{Q}_p)$ the subgroup of points with nonsingular reduction modulo p. We define

$$\mathfrak{C}_p(E) = E(\mathbb{Q}_p)/E_0(\mathbb{Q}_p),$$

and recall that the Tamagawa factor $c_p(E)$ is defined by

$$c_p(E) = [E(\mathbb{Q}_p) : E_0(\mathbb{Q}_p)]. \tag{20}$$

If A is any abelian group, $A[m]$ will denote the kernel of multiplication by a positive integer m on A. The following lemma is very well-known, but we give it for completeness.

Lemma 5.1. *Let E be any elliptic curve over $\mathbb{Q}$, and let p be a prime number where E has bad additive reduction. Then, for all positive integers m with $(m, p) = 1$, we have*

$$\mathfrak{C}_p(E)[m] = E(\mathbb{Q}_p)[m].$$

Proof. Let $E_1(\mathbb{Q}_p)$ denote the group of points on the formal group of E at p. Since E has additive reduction modulo p, the group of nonsingular points on the reduction of E modulo p is isomorphic to the additive group of the field $\mathbb{F}_p$. As $E_1(\mathbb{Q}_p)$ is pro-p, and we have the exact sequence

$$0 \to E_1(\mathbb{Q}_p) \to E_0(\mathbb{Q}_p) \to \mathbb{F}_p \to 0,$$

it follows immediately that multiplication by m is an isomorphism on $E_0(\mathbb{Q}_p)$, whence the assertion of the lemma follows easily from a simple application of the snake lemma to the sequence

$$0 \to E_0(\mathbb{Q}_p) \to E(\mathbb{Q}_p) \to \mathfrak{C}_p(E) \to 0.$$

□

Lemma 5.2. *Let E be any elliptic curve defined over $\mathbb{Q}$, and let R be an odd squarefree integer such that $(R, N(E)) = 1$. Then, for all primes p dividing R, we have*

$$\mathrm{ord}_2(c_p(E^{(R)})) = \mathrm{ord}_2(\#(E(\mathbb{Q}_p)[2])).$$

In particular, the left hand side of this equation depends only on E and p, and not on the integer R.

Proof. Since the j-invariant of $E^{(R)}$ is integral at p, it follows from the usual table of reduction types (see [6, p.365]) that the 2-primary subgroup of $\mathfrak{C}_p(E^{(R)})$ is one of the groups three 0, $\mathbb{Z}/2\mathbb{Z}$, or $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2Z$. Moreover, $E^{(R)}$ has bad additive reduction at p, and p is odd because R is odd. Hence, by the previous lemma

$$\mathrm{ord}_2(c_p(E^{(R)})) = \mathrm{ord}_2(\#(E^{(R)}(\mathbb{Q}_p)[2])).$$

But clearly $E^{(R)}(\mathbb{Q}_p)[2] = E(\mathbb{Q}_p)[2]$, and the proof of the lemma is complete. □

Lemma 5.3. *Let E be any elliptic curve defined over $\mathbb{Q}$, and let R be an odd squarefree integer such that $(R, N(E)) = 1$. Let p be any prime dividing R. Assume first that E has supersingular reduction at p and that $p > 3$. Then* $\mathrm{ord}_2(c_p(E^{(R)})) = 1$ *or* 2*, and it is equal to 1 when $p \equiv 1 \bmod 4$. Assume next that E has good ordinary reduction at p, and let t_p be the trace of the Frobenius endomorphism at p. Then* $\mathrm{ord}_2(c_p(E^{(R)})) = 0$ *if t_p is odd, and* $\mathrm{ord}_2(c_p(E^{(R)})) = 1$ *or* 2 *when t_p is even.*

Proof. As p is odd and is a prime of good reduction for E, reduction modulo p defines an isomorphism

$$E(\mathbb{Q}_p)[2] = \tilde{E}(\mathbb{F}_p)[2], \tag{21}$$

where $\tilde{E}$ denotes the reduction of E modulo p. Granted Lemma 5.2, the assertions of the present lemma then follow immediately from (21) and the following observations. The group $\tilde{E}(\mathbb{F}_p)$ has cardinality $A_p = p+1-t_p$, where t_p is the trace of the Frobenius endomorphism of $\tilde{E}$. If E has supersingular reduction at p, then $t_p = 0$ because we assume that $p > 3$ in this case. If E has ordinary reduction at p, we see that A_p is odd when t_p is odd, and A_p is even when t_p is even. □

The next lemma shows that one can strengthen these general results a little if the curve E has complex multiplication.

Lemma 5.4. *Assume that E is an elliptic curve defined over $\mathbb{Q}$, with good reduction at 2, and having complex multiplication by the maximal order of an imaginary quadratic field K. Let R be a squarefree integer with $(R, N(E)) = 1$. If p is any prime dividing $N(E)$, then* $\mathrm{ord}_2(c_p(E)) = \mathrm{ord}_2(c_p(E^{(R)}))$*. If p is any prime dividing R, and E has ordinary reduction at p, then* $\mathrm{ord}_2(c_p(E^{(R)}))$ $= 2$ *whenever the trace of the Frobenius endomorphism of E at p is even.*

Proof. If p is any prime dividing $N(E)$, then p is odd because E has good reduction at 2, and the j-invariant of E is integral at p because E has complex multiplication, and thus E must have additive reduction at p. The same statements are also true when we replace E by $E^{(R)}$ because $(R, N(E)) = 1$. As before, the standard reduction types then show that the 2-primary subgroup of $\mathfrak{C}_p(E)$ and $\mathfrak{C}_p(E^{(R)})$ are both annihilated by 2. Thus we conclude from Lemma 5.1 ,and the fact that $E(\mathbb{Q}_p)[2] = E^{(R)}(\mathbb{Q}_p)[2]$, that

$$\mathrm{ord}_2(c_p(E)) = \mathrm{ord}_2(\#(E(\mathbb{Q}_p)[2])) = \mathrm{ord}_2(c_p(E^{(R)})).$$

This proves the first assertion of the lemma. Suppose next that p is a good ordinary prime for E which divides R, and which is such that the trace t_p of Frobenius at p is even. Then p splits in K. Let τ_p be any Frobenius automorphism at p. Note that the extension $K(E[2])/K$ is unramified at p because p is odd and E has good reduction at p. Let $\mathcal{O}_K$ denote the ring of integers of K. Since p splits in K, we can view τ_p as an element of the absolute Galois group of K, and we write ϕ_p for its image in the $\mathcal{O}_K$-automorphism group of the module $E[2]$, which is equal to $(\mathcal{O}_K/2\mathcal{O}_K)^*$. Then ϕ_p must have order dividing 2 because, since t_p is even, its characteristic polynomial is equal to $X^2 - 1$. But 2 is not ramified in K because E has good reduction at 2. Thus the group $(\mathcal{O}_K/2\mathcal{O}_K)^*$ has no element of order 2, whence we must have $\phi_p = 1$ and $E(\mathbb{Q}_p)[2] = E[2]$. The final assertion of the lemma is now clear from Lemma 5.1, and the proof is complete. □

Combining Lemmas 5.3 and 5.4, we immediately obtain:

Corollary 5.5. *Assume that E is defined over $\mathbb{Q}$, has good reduction at 2, and complex multiplication by the ring of integers of $K \neq \mathbb{Q}(\sqrt{-3})$. Let M be a positive squarefree integer which is admissible for E in the sense of Definition 4.4, and has the property that every prime factor of M is $\equiv 1$ mod 4. Write $r(M)$ for the number of primes divisors of M in K. Then*

$$\operatorname{ord}_2\left(\prod_{p|M} c_p(E^{(M)})\right) = r(M). \tag{22}$$

Finally, we now compare some of our estimates with those predicted by the conjecture of Birch and Swinnerton-Dyer. The next proposition is an immediate consequence of Corollaries 4.6 and 5.5.

Proposition 5.6. *Assume that E is defined over $\mathbb{Q}$ and has good reduction at 2, and that $K \neq \mathbb{Q}(\sqrt{-3})$. Assume further that $\operatorname{ord}_2(L^{(alg)}(E,1)) = -1$. Then, for all positive integers M, which are admissible for E, and have the property that all of their prime factors are $\equiv 1$ mod 4, we have*

$$\operatorname{ord}_2\left(\frac{L^{(alg)}(E^{(M)},1)}{L^{(alg)}(E,1)}\right) \geq \operatorname{ord}_2\left(\prod_{p|M} c_p(E^{(M)})\right). \tag{23}$$

As we shall now explain, the lower bound given by (23) is exactly what the conjecture of Birch and Swinnerton-Dyer would predict for elliptic curves with $L^{(\mathrm{alg})}(E^{(M)},1) \neq 0$ satisfying the hypotheses of this proposition, provided we neglect any contribution coming from the 2-primary subgroup of the Tate–Shafarevich group of $E^{(M)}$.

Proposition 5.7. *Let E be an elliptic curve defined over $\mathbb{Q}$, having good reduction at 2, and with complex multiplication by the ring of integers of K. Let R denote any squarefree integer with $(R, N(E)) = 1$, and $R \equiv 1$ mod 4. Then the 2-primary subgroups of $E(\mathbb{Q})$ and $E^{(R)}(\mathbb{Q})$ have the same order, and this order is equal to 2 or 1, according as the prime 2 splits or is inert in K.*

Proof. Let A denote the elliptic curve E or $E^{(R)}$, so that A also has good reduction at 2. In order to show that the 2-primary subgroup of $A(\mathbb{Q})$ is annihilated by 2, it suffices to prove that the 2-primary subgroup of $A(K)$ is annihilated by 2. Now, as E has good reduction at 2, the prime 2 does not ramify in K, and thus it either splits or is inert in K. Let v denote any prime of K above 2. Since A has good reduction at v, the formal group of A at v is a Lubin–Tate formal group with parameter $\pi = \psi_A(v)$, where ψ_A denotes the Grossencharacter of A/K. Let n be any integer ≥ 1. As the group $A[\pi^n]$ of π^n-division points on A lies on the formal group of A at v, it follows from Lubin–Tate theory the extension $K(A[\pi^n])/K$ has Galois group isomorphic to $(\mathcal{O}_K/\pi^n\mathcal{O}_K)^*$, which is nontrivial for all $n \geq 1$ if 2 is inert in K, and which is nontrivial for all $n \geq 2$ if 2 splits in K. In particular, the 2-primary subgroup of $A(K)$ must be trivial if 2 is inert in K, and it must be killed by 2 when 2 splits in K. But 2 splits in K happens precisely when $K = \mathbb{Q}(\sqrt{-7})$, and then A must be a quadratic twist of one of the four isogenous elliptic curves, defined over $\mathbb{Q}$, of conductor 49. Moreover, each of these four curves of conductor 49 has a unique rational point of order 2. It follows that $A(\mathbb{Q})$ must also have a unique point of order 2, because A is a quadratic twist of (16). This completes the proof. □

Now assume that E satisfies the hypotheses of Proposition 5.6. Since $L(E,1) \neq 0$, we know that both $E(\mathbb{Q})$ and the Tate–Shafarevich group of $E/\mathbb{Q}$ are finite, and we write $w(E)$ and $t(E)$ for their respective orders. Then the conjecture of Birch and Swinnerton-Dyer predicts that

(24)
$$\operatorname{ord}_2(L^{(\mathrm{alg})}(E,1)) = \operatorname{ord}_2\left(c_\infty(E)\prod_{p\mid N(E)} c_p(E)\right) + \operatorname{ord}_2(t(E)) - 2\operatorname{ord}_2(w(E)).$$

where $c_\infty(E)$ denotes the number of connected components of $E(\mathbb{R})$. If we recall Proposition 5.7, and the fact that the Cassels–Tate theorem implies that $t(E)$ is the square of an integer, we see that the combination of our hypothesis that $\operatorname{ord}_2(L^{(\mathrm{alg})}(E,1)) = -1$ and the conjectural formula (24) imply that necessarily

$$\operatorname{ord}_2(t(E)) = 0. \tag{25}$$

Suppose now that $L(E^{(M)},1) \neq 0$. Again, we then know that both $E^{(M)}(\mathbb{Q})$ and the Tate–Shafarevich group of $E^{(M)}/\mathbb{Q}$ are finite, and we write $w(E^{(M)})$ and $t(E^{(M)})$ for their respective orders. Then, in this case, the conjecture of Birch and Swinnerton-Dyer predicts that

$$\begin{aligned}\operatorname{ord}_2(L^{(\mathrm{alg})}(E^{(M)},1)) = \operatorname{ord}_2&\left(c_\infty(E^{(M)})\prod_{p\mid N(E)M} c_p(E^{(M)})\right)\\ &+ \operatorname{ord}_2(t(E^{(M)})) - 2\operatorname{ord}_2(w(E^{(M)})).\end{aligned} \tag{26}$$

where $c_\infty(E^{(M)})$ denotes the number of connected components of $E^{(M)}(\mathbb{R})$. Obviously, $c_\infty(E) = c_\infty(E^{(M)})$ since $\mathbb{Q}(\sqrt{M})$ is a real quadratic field. Moreover, Proposition 5.7 shows that $\mathrm{ord}_2(w(E)) = \mathrm{ord}_2(w(E^{(M)}))$, and Lemma 5.4 tells us that, for primes p dividing $N(E)$, we have $\mathrm{ord}_2(c_p(E)) = \mathrm{ord}_2(c_p(E^{(M)}))$. Hence, recalling (25), we conclude that the conjecture of Birch and Swinnerton-Dyer predicts that

$$\mathrm{ord}_2\left(\frac{L^{(\mathrm{alg})}(E^{(M)},1)}{L^{(\mathrm{alg})}(E,1)}\right) = \mathrm{ord}_2\left(\prod_{p|M} c_p(E^{(M)})\right) + \mathrm{ord}_2(t(E^{(M)})). \tag{27}$$

Thus, under the above hypotheses, the lower bound given by (23) is precisely what the conjecture of the Birch and Swinnerton-Dyer would predict if we ignore the unknown term $\mathrm{ord}_2(t(E^{(M)}))$, arising from the order of the 2-primary subgroup of the Tate–Shafarevich group of the curve $E^{(M)}$.

We end this section with the following remark. Let E be an elliptic curve over $\mathbb{Q}$, and satisfying the hypotheses of Proposition 5.6. It is a very intriguing fact that, in order to generalize the method discovered by Tian in [7] and [8] to prove the existence of many quadratic twists of E, whose complex L-series all have a simple zero at $s = 1$, the lower bound given by (23) is not strong enough. Instead, Tian's method requires the use of quadratic twists $E^{(M)}$ of E , for which, when $L(E^{(M)}, 1) \neq 0$, one has a lower bound as predicted by (27) when the 2-primary subgroup of the Tate–Shafarevich group of $E^{(M)}$ is nontrivial. In the case of the curve $E = X_0(49)$, this is indeed shown to be the case in [1] if we assume that every prime factor of M splits completely in the field $\mathbb{Q}(E[4])$.

6. Tables

In this section, we include some short tables of numerical examples of our results for two elliptic curves E defined over $\mathbb{Q}$. We use the same notation as earlier. For the curve of conductor 49 in Table I, the root number of the curve is $+1$, and for the curve of conductor 121 in Table II the root number is -1. As always, M will denote a squarefree positive integer which is admissible for the elliptic curve E, and $r(M)$ will denote the number of prime divisors of M in the field of complex multiplication K.

Table I. Case $X_0(49)$: $y^2 + xy = x^3 - x^2 - 2x - 1$.

<table>
<tr><td colspan="6">The Tamagawa factor of twists $E^{(M)}$ at 7 is always 2.
$\ell_M = L^{(\mathrm{alg})}(E^{(M)}, 1)$ and $L^{(\mathrm{alg})}(E, 1) = 1/2$.</td></tr>
<tr><td>M</td><td>$L(E^{(M)}, 1)$</td><td>ℓ_M</td><td>$\mathrm{ord}_2\,\ell_M$</td><td>$r(M)$</td><td>Tamagawa factors</td></tr>
<tr><td>29</td><td>0.7180139420</td><td>2</td><td>1</td><td>2</td><td>$c_{29} = 4$</td></tr>
<tr><td>37</td><td>0.6356689731</td><td>2</td><td>1</td><td>2</td><td>$c_{37} = 4$</td></tr>
<tr><td>109</td><td>0.3703553538</td><td>2</td><td>1</td><td>2</td><td>$c_{109} = 4$</td></tr>
<tr><td>113</td><td>1.454965333</td><td>8</td><td>3</td><td>2</td><td>$c_{113} = 4$</td></tr>
</table>

continued on next page

Continued from previous page

137	0.3303479321	2	1	2	$c_{137} = 4$
145	0.6422111932	4	2	3	$c_5 = 2$, $c_{29} = 4$
185	2.274238456	16	4	3	$c_5 = 2$, $c_{37} = 4$
233	2.279798298	18	1	2	$c_{233} = 4$
265	4.275446184	36	2	3	$c_5 = 2$, $c_{53} = 4$
277	0.9292915388	8	3	2	$c_{277} = 4$
281	0.2306634143	2	1	2	$c_{281} = 4$
285	1.832312031	16	4	3	$c_3 = 2$, $c_5 = 2$, $c_{19} = 2$
317	0.8686848279	8	3	2	$c_{317} = 4$
337	0.2106283985	2	1	2	$c_{337} = 4$
377	0.3982824745	4	2	3	$c_{13} = 2$, $c_{29} = 4$
389	1.764410302	18	1	2	$c_{389} = 4$
401	1.737809629	18	1	2	$c_{401} = 4$
421	0.7537907774	8	3	2	$c_{421} = 4$
449	2.919635854	32	5	2	$c_{449} = 4$
457	0.7234920569	8	3	2	$c_{457} = 4$
481	1.410422816	16	4	3	$c_{13} = 2$, $c_{37} = 4$
545	0.3312558988	4	2	3	$c_5 = 2$, $c_{109} = 4$
557	0.6553363680	8	3	2	$c_{557} = 4$
565	0.3253401390	4	2	3	$c_5 = 2$, $c_{113} = 4$
569	0.1620972858	2	1	2	$c_{569} = 4$
613	0.1561714487	2	1	2	$c_{613} = 4$
617	0.1556643972	2	1	2	$c_{617} = 4$
629	1.233378974	16	4	3	$c_{17} = 2$, $c_{37} = 4$
641	0.1527224426	2	1	2	$c_{641} = 4$
653	0.1513126668	2	1	2	$c_{653} = 4$
673	1.341426413	18	1	2	$c_{673} = 4$
701	0.1460403507	2	1	2	$c_{701} = 4$
705	1.165003700	16	4	3	$c_3 = 2$, $c_5 = 2$, $c_{47} = 2$
709	0.1452140903	2	1	2	$c_{709} = 4$
757	0.1405348183	2	1	2	$c_{757} = 4$
809	0.5437729586	8	3	2	$c_{809} = 4$
821	0.5397843500	8	3	2	$c_{821} = 4$
877	1.175099358	18	1	2	$c_{877} = 4$
901	1.030527220	16	4	3	$c_{17} = 2$, $c_{53} = 4$
953	0.5010088727	8	3	2	$c_{953} = 4$
965	0.2489420234	4	2	3	$c_5 = 2$, $c_{193} = 4$
969	0.9937107192	16	4	3	$c_3 = 2$, $c_{17} = 2$, $c_{19} = 2$
977	1.113338183	18	1	2	$c_{977} = 4$
985	2.217615590	36	2	3	$c_5 = 2$, $c_{197} = 4$

Table II. Case E: $y^2 + y = x^3 - x^2 - 7x + 10$ of conductor 121.

The Tamagawa factor of twists $E^{(-M)}$ at 11 is always 2. $\ell'_M = L^{(\mathrm{alg})}(E^{(-M)},1)$.					
M	$\lvert L(E^{(-M)},1)\rvert$	$\lvert\ell'_M\rvert$	$\mathrm{ord}_2 \lvert\ell'_M\rvert$	$r(M)$	Tamagawa factors
7	2.1891468090287	4	2	1	$c_7 = 2$
43	0.88326227057036	4	2	1	$c_{43} = 2$
79	0.65164394118303	4	2	1	$c_{79} = 2$
83	0.63574779287777	4	2	1	$c_{83} = 2$
107	0.55992778456568	4	2	1	$c_{107} = 2$
119	1.0618921792481	8	3	2	$c_7 = 2$, $c_{17} = 2$
127	2.0558055688072	16	4	1	$c_{127} = 2$
131	0.50604397615652	4	2	1	$c_{131} = 2$
139	0.49126577270056	4	2	1	$c_{139} = 2$
151	0.47134123309515	4	2	1	$c_{151} = 2$
203	0.81302871404360	8	3	2	$c_7 = 2$, $c_{29} = 2$
211	1.5949338338737	16	4	1	$c_{211} = 2$
227	0.38442442965574	4	2	1	$c_{227} = 2$
239	0.37464932703022	4	2	1	$c_{239} = 2$
247	0.73706438460315	8	3	2	$c_{13} = 2$, $c_{19} = 2$
263	0.35714619952350	4	2	1	$c_{263} = 2$
271	1.4073407182665	16	4	1	$c_{271} = 2$
287	0.68377458498490	8	3	2	$c_7 = 2$, $c_{41} = 2$
307	5.2890138248933	64	6	1	$c_{307} = 2$
323	0.64454410663003	8	3	2	$c_{17} = 2$, $c_{19} = 2$
347	1.2437101001270	16	4	1	$c_{347} = 2$
371	1.2028097610186	16	4	3	$c_7 = 2$, $c_{53} = 4$
427	0.56058305428618	8	3	2	$c_7 = 2$, $c_{61} = 2$
431	0.27898783855424	4	2	1	$c_{431} = 2$
439	1.1057364815655	16	4	1	$c_{439} = 2$
491	1.0455460185550	16	4	1	$c_{491} = 2$
503	0.25824975297425	4	2	1	$c_{503} = 2$
511	0.51244050781894	8	3	2	$c_7 = 2$, $c_{73} = 2$
547	3.9623262060061	64	6	1	$c_{547} = 2$
551	0.49348971241960	8	3	2	$c_{19} = 2$, $c_{29} = 2$
559	0.48994575480372	8	3	2	$c_{13} = 2$, $c_{43} = 2$
563	0.97640434014975	16	4	1	$c_{563} = 2$
607	2.1157876178789	36	2	1	$c_{607} = 2$
659	0.22562187289831	4	2	1	$c_{659} = 2$
707	1.7426259918505	32	5	2	$c_7 = 2$, $c_{101} = 2$
731	0.42844513372759	8	3	2	$c_{17} = 2$, $c_{43} = 2$
739	0.21305988491668	4	2	1	$c_{739} = 2$
743	0.84994239387238	16	4	1	$c_{743} = 2$
763	1.6774578847166	32	5	2	$c_7 = 2$, $c_{109} = 2$

continued on next page

Continued from previous page

787	3.3033647015624	64	6	1	$c_{787} = 2$
811	1.8304420733348	36	2	1	$c_{811} = 2$
887	0.19447424646223	4	2	1	$c_{887} = 2$
919	0.19105840666028	4	2	1	$c_{919} = 2$

References

[1] J. Coates, Y. Li, Y. Tian, and S. Zhai, Quadratic twists of elliptic curves, to appear in Proc. London Math. Soc.

[2] R. M. Damerell, L-functions of elliptic curves with complex multiplication. II, Acta Arith. **19** (1971), 311–317. MR0399103 (53 #2954)

[3] C. Goldstein and N. Schappacher, Séries d'Eisenstein et fonctions L de courbes elliptiques à multiplication complexe, J. Reine Angew. Math. **327** (1981), 184–218. MR0631315 (82m:12007)

[4] B. H. Gross, *Arithmetic on elliptic curves with complex multiplication*, Lecture Notes in Mathematics, 776, Springer, Berlin, 1980. MR0563921 (81f:10041)

[5] K. Rubin, The "main conjectures" of Iwasawa theory for imaginary quadratic fields, Invent. Math. **103** (1991), no. 1, 25–68. MR1079839 (92f:11151)

[6] J. H. Silverman, *Advanced topics in the arithmetic of elliptic curves*, Graduate Texts in Mathematics, 151, Springer, New York, 1994. MR1312368 (96b:11074)

[7] Y. Tian, Congruent numbers with many prime factors, Proc. Natl. Acad. Sci. USA **109** (2012), no. 52, 21256–21258. MR3023667

[8] Y. Tian, Congruent numbers and Heegner points, Cambridge Journal of Mathematics **2** (2014), no. 1, 117–161.

[9] L. Cai, J. Shu, Y. Tian, Explicit Gross-Zagier and Waldspurger formulas and twists of elliptic curves, to appear.

[10] C. Zhao, A criterion for elliptic curves with lowest 2-power in $L(1)$, Math. Proc. Cambridge Philos. Soc. **121** (1997), no. 3, 385–400. MR1434649 (97m:11088)

[11] C. Zhao, A criterion for elliptic curves with second lowest 2-power in $L(1)$, Math. Proc. Cambridge Philos. Soc. **131** (2001), no. 3, 385–404. MR1866384 (2003c:11073)

[12] C. Zhao, A criterion for elliptic curves with lowest 2-power in $L(1)$. II, Math. Proc. Cambridge Philos. Soc. **134** (2003), no. 3, 407–420. MR1981208 (2004e:11070)

[13] C. L. Zhao, A criterion for elliptic curves with second lowest 2-power in $L(1)$. II, Acta Math. Sin. (Engl. Ser.) **21** (2005), no. 5, 961–976. MR2176306 (2006g:11132)

Received March 21, 2013; accepted June 30, 2013

John Coates
Emmanuel College
Cambridge, England
and Department of Mathematics, POSTECH
Pohang, South Korea
E-mail: `jhc13@dpmms.cam.ac.uk`

Minhyong Kim
Merton College
Oxford, England
and Department of Mathematical Sciences, Seoul National University
Seoul, Korea
E-mail: `minhyong.kim@maths.ox.ac.uk`

Zhibin Liang
School of Mathematical Sciences, Capital Normal University
and Beijing International Center for Mathematical Research, Peking University
Beijing, People's Republic of China
E-mail: liangzhb@gmail.com

Chunlai Zhao
Department of Mathematics, Peking University
Beijing, People's Republic of China
E-mail: zhao@math.pku.edu.cn