Journal of Number Theory 204 (2019) 405–422

Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

General Section

On the 2-adic valuations of central L-values of elliptic curves

Junhwa Choi

School of Mathematics, Korea Institute for Advanced Study, 85 Hoegi-ro, Dongdaemun-gu, Seoul 02455, Republic of Korea

ARTICLE INFO

Article history:
Received 12 January 2019
Received in revised form 20 March 2019
Accepted 2 April 2019
Available online 17 May 2019
Communicated by F. Pellarin

MSC:
primary 11G05, 11G40

Keywords:
Elliptic curves
L-values
Birch and Swinnerton-Dyer conjecture

ABSTRACT

The paper generalizes the method of Zhao for an infinite family of $\mathbb{Q}$-curves and establishes some analytic results on the 2-part of the Birch and Swinnerton-Dyer conjecture. We give lower bounds on the 2-adic valuations of the algebraic part of the L-values at $s = 1$ for those $\mathbb{Q}$-curves. Moreover, we also discuss 2-descent on $\mathbb{Q}$-curves and compute their Mordell-Weil group and Tate-Shafarevich group.

1. Introduction

Let K be an imaginary quadratic field, F a finite abelian extension of K, and let A be an elliptic curve defined over F with complex multiplication by the full ring of integers of K. By the classical theory of complex multiplication, F contains the Hilbert class field H of K. We assume that A has the additional property that the field obtained by adjoining to F the coordinates of all torsion points on A is an abelian extension of

E-mail address: jhchoi.math@gmail.com.

https://doi.org/10.1016/j.jnt.2019.04.011
0022-314X/

K. For each square-free positive integer D, we write $A^{(D)}$ for the twist of A by the quadratic extension $F(\sqrt{D})/F$. Let $L(A^{(D)}/F, s)$ denote the complex L-series for $A^{(D)}$ over F. If $L(A^{(D)}/F, s)$ does not vanish at $s = 1$, it is well-known that the Mordell-Weil group $A^{(D)}(F)$ and the Tate-Shafarevich group $Ш(A^{(D)}/F)$ are both finite. However, no one unfortunately has found a general criterion for deciding when $L(A^{(D)}/F, 1) \neq 0$. Moreover, the conjectural exact Birch and Swinnerton-Dyer formula for the order of $Ш(A^{(D)}/F)$ when $L(A^{(D)}/F, 1) \neq 0$ is only proven at present for a few families of such curves in the special case when $K = F$ and K has class number 1.

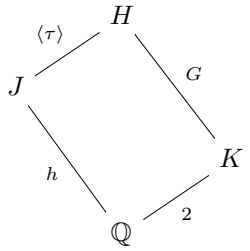
For the elliptic curve $A = X_0(32) : y^2 = x^3 - x$, we have $K = \mathbb{Q}(i)$ and take $K = F$. In this case, Zhao [15], [16], [17] and Tian, Yuan and Zhang [12] have developed techniques which prove the existence of explicit infinite families of D such that $L(A^{(D)}/F, 1) \neq 0$ and the 2-part of the Birch and Swinnerton-Dyer conjecture is valid for $A^{(D)}$. In a similar manner, using Zhao's method, Tian and his collaborators [6] have proven analogous results for the quadratic twists of the elliptic curve $A = X_0(49) : y^2 + xy = x^3 - x^2 - 2x - 1$, where $K = F = \mathbb{Q}(\sqrt{-7})$. In both cases, by using additional arguments from Iwasawa theory [11], the Birch and Swinnerton-Dyer exact formula for the order of $Ш(A^{(D)}/F)$ is then valid. For more general elliptic curves, analogous results on the 2-part of the Birch and Swinnerton-Dyer conjecture have been made recently due to Cai, Li and Zhai [2].

A remarkable feature of Zhao's method, which is more fully discussed in [5], is that it is rather elementary, using only classical expressions for the L-values as finite sums of Eisenstein series, and no arguments from Iwasawa theory. The aim of the present paper is to use a generalization of his method (see §3) to establish some analytic results about the 2-part of the Birch and Swinnerton-Dyer conjecture for an infinite family of $\mathbb{Q}$-curves E in the sense of Gross [9]. More precisely, we will obtain in §4 a lower bound on the 2-adic valuation of the algebraic part of the L-value at $s = 1$ for the $\mathbb{Q}$-curves E/H. We recall that a $\mathbb{Q}$-curve is defined to be an elliptic curve over the Hilbert class field H of an imaginary quadratic field K with complex multiplication by the full ring of integers of K, which is isogenous over H to all of its conjugates under the Galois group of H over $\mathbb{Q}$. We will briefly discuss the theory of $\mathbb{Q}$-curves in §2. In the rest of the paper, using 2-descent, we will find an explicit infinite family of $\mathbb{Q}$-curves E for which the Mordell-Weil group $E(H)$ is finite (see §5).

2. Gross curves and $\mathbb{Q}$-curves

We begin with a brief review of the general theory [9] of $\mathbb{Q}$-curves. Let K be an imaginary quadratic field, viewed as a subfield of $\mathbb{C}$. We denote by $\mathcal{O}$ its ring of integers and h its class number. By the classical theory of complex multiplication, the Hilbert class field of K is given by $H = K(j(\mathcal{O}))$ where j is the classical modular function of weight zero. If we write G for the Galois group of H over K, the Artin map of global class field theory gives an isomorphism $G \simeq \mathrm{Cl}(K)$.

We define the field $J = \mathbb{Q}(j(\mathcal{O}))$. In fact, the value $j(\mathcal{O})$ is a real number which satisfies an irreducible equation of degree h over $\mathbb{Q}$. Hence J is embedded in $\mathbb{R}$, and we have the tower of fields



where τ is the complex conjugation acting on $G \simeq \mathrm{Cl}(K)$ by inversion. The Galois group of H over $\mathbb{Q}$ is the semi-direct product $\mathrm{Cl}(K) \rtimes \langle\tau\rangle$.

Let E be an elliptic curve defined over H with j-invariant $j(E) = j(\mathcal{O})$. By the theory of complex multiplication, it has complex multiplication by $\mathcal{O}$. We say that E is a $\mathbb{Q}$-curve if E is H-isogenous to all of its conjugates E^σ with $\sigma \in \mathrm{Gal}(H/\mathbb{Q})$. In terms of Grössencharacters, this definition is equivalent to saying that

$$\psi_E = \psi_E^\sigma \text{ for all } \sigma \in \mathrm{Gal}(H/\mathbb{Q}) \tag{2.1}$$

where $\psi_E : I_H \to K^\times$ is the Grössencharacter determined by the isogeny class of E over H. Here I_H denotes the group of idèles of H. Furthermore, the condition $\psi_E = \psi_E^\tau$ describes that E can be descended to the field J. Hence there exists an elliptic curve defined over J isomorphic to E over H.

We shall now restrict our attention to the case where $K = \mathbb{Q}(\sqrt{-q})$, with $q > 3$ a prime congruent to 3 modulo 4. We have $\mathcal{O}^\times = \{\pm 1\}$, and by the genus theory the class number h is odd. Gross [9] proved that there exists a unique $\mathbb{Q}$-curve $A(q)$, called a Gross curve, with the property that it is defined over J and has minimal discriminant ideal equal to $(-q^3)$. It is given by the following explicit equation defined over J

$$y^2 = x^3 + \frac{mq}{2^4 3}x - \frac{nq^2}{2^5 3^3} \tag{2.2}$$

where $m^3 = j(\mathcal{O})$ and $-qn^2 = j(\mathcal{O}) - 1728$. Here the sign of n is determined by the Legendre symbol $(2/q)$. On the other hand, Gross also proved in [10] that $A(q)$ has always a global minimal Weierstrass equation over the field J, but these equations are only known explicitly for $q = 11$ and 23. For example, when $q = 23$, $A(23)$ has a global minimal equation over $J = \mathbb{Q}(\alpha)$ given by (see §24 in [9])

$$y^2 + \alpha^3 xy + (\alpha + 2)y = x^3 + 2x^2 - (12\alpha^2 + 27\alpha + 16)x - (73\alpha^2 + 99\alpha + 62), \tag{2.3}$$

where α is a root of the cubic equation $x^3 - x - 1 = 0$.

We assume from now on that the prime q is congruent to 7 modulo 8. This additional condition guarantees that the prime 2 splits in K into two distinct primes which we denote by $\mathfrak{p}$ and $\mathfrak{p}^*$. The theory of complex multiplication then shows that $A(q)$ has good ordinary reduction at the primes of J above 2. This fact is very crucial for our main arguments. We fix once and for all one of the primes $\mathfrak{p}$ of K dividing 2. In what follows, we will only consider twists of $A(q)$ by quadratic extensions $J(\sqrt{D})/J$, where D is a square-free positive integer which is congruent to 1 modulo 4. Clearly, such twists are again $\mathbb{Q}$-curves having good ordinary reduction at the primes of J above 2.

We end this section by recalling, without proof, two properties of arbitrary $\mathbb{Q}$-curves E proven in [9], which we will use later.

Theorem 2.1 *(Theorem 14.2.1 in [9]). Assume that $q \equiv 7 \bmod 8$ is a prime. If E is any $\mathbb{Q}$-curve defined over J, then we have*

$$E(J)_{\mathrm{tor}} = \mathbb{Z}/2\mathbb{Z} \quad \textit{and} \quad E(H)_{\mathrm{tor}} = \mathcal{O}/2\mathcal{O}.$$

The next theorem determines the structure of $E(H)/2E(H)$. Let $B = \mathrm{Res}_{H/K}(E)$ be the abelian variety over K which is the restriction of scalars from H to K of E. Let $\mathcal{R} = \mathrm{End}_K(B)$ and $T = \mathcal{R} \otimes_{\mathbb{Z}} \mathbb{Q}$. It is easily seen (see §15 in [9]) that $\mathcal{R}$ is a projective $\mathcal{O}$-module of rank h, and T is a CM field of degree $2h$ over $\mathbb{Q}$. Since $E(H) = B(K)$ is a module for $\mathcal{R}$, $E(H) \otimes \mathbb{Q} = B(K) \otimes \mathbb{Q}$ is a module for the field T. Hence, if we write $n_H(E)$ for the rank of $E(H)$ over $\mathbb{Z}$, then $n_H(E) \equiv 0 \bmod 2h$. We can therefore define the $\mathbb{Q}$-rank of E by

$$n(E) = n_H(E)/2h. \tag{2.4}$$

Theorem 2.2 *(Theorem 16.2.5 in [9]). Assume that $q \equiv 7 \bmod 8$ is a prime. Let E be any $\mathbb{Q}$-curve defined over J. Then the algebra $\mathcal{R}/2\mathcal{R} = \mathcal{R} \otimes_{\mathcal{O}} \mathcal{O}/2\mathcal{O}$ is isomorphic to $\mathcal{O}/2\mathcal{O}[G]$. Furthermore, the module $E(H)/2E(H) \simeq E(H) \otimes_{\mathcal{O}} \mathcal{O}/2\mathcal{O}$ is isomorphic to the direct sum of $E(H)_2 \simeq \mathcal{O}/2\mathcal{O}$ with $n(E)$ copies of the regular representations $\mathcal{R}/2\mathcal{R}$.*

3. Averaging lemma

Let $K = \mathbb{Q}(\sqrt{-q})$ where q is a prime congruent to 7 modulo 8, and let E be any $\mathbb{Q}$-curve defined over J. It is well-known (cf. §9 in [9]) that the condition (2.1) is equivalent to

$$\psi_E = \varphi_E \circ \mathrm{N}_{H/K} \quad \text{and} \quad \varphi_E = \bar{\varphi}_E, \tag{3.1}$$

where φ_E is a Grössencharacter of K and $\mathrm{N}_{H/K}$ denotes the norm map from the group of idèles I_H of H to the group of idèles I_K of K. Indeed, this φ_E is the Grössencharacter attached to the abelian variety $B = \mathrm{Res}_{J/\mathbb{Q}}(E)$ viewed over K, and it takes values in the group $T^\times$, where, as earlier, $T = \mathcal{R} \otimes_{\mathbb{Z}} \mathbb{Q}$. We then have

$$L(\bar{\psi}_E, s) = \prod_{\chi \in \widehat{G}} L(\bar{\varphi}_E \chi, s), \tag{3.2}$$

where $\widehat{G}$ denotes the group of characters of G.

Let $\mathfrak{f}$ be the conductor of φ_E, and let $\mathfrak{g}$ be any integral multiple of $\mathfrak{f}$. Let S denote the set of prime ideals of K dividing $\mathfrak{g}$. We define the imprimitive Hecke L-functions associated to $\bar{\varphi}_E \chi$ by

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

where $\mathfrak{a}$ runs over all integral ideals of K prime to $\mathfrak{g}$ and $\sigma_{\mathfrak{a}}$ denotes the Artin symbol of $\mathfrak{a}$ in G. Moreover, for each element $\sigma \in G$, if we define the partial L-series for $\bar{\varphi}_E$ relative to σ by

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

we have

$$L_S(\bar{\varphi}_E \chi, s) = \sum_{\sigma \in G} \chi(\sigma) L_S(\bar{\varphi}_E, \sigma, s). \tag{3.3}$$

Writing $L_S(\bar{\psi}_E, s)$ for the imprimitive L-series obtained by removing the Euler factors at the primes above S from $L(\bar{\psi}_E, s)$, we then have

$$L_S(\bar{\psi}_E, s) = \prod_{\chi \in \widehat{G}} \sum_{\sigma \in G} \chi(\sigma) L_S(\bar{\varphi}_E, \sigma, s). \tag{3.4}$$

In this section, we will give an expression for each summand $L_S(\bar{\varphi}_E, \sigma, s)$ in terms of Kronecker-Eisenstein series, and then prove Theorem 3.2, called the averaging lemma, using similar arguments to [5].

Before stating the averaging lemma, we first recall the relation between the various period lattices involved. Note that Gross [10] proved that E admits a global minimal Weierstrass equation over H. Hence we can denote by ω_E the Néron differential attached to a global minimal equation for E. Let $\mathfrak{a}$ be an integral ideal of K prime to $\mathfrak{g}$. Applying $\sigma_{\mathfrak{a}}$ to the coefficients of this equation, we obtain a global minimal equation for $E^{\sigma_{\mathfrak{a}}}$ over H, and we write $\omega_{E^{\sigma_{\mathfrak{a}}}}$ for the Néron differential attached to this equation. As is explained in [9], we can then interpret $\varphi_E(\mathfrak{a})$ as an isogeny

$$\varphi_E(\mathfrak{a}) : E \to E^{\sigma_{\mathfrak{a}}}. \tag{3.5}$$

Thanks to this isogeny, we may define $\Lambda(\mathfrak{a}) \in H^{\times}$ by the pullback equation

$$\varphi_E(\mathfrak{a})^*(\omega_{E^{\sigma_\mathfrak{a}}}) = \Lambda(\mathfrak{a})\omega_E. \tag{3.6}$$

Moreover, as $j(\mathcal{O})^{\sigma_\mathfrak{a}} = j(\mathfrak{a}^{-1})$, it follows easily (cf. Proposition 4.10 in [8]) that the period lattice for $E^{\sigma_\mathfrak{a}}$ is given by

$$\mathfrak{L}_{E^{\sigma_\mathfrak{a}}} = \Lambda(\mathfrak{a})\Omega_E\mathfrak{a}^{-1}, \tag{3.7}$$

where Ω_E is a complex number such that $\mathfrak{L}_E = \Omega_E\mathcal{O}$.

Secondly, we recall the expression of the partial L-series $L_S(\bar{\varphi}_E, \sigma, s)$ in terms of Kronecker-Eisenstein series, which are defined as follows. Let z and s be complex variables. For any lattice L in $\mathbb{C}$, we 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 $z \in L$. It defines a holomorphic function of s in the half plane $\mathrm{Re}(s) > 3/2$, and it has an analytic continuation to the whole s-plane. For the following proposition, we assume for the moment that $\mathfrak{g}$ is principal, say $\mathfrak{g} = g\mathcal{O}$ with $g \in \mathcal{O}$. Let $H(E_\mathfrak{g})$ denote the field obtained by adjoining to H the $\mathfrak{g}$-division points on E.

Proposition 3.1. *Let $\mathfrak{g}$ be any non-zero principal ideal, say $\mathfrak{g} = g\mathcal{O}$ with $g \in \mathcal{O}$, which is a multiple of the conductor $\mathfrak{f}$ of φ_E, and let $\mathfrak{a}$ be an integral ideal of K prime to $\mathfrak{g}$. Let $\mathfrak{B}$ denote any set of integral ideals $\mathfrak{b}$ of K prime to $\mathfrak{g}$, whose Artin symbols $\sigma_\mathfrak{b}$ give precisely the Galois group of $H(E_\mathfrak{g})$ over H. For $\mathrm{Re}(s) > 3/2$, we have*

$$L_S(\bar{\varphi}_E, \sigma_\mathfrak{a}, s) = \frac{|\Lambda(\mathfrak{a})\Omega_E/g|^{2s}}{\overline{(\Lambda(\mathfrak{a})\Omega_E/g)}} \cdot \frac{(\mathrm{N}\mathfrak{a})^{1-s}}{\varphi_E(\mathfrak{a})} \cdot \sum_{\mathfrak{b}\in\mathfrak{B}} H_1\left(\varphi_E(\mathfrak{b})\Lambda(\mathfrak{a})\frac{\Omega_E}{g}, s, \mathfrak{L}_{E^{\sigma_\mathfrak{a}}}\right).$$

Proof. The proposition is the special case of Proposition 5.5 in [8] where $\rho = \Omega_E/g$, $\mathfrak{h} = 1$ and $k = 1$. □

For any lattice L in $\mathbb{C}$, the non-holomorphic Eisenstein series $\mathcal{E}_1^*(z, L)$ is defined by

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

It is well-known (cf. Théorème 6.2 in [8]) that $\mathcal{E}_1^*(\Lambda(\mathfrak{a})\Omega_\infty/g, \mathfrak{L}_{E^{\sigma_\mathfrak{a}}})$ belongs to the field $H(E_\mathfrak{g})$, and satisfies

$$\mathcal{E}_1^*\left(\varphi_E(\mathfrak{b})\Lambda(\mathfrak{a})\frac{\Omega_E}{g}, \mathfrak{L}_{E^{\sigma_\mathfrak{a}}}\right) = \mathcal{E}_1^*\left(\Lambda(\mathfrak{a})\frac{\Omega_E}{g}, \mathfrak{L}_{E^{\sigma_\mathfrak{a}}}\right)^{\sigma_\mathfrak{b}}. \tag{3.8}$$

Hence Proposition 3.1 immediately implies that

$$L_S(\bar{\varphi}_E, \sigma_{\mathfrak{a}}, 1) = \frac{\Lambda(\mathfrak{a})\Omega_E}{\varphi_E(\mathfrak{a})g} \cdot \mathrm{Tr}_{H(E_{\mathfrak{g}})/H}\left(\mathcal{E}_1^*\left(\Lambda(\mathfrak{a})\frac{\Omega_E}{g}, \mathfrak{L}_{E^{\sigma_{\mathfrak{a}}}}\right)\right), \tag{3.9}$$

where $\mathrm{Tr}_{H(E_{\mathfrak{g}})/H}$ denotes the trace map from $H(E_{\mathfrak{g}})$ to H.

In what follows, we now take $A = A(q)$ to be the Gross curve over J as defined in Section 2. Let $\mathscr{M}$ denote the set of all square-free positive integers M having the property that all prime factors of M are congruent to 1 modulo 4, and inert in K. For each M in $\mathscr{M}$, let

$$E = A^{(M)}$$

be the twist of A by the quadratic extension $J(\sqrt{M})/J$. We simply write φ_M for the Grössencharacter φ_E, ψ_M for the Grössencharacter ψ_E, $\mathfrak{L}_M$ for the lattice $\mathfrak{L}_E$, and $\mathfrak{L}_{M,\mathfrak{a}}$ for the lattice $\mathfrak{L}_{E^{\sigma_{\mathfrak{a}}}}$. In the special case where $E = A$, we simply write them as φ, ψ, $\mathfrak{L}$ and $\mathfrak{L}_{\mathfrak{a}}$, respectively. Since $\varphi_M = \varphi\eta_M$, where η_M is the character of K defining the quadratic extension $K(\sqrt{M})/K$, it is easily seen that φ_M has conductor $M\sqrt{-q}\mathcal{O}$. Moreover, we fix a global minimal Weierstrass equation for E/H by

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

where the a_i lie in the ring of integers of H. If $\wp(z, \mathfrak{L}_M) = x + (a_1^2 + 4a_2)/12$ and $\wp'(z, \mathfrak{L}_M) = 2y + a_1x + a_3$, then E has the associated Weierstrass equation

$$\wp'(z, \mathfrak{L}_M)^2 = 4\wp(z, \mathfrak{L}_M)^3 - g_2(\mathfrak{L}_M)\wp(z, \mathfrak{L}_M) - g_3(\mathfrak{L}_M),$$

where $g_2(\mathfrak{L}_M)$ and $g_3(\mathfrak{L}_M)$ are given explicitly by

$$g_2(\mathfrak{L}_M) = \frac{-qmM^2}{2^6 3}, \ g_3(\mathfrak{L}_M) = \frac{q^2nM^3}{24^3}.$$

Here m and n are defined as in (2.2). Hence writing $\mathfrak{L} = \Omega_\infty\mathcal{O}$ for some fixed $\Omega_\infty \in \mathbb{C}^\times$, the period lattice for E over $\mathbb{C}$ is given by

$$\mathfrak{L}_M = \frac{\Omega_\infty}{\sqrt{M}}\mathcal{O}. \tag{3.10}$$

Moreover, by (3.7), the period lattice for $E^{\sigma_{\mathfrak{a}}}$ over $\mathbb{C}$ is then given by

$$\mathfrak{L}_{M,\mathfrak{a}} = \Lambda(\mathfrak{a})\frac{\Omega_\infty}{\sqrt{M}}\mathfrak{a}^{-1}. \tag{3.11}$$

We now suppose that $r \geq 0$ is an integer, and that $p_1, \cdots, p_r$ are distinct primes which are congruent to 1 modulo 4, and inert in K. We define

$$\mathfrak{M}_r = p_1 \cdots p_r, \ g_r = \mathfrak{M}_r\sqrt{-q}$$

and $\mathfrak{g}_r = g_r\mathcal{O}$. Of course, $\mathfrak{M}_r$ belongs to $\mathscr{M}$. For each $1 \le i \le r$, the quadratic extension $K(\sqrt{p_i})/K$ has conductor $p_i\mathcal{O}$, so that it is certainly contained in the ray class field of K modulo $\mathfrak{g}_r$, which we denote by $\mathfrak{R}_r$. By the classical theory of complex multiplication, $\mathfrak{R}_r$ is contained in the field $H(E_{\mathfrak{g}_r})$. Moreover, since $\mathfrak{g}_r$ is equal to the least common multiple of the conductor $\mathcal{O}$ of H over K and the conductor of the Grössencharacter $\varphi_{\mathfrak{M}_r}$, it is well-known (cf. Lemma 3 in [4]) that in fact we have $\mathfrak{R}_r = H(E_{\mathfrak{g}_r})$. Hence the fields

$$\mathfrak{J}_r = H(\sqrt{p_1}, \cdots, \sqrt{p_r})$$

are always contained in $\mathfrak{R}_r$. Finally, let S_r denote the set of prime ideals of K dividing $\mathfrak{g}_r$ and let $\mathcal{D}_r$ denote the set of all positive integers dividing $\mathfrak{M}_r$.

Theorem 3.2 *(Averaging lemma). Assume that $r \ge 0$, and let $\mathfrak{a}$ be an integral ideal of K prime to $\mathfrak{g}_r$. Then*

$$\sum_{M\in\mathcal{D}_r} \frac{L_{S_r}(\bar{\varphi}_M, \sigma_{\mathfrak{a}}, 1)}{\Omega_\infty} = 2^r \cdot \frac{\Lambda(\mathfrak{a})}{\varphi(\mathfrak{a})} \cdot \mathrm{Tr}_{\mathfrak{R}_r/\mathfrak{J}_r}\left(g_r^{-1}\mathcal{E}_1^*\left(\Lambda(\mathfrak{a})\frac{\Omega_\infty}{g_r}, \mathfrak{L}_{\mathfrak{a}}\right)\right) \tag{3.12}$$

provided that $\eta_M(\mathfrak{a}) = 1$ for all $M \in \mathcal{D}_r$.

Proof. The proof of the lemma is essentially the same as that of Theorem 2.4 in [5]. By our hypothesis, we have $\varphi_M(\mathfrak{a}) = \varphi(\mathfrak{a})$. Applying (3.9) to the curve $E = A^{(M)}$ with $S = S_r$ and $g = g_r$, we have

$$L_{S_r}(\bar{\varphi}_M, \sigma_{\mathfrak{a}}, 1) = \frac{\Lambda(\mathfrak{a})}{\varphi(\mathfrak{a})} \cdot \frac{\Omega_\infty}{g_r\sqrt{M}} \cdot \mathrm{Tr}_{\mathfrak{R}_r/H}\left(\mathcal{E}_1^*\left(\Lambda(\mathfrak{a})\frac{\Omega_\infty}{g_r\sqrt{M}}, \mathfrak{L}_{M,\mathfrak{a}}\right)\right).$$

It is well-known that $\mathcal{E}_1^*(z, \mathfrak{L}_{M,\mathfrak{a}}) = \lambda\mathcal{E}_1^*(\lambda z, \lambda\mathfrak{L}_{M,\mathfrak{a}})$ for any nonzero complex number λ. Putting $\lambda = \sqrt{M}$, we conclude that

$$\frac{L_{S_r}(\bar{\varphi}_M, \sigma_{\mathfrak{a}}, 1)}{\Omega_\infty} = \sum_{\sigma\in G_r} (\sqrt{M})^{\sigma-1}\frac{\Lambda(\mathfrak{a})}{\varphi(\mathfrak{a})} \cdot g_r^{-1}\mathcal{E}_1^*\left(\Lambda(\mathfrak{a})\frac{\Omega_\infty}{g_r}, \mathfrak{L}_{\mathfrak{a}}\right)^{\sigma} \tag{3.13}$$

where G_r denotes the Galois group of $\mathfrak{R}_r$ over H. Finally, Lemma 2.5 in [5] shows that for each $\sigma \in G_r$

$$\sum_{M\in\mathcal{D}_r} (\sqrt{M})^{\sigma-1} = \begin{cases} 2^r & \text{if } \sigma \text{ fixes } \mathfrak{J}_r, \\ 0 & \text{otherwise.} \end{cases} \tag{3.14}$$

This completes the proof of the theorem. □

For the induction argument in the next section, it is important to have a parallel statement of Theorem 3.2 in terms of L-functions, rather than partial L-functions. Define $\mathcal{A}_{\mathfrak{M}_r}$ to be any set of integral ideals $\mathfrak{a}$ of K, which are prime to $2(\sqrt{-q})$, whose Artin symbols give precisely the Galois group $G = \mathrm{Gal}(H/K)$, and which, in addition, are such that $\eta_M(\mathfrak{a}) = 1$ for all $M \in \mathcal{D}_r$. Such a set $\mathcal{A}_{\mathfrak{M}_r}$ exists because plainly $H \cap K(\sqrt{p_1}, \dots \sqrt{p_r}) = K$. In the remainder of the paper, we will always assume that $\mathfrak{a}$ belongs to $\mathcal{A}_{\mathfrak{M}_r}$.

Corollary 3.3. *For all $r \geq 0$ and for all characters χ of $G = \mathrm{Gal}(H/K)$, we have*

$$\sum_{M \in \mathcal{D}_r} \frac{L_{S_r}(\bar{\varphi}_M \chi, 1)}{\Omega_\infty} = 2^r \sum_{\mathfrak{a} \in \mathcal{A}_{\mathfrak{M}_r}} \chi(\sigma_\mathfrak{a}) \frac{\Lambda(\mathfrak{a})}{\varphi(\mathfrak{a})} \mathrm{Tr}_{\mathfrak{R}_r/\mathfrak{J}_r} \left(g_r^{-1} \mathcal{E}_1^* \left(\Lambda(\mathfrak{a}) \frac{\Omega_\infty}{g_r}, \mathfrak{L}_\mathfrak{a} \right) \right).$$

4. Integrality at 2 and the induction argument

We now use an induction argument to establish our main analytic results for the curves $E = A^{(M)}$ for $M \in \mathscr{M}$. We fix once and for all a place $\mathfrak{P}$ of the algebraic closure of $\mathbb{Q}$ above 2, and write ord_2 for the valuation at $\mathfrak{P}$, always normalized so that $\mathrm{ord}_2(2) = 1$. We have (cf. Exercise II.1.5 in [7] and Lemme 4.9(ii) in [8])

$$\Lambda(\mathfrak{a})\mathcal{O}_H = \mathfrak{a}\mathcal{O}_H \quad \text{and} \quad \varphi(\mathfrak{a})\mathcal{O}_T = \mathfrak{a}\mathcal{O}_T, \tag{4.1}$$

where $\mathcal{O}_H$ (resp. $\mathcal{O}_T$) denote the ring of integers of H (resp. the ring of integers of T). This implies that the element $\Lambda(\mathfrak{a})/\varphi(\mathfrak{a}) \in \overline{\mathbb{Q}}$ is a $\mathfrak{P}$-unit.

Proposition 4.1. *For each $r \geq 0$, we define*

$$\Psi_{\mathfrak{a},r} = \mathrm{Tr}_{\mathfrak{R}_r/\mathfrak{J}_r} \left(g_r^{-1} \mathcal{E}_1^* \left(\Lambda(\mathfrak{a}) \frac{\Omega_\infty}{g_r}, \mathfrak{L}_\mathfrak{a} \right) \right).$$

Then the element $2\Psi_{\mathfrak{a},r}$ in $\mathfrak{J}_r$ is integral at all places of $\mathfrak{J}_r$ above 2.

Proof. We can apply the proof of Proposition 4.1 in [6] to our case. Let L be any lattice in $\mathbb{C}$ and let ω be a complex number such that $\omega + L$ has exact finite order $m \geq 3$ in $\mathbb{C}/L$. Then we have the identity

$$m\mathcal{E}_1^*(\omega, L) = \sum_{k=1}^{m-2} \left(\wp((k+1)\omega, L) + \wp(k\omega, L) + \wp(\omega, L) \right)^{1/2} \tag{4.2}$$

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

We can take $L = \mathfrak{L}_\mathfrak{a}$ and $\omega = \varphi(\mathfrak{b})\Lambda(\mathfrak{a})\Omega_\infty/g_r$, where $\mathfrak{b}$ is any integral ideal of K prime to $\mathfrak{g}_r$. Since $\mathcal{E}_1^*(\omega, \mathfrak{L}_\mathfrak{a})$ is one of the conjugates of $\mathcal{E}_1^*(\Lambda(\mathfrak{a})\Omega_\infty/g_r, \mathfrak{L}_\mathfrak{a})$ over H, it suffices to show that $2\mathcal{E}_1^*(\omega, \mathfrak{L}_\mathfrak{a})$ is integral at all places of $\mathfrak{R}_r$ above 2. Let P be the point on $A^{\sigma_\mathfrak{a}}$ corresponding to ω. We then have $m = p_1 \cdots p_r q$, which is odd. Now

$$\wp(k\omega, \mathfrak{L}_{\mathfrak{a}}) = x(kP) + \frac{a_{1,\sigma_{\mathfrak{a}}}^2 + 4a_{2,\sigma_{\mathfrak{a}}}}{12}, \quad k = 1, 2, \cdots, m-1.$$

Here $a_{1,\sigma_{\mathfrak{a}}}, a_{2,\sigma_{\mathfrak{a}}}$ are the respective images of a_1, a_2 under $\sigma_{\mathfrak{a}}$, where a_1, a_2 are the usual coefficients of a global minimal Weierstrass equation for $A^{\sigma_{\mathfrak{a}}}/H$. However, $x(kP)$ is integral at all places of $\mathfrak{R}_r$ above 2. Indeed, if $x(kP)$ is not integral at a place v above 2, the point kP would necessarily lie on the formal group of $A^{\sigma_{\mathfrak{a}}}$ at v since $A^{\sigma_{\mathfrak{a}}}$ has good reduction at v. But this is impossible because kP has odd order. Hence by (4.2), this completes the proof. □

For each $M \in \mathscr{M}$ and $\chi \in \widehat{G}$, we now define

$$L^{(\mathrm{alg})}(\bar{\varphi}_M\chi, 1) = \frac{L(\bar{\varphi}_M\chi, 1)}{\Omega_\infty/\sqrt{M}}, \; L^{(\mathrm{alg})}(\bar{\psi}_M, 1) = \frac{L(\bar{\psi}_M, 1)}{(\Omega_\infty/\sqrt{M})^h}\left(\prod_{\mathfrak{a}\in\mathcal{A}_M}\Lambda(\mathfrak{a})\right)^{-1}.$$

Note that the latter L-value belongs to K (cf. Théorème 7.1 in [8]). Now Proposition 4.1 and Theorem 3.2 for $r = 0$ give

$$\mathrm{ord}_2\left(L_{S_0}(\bar{\varphi}, \sigma_{\mathfrak{a}}, 1)/\Omega_\infty\right) \geq -1, \tag{4.3}$$

whence, by (3.3) with $s = 1$,

$$\mathrm{ord}_2\left(L^{(\mathrm{alg})}(\bar{\varphi}\chi, 1)\right) \geq -1 \tag{4.4}$$

for all $\chi \in \widehat{G}$. More generally, we have the following result.

Theorem 4.2. *Assume that $M \in \mathscr{M}$ has $r \geq 0$ prime factors. Then we have*

$$\mathrm{ord}_2\left(L^{(\mathrm{alg})}\left(\bar{\varphi}_M\chi, 1\right)\right) \geq r - 1, \tag{4.5}$$

for all $\chi \in \widehat{G}$.

Proof. We prove the theorem by induction on r, noting that it is true for $r = 0$ by (4.4). Now suppose that $r \geq 1$, and assume by induction that (4.5) is valid for all $M \in \mathscr{M}$ with strictly fewer than r prime factors. Suppose that M' is any element of $\mathscr{M}$ with r prime factors. Let p be any prime dividing M', and let M be any positive divisor of M' which is not divisible by p. Since p is inert in K, the ideal $(p) = p\mathcal{O}$ splits completely in H, whence $\chi(\sigma_{(p)}) = 1$, where, as usual, $\sigma_{(p)}$ denotes the Artin symbol of (p) in G. We claim that we then always have

$$\varphi_M((p)) = -p. \tag{4.6}$$

We first note that necessarily $\eta_M((p)) = 1$. Indeed, the prime p is unramified in the extension $K(\sqrt{M})/\mathbb{Q}$, and it is inert in K, whence it must then split in $K(\sqrt{M})/K$

because $K(\sqrt{M}) = \mathbb{Q}(\sqrt{-q}, \sqrt{-Mq})$ is not a cyclic extension of $\mathbb{Q}$. Moreover, recalling that ψ denotes the Grössencharacter of A/H, we must have $\varphi((p)) = \psi(w)$ for every prime w of H lying above p. On the other hand, by the theory of complex multiplication, the complex L-series of $A/\mathbb{Q}(j(\mathcal{O}))$ coincides with the Hecke L-function $L(\psi, s)$, whence it follows easily that we must have $\psi(w) = -p$, and so $\varphi((p)) = -p$, completing the proof of (4.6). Hence the value at $s = 1$ of the Euler factor at (p) of the L-series $L(\bar{\varphi}_M\chi, s)$ is given by

$$\left(1 + p^{-1}\right)^{-1}. \tag{4.7}$$

Since $\mathrm{ord}_2(1+p^{-1}) = 1$ because we have assumed p is congruent to 1 modulo 4, it follows by induction that, writing S for the set of all primes of K dividing M', we have

$$\mathrm{ord}_2\left(\frac{L_S(\bar{\varphi}_M\chi, 1)}{\Omega_\infty}\right) = \mathrm{ord}_2\left(\frac{L(\bar{\varphi}_M\chi, 1)}{\Omega_\infty}\right) \cdot \prod_{p|M'/M} \mathrm{ord}_2\left(1 + p^{-1}\right) \geq r - 1 \tag{4.8}$$

for all proper divisors M of M'. Granted Proposition 4.1, the assertion (4.5) now follows from Corollary 3.3 with $M' = \mathfrak{M}_r$. This completes the proof. □

Corollary 4.3. *If $M \in \mathscr{M}$ has $r \geq 0$ prime factors, we have*

$$\mathrm{ord}_2(L^{(\mathrm{alg})}(\bar{\psi}_M, 1)) \geq h(r-1). \tag{4.9}$$

In the next section, we will prove that, for all $M \in \mathscr{M}$, $E = A^{(M)}$ satisfies $E(H) = \mathcal{O}/2\mathcal{O}$. Hence the conjecture of Birch and Swinnerton-Dyer predicts that $L(\bar{\psi}_M, 1) \neq 0$, and, also, since the Tamagawa factor at each of the bad primes of E is well-known to be 2, that

$$\mathrm{ord}_2\left(L^{(\mathrm{alg})}(\bar{\psi}_M, 1)\right) = \mathrm{ord}_2\left(\#Ш(E/H)(\mathfrak{p})\right) + h(r+1) - 2.$$

Unfortunately, it does not seem easy to prove that $L(\bar{\psi}_M, 1) \neq 0$, nor possible to strengthen the averaging method used in this section to give the lower bound of $h(r+1)-2$ for $\mathrm{ord}_2\left(L^{(\mathrm{alg})}(\bar{\psi}_M, 1)\right)$.

5. Trivial 2-Selmer groups

Again let $K = \mathbb{Q}(\sqrt{-q})$, where q is a prime congruent to 7 modulo 8, and let $\mathcal{O}$ be the ring of integers of K. Let E be any $\mathbb{Q}$-curve defined over $J = \mathbb{Q}(j(\mathcal{O}))$. We now carry out a classical 2-descent on E.

We begin by recalling the definition of the 2-Selmer group of E. We use the standard notation for Galois cohomology groups. If f is any nonzero element of $\mathcal{O}$, E_f will denote the Galois module of f-division points on E. In particular, we have the exact sequence of Galois modules

$$0 \longrightarrow E_2 \longrightarrow E(\overline{H}) \xrightarrow{2} E(\overline{H}) \longrightarrow 0,$$

which gives rise to a short exact sequence

$$0 \longrightarrow E(H)/2E(H) \xrightarrow{\lambda} \mathrm{H}^1(H, E_2) \longrightarrow \mathrm{H}^1(H, E)_2 \longrightarrow 0.$$

This exact sequence has a local analogue for all places v of H. Hence we obtain the following commutative diagram with exact rows

$$\begin{array}{ccccccccc} 0 & \longrightarrow & E(H)/2E(H) & \xrightarrow{\lambda} & \mathrm{H}^1(H, E_2) & \longrightarrow & \mathrm{H}^1(H, E)_2 & \longrightarrow & 0\ . \\ & & \downarrow & & \downarrow{\scriptstyle \mathrm{Res}} & & \downarrow{\scriptstyle \mathrm{Res}} & & \\ 0 & \longrightarrow & \prod_v E(H_v)/2E(H_v) & \xrightarrow{\prod_v \lambda_v} & \prod_v \mathrm{H}^1(H_v, E_2) & \longrightarrow & \prod_v \mathrm{H}^1(H_v, E)_2 & \longrightarrow & 0 \end{array} \tag{5.1}$$

We define the 2-Selmer group $S_2(E/H)$ of E over H and the Tate-Shafarevich group $Ш(E/H)$ of E over H by

$$\begin{aligned} S_2(E/H) &= \mathrm{Ker}\left(\mathrm{H}^1(H, E_2) \longrightarrow \prod_v \mathrm{H}^1(H_v, E)\right), \\ Ш(E/H) &= \mathrm{Ker}\left(\mathrm{H}^1(H, E) \longrightarrow \prod_v \mathrm{H}^1(H_v, E)\right). \end{aligned} \tag{5.2}$$

It follows immediately that we have a short exact sequence

$$0 \longrightarrow E(H)/2E(H) \xrightarrow{\lambda} S_2(E/H) \longrightarrow Ш(E/H)_2 \longrightarrow 0. \tag{5.3}$$

Now, as is remarked in (17.2.1) of [9], we have $E_2 = \mu_2 \times \mu_2$, allowing us to view E_2 as a trivial G-module, and then $G = \mathrm{Gal}(H/K)$ acts on $\mathrm{H}^1(H, E_2)$. Since the class number h of K is odd, the restriction map induces an isomorphism

$$\mathrm{H}^1(K, E_2) \simeq \mathrm{H}^1(H, E_2)^G.$$

We define $S_2(E)$ by

$$S_2(E) = S_2(E/H)^G. \tag{5.4}$$

We remark that $E(H)/2E(H)$ is a G-module in the sense of Theorem 2.2, and the map $\lambda : E(H)/2E(H) \to \mathrm{H}^1(H, E_2)$ is indeed a homomorphism of G-modules (cf. Theorem 17.2.3 in [9]). Hence λ induces an injection

$$\lambda_G : (E(H)/2E(H))^G \hookrightarrow S_2(E). \tag{5.5}$$

Hence the calculation of $S_2(E)$, rather than the full 2-Selmer group $S_2(E/H)$, can provide an upper bound of the $\mathbb{Q}$-rank of E. In fact, by Theorem 2.2, we have

$$\mathrm{rank}_{\mathcal{O}/2\mathcal{O}}(E(H)/2E(H))^G = n(E) + 1. \tag{5.6}$$

Let D denote a square-free integer such that $D \equiv 1 \bmod 4$, with the property that each prime factor of D is inert in K. We denote by M (resp. N) the product of the primes dividing D, all of which are congruent to 1 modulo 4 (resp. congruent to 3 modulo 4). Thus

$$D = (-1)^k MN,$$

where k is the number of prime factors of N. In what follows, we take $E = A^{(D)}$ so that E has good reduction outside the set of primes of H dividing qD. Now $E_2 = E_{\mathfrak{p}} \oplus E_{\mathfrak{p}^*}$, and so we have

$$\mathrm{H}^1(H, E_2) = \mathrm{H}^1(H, E_{\mathfrak{p}}) \times \mathrm{H}^1(H, E_{\mathfrak{p}^*}) \simeq (H^\times/H^{\times 2})^2,$$

where the last isomorphism is given by multiplicative Kummer theory. Moreover, we have the injection

$$\lambda = (\lambda_{\mathfrak{p}}, \lambda_{\mathfrak{p}^*}) : E(H)/2E(H) \hookrightarrow (H^\times/H^{\times 2})^2$$

which is described as follows. If P is in $E(H)$, we choose a point R in $E(\overline{H})$ such that $2R = P$, and then define $\lambda(P)(\sigma) = \sigma(R) - R$. It follows that R generates an extension $H(R) = H(\sqrt{\alpha}, \sqrt{\beta})$ of H, where we may choose α and β such that

$$\lambda(P) \equiv (\alpha, \beta) \bmod H^{\times 2}. \tag{5.7}$$

For each prime v of H, the map $\lambda_v = (\lambda_{v,\mathfrak{p}}, \lambda_{v,\mathfrak{p}^*})$ can be described similarly. Thus, in order to determine $S_2(E)$, we must decide which elements of

$$\mathrm{H}^1(K, E_2) \simeq (K^\times/K^{\times 2})^2 \hookrightarrow (H^\times/H^{\times 2})^2$$

are in the image of $\prod_v \lambda_v$, viewed inside $\prod_v (H_v^\times/H_v^{\times 2})^2$. Now let $\mathcal{O}_v$ denote the ring of integers of H_v.

Lemma 5.1. *Let v be any prime of H. If $v \nmid 2$, then the image of λ_v has order 4. If $v \nmid qD$, then the image of λ_v is contained in the subgroup $(\mathcal{O}_v^\times/\mathcal{O}_v^{\times 2})^2$.*

Proof. For the first assertion, we remark that if $v \nmid 2$, the classical theory of formal groups of elliptic curves shows that (cf. see Lemma 3.1 in [1])

$$\#E(H_v)/2E(H_v) = \#E(H_v)_2 = 4,$$

and hence $\mathrm{Im}(\lambda_v)$ has order 4. The second assertion is essentially the same as Lemma 22.1.3 in [9]. If $v \nmid 2qD$, it is easily seen that the extension $H_v(R)/H_v$ is unramified. It follows that α and β in (5.7) have even valuation at v, from which the image of λ_v is given by $(\mathcal{O}_v^\times/\mathcal{O}_v^{\times 2})^2$. Finally, if $v \mid 2$, the assertion of the lemma follows from Proposition 3.6 in [1]. □

The following lemma is a fundamental result on the theory of elliptic curves with complex multiplication.

Lemma 5.2. *E has good reduction everywhere over the fields $H(E_{\mathfrak{p}^2})$ and $H(E_{\mathfrak{p}^{*2}})$.*

Proof. The proof uses the Serre-Tate homomorphism and is entirely similar to that given for Lemma 2.1 in [3]. □

The next sequence of lemmas gives the determination of the image of λ_v when v is a prime of bad reduction for E, that is, when v divides qD. If v lies above a prime $p \mid D$, then we have $H_v = K_p$. Similarly, if v divides q, then we have $H_v = K_{\mathfrak{q}}$ where $\mathfrak{q}$ denote the prime ideal $\sqrt{-q}\mathcal{O}$ of K. We also note that when v divides D, -1 is a square in H_v, but not a square when v divides q.

Lemma 5.3. *Let v be any prime of H lying above a prime $p \mid M$. Then the image of λ_v is given by*

$$\{(1,1),(1,\sqrt{-q}D),(\sqrt{-q}D,1),(\sqrt{-q}D,\sqrt{-q}D)\} \subset (H_v^\times/H_v^{\times 2})^2.$$

Proof. By the first assertion of Lemma 5.1, it clearly suffices to show that there exists $P \in E(H)$ such that $\lambda_{v,\mathfrak{p}}(P) \equiv \alpha \equiv \sqrt{-q}D \bmod H_v^{\times 2}$, and similarly for the map $\lambda_{v,\mathfrak{p}^*}$. We will give the proof of the former case, because that of the latter one is essentially parallel.

Let P be any nonzero $\mathfrak{p}$-torsion point in $E(H)$, and choose $R \in E_{\mathfrak{p}^2}$ such that $2R = P$. It follows that $\lambda_v(P) \equiv (\alpha, 1) \bmod H_v^{\times 2}$, whence

$$H_v(R) = K_p(R) = K_p(\sqrt{\alpha}). \tag{5.8}$$

By Lemma 5.2, E has good reduction everywhere over $H(E_{\mathfrak{p}^2})$. Since E has bad reduction at all the primes of H above p, the field $K_p(R)$ should be ramified over K_p. We now define $F_p = K_p(\sqrt{D})$. If E is viewed as an elliptic curve defined over F_p, then it has good reduction. It allows us to consider the reduced curve $\widetilde{E}$ on the residue field of F_p,

which is isomorphic to $\mathbb{F}_{p^2}$. Let α_p be a root of the characteristic polynomial of the p-th Frobenius endomorphism for A over $\mathbb{F}_p$. The curves A and E are isomorphic over F_p, so that we have

$$\#\widetilde{E}(\mathbb{F}_{p^2}) = \#\widetilde{A}(\mathbb{F}_{p^2}) = p^2 + 1 - \alpha_p^2 - \bar{\alpha}_p^2.$$

However, p is a supersingular prime for A, it follows that $\alpha_p + \bar{\alpha}_p = 0$ and therefore

$$\#\widetilde{E}(\mathbb{F}_{p^2}) = (p+1)^2, \tag{5.9}$$

which is divisible by 4, not by 8. It follows that $E(F_p)$ has no $\mathfrak{p}^2$-torsion points; otherwise, by Theorem 2.1, $E(F_p)$ would contain the subgroup $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, and so does $\widetilde{E}(\mathbb{F}_{p^2})$, which is a contradiction. Hence $K_p(R)$ is not equal to $F_p = K_p(\sqrt{D})$. Moreover, as the field extension $F_p(R)$ over F_p is quadratic, so is the field extension $K_p(R)$ over K_p. Hence we have

$$K_p(R) = K_p(\sqrt{uD}),$$

where u is any non-square element in $K_p^\times$. However, $\sqrt{-q}$ is always a non-square element in $K_p^\times$. By Hensel's lemma, we may check this claim in the residue field $\mathbb{F}_{p^2}$. We have

$$\left(\sqrt{-q}\right)^2 = -q \in \mathbb{F}_p^\times \quad \text{and} \quad \left(\sqrt{-q}\right)^{2(p-1)} = 1. \tag{5.10}$$

The group $\mathbb{F}_{p^2}^\times$ is cyclic of order $p^2 - 1 = 2(p-1)\left(\frac{p+1}{2}\right)$, where $\frac{p+1}{2}$ is odd. Thus $\sqrt{-q}$ is an odd power of a generator of $\mathbb{F}_{p^2}^\times$, and so is a non-square element. □

Lemma 5.4. *Let v be any prime of H lying above a prime $p \mid N$. Then the image of λ_v is given by*

$$\{(1,1),(1,D),(D,1),(D,D)\} \subset (H_v^\times / H_v^{\times 2})^2.$$

Proof. The proof follows immediately from the similar arguments of the previous lemma. As in the proof of Lemma 5.3, one can obtain the equation (5.9). Contrary to Lemma 5.3, $(p+1)^2$ is divisible by 16, which follows that $E(F_p)$ has all $\mathfrak{p}^2$-torsion points. Hence we have

$$K_p(R) = F_p = K_p(\sqrt{D}) \tag{5.11}$$

which completes the proof of the lemma. Here we remark that $\sqrt{-q}$ is now a square element in $K_p^\times$. □

Lemma 5.5. *Let v be any prime of H lying above $\mathfrak{q}$. Then the image of λ_v is given by*

$$\{(1,1),(1,\epsilon'\sqrt{-q}D),(\epsilon\sqrt{-q}D,1),(\epsilon\sqrt{-q}D,\epsilon'\sqrt{-q}D)\} \subset (H_v^\times / H_v^{\times 2})^2,$$

where the values ϵ, ϵ' *are either* 1 *or* -1.

Proof. Similarly, since E has bad reduction at all the primes of H above $\mathfrak{q}$, the field extension $K_{\mathfrak{q}}(R)$ over $K_{\mathfrak{q}}$ is ramified. Recall that -1 is not a square in $H_v = K_{\mathfrak{q}}$, and so we have

$$K_{\mathfrak{p}}(R) = K_{\mathfrak{q}}(\sqrt{\sqrt{-q}D}) \quad \text{or} \quad K_{\mathfrak{q}}(\sqrt{-\sqrt{-q}D}).$$

In any case, the assertion of the lemma follows Lemma 5.1. □

Combining all of these lemmas above, we finally obtain the following result.

Proposition 5.6. *Let* $D \equiv 1 \bmod 4$ *be a square-free integer, all of whose prime factors are inert in* K. *For* $E = A^{(D)}$, *we have* $S_2(E) \simeq (\mathcal{O}/2\mathcal{O})^{k+1}$ *where* k *denotes the number of prime factors of* D *which are congruent to* 3 *modulo* 4.

Proof. Let $r \geq k \geq 0$ be integers and write $N = p_1 \cdots p_k$ and $M = p_{k+1} \cdots p_r$. We now assume that $(\alpha, \beta) \in (K^\times/K^{\times 2})^2$ belongs to the image of λ_v for all v. By Lemma 5.1 and the fact that H is unramified over K, α and β have even valuation at all places v of K not dividing qD. Since the class number of K is odd, we may write

$$\begin{aligned} \alpha &\equiv (-1)^a(\sqrt{-q})^b p_1^{m_1} \cdots p_r^{m_r} \bmod K^{\times 2}, \\ \beta &\equiv (-1)^c(\sqrt{-q})^d p_1^{n_1} \cdots p_r^{n_r} \bmod K^{\times 2}, \end{aligned} \tag{5.12}$$

where a, b, c, d and all the m_i, n_i belong to $\{0, 1\}$. Hence the Selmer group $S_2(E) \subset (K^\times/K^{\times 2})^2$ consisting of such pairs (α, β), restricts isomorphically onto

$$(K_{\mathfrak{q}}^\times/K_{\mathfrak{q}}^{\times 2})^2 \times (K_{p_1}^\times/K_{p_1}^{\times 2})^2 \times \cdots \times (K_{p_r}^\times/K_{p_r}^{\times 2})^2.$$

Note that $\sqrt{-q} \in K_p^\times$ is a square if $p \mid N$, and is a non-square if $p \mid M$. Moreover, by using a similar argument, all the p_j with $j \neq i$ are squares in K_{p_i}. Comparing these facts with Lemma 5.3, Lemma 5.4 and Lemma 5.5, it follows that the exponents a and $m_{k+1}, \cdots, m_r$ (resp. c and $n_{k+1}, \cdots, n_r$) are determined by b (resp. d). Moreover, the exponents b and $m_1, \cdots, m_k$ (resp. d and $n_1, \cdots, n_k$) are independent of each other. Hence we conclude that $S_2(E)$ is isomorphic to $(\mathcal{O}/2\mathcal{O})^{k+1}$. □

Corollary 5.7. *Assume that* $k = 0$, *in other words,* $D = M \in \mathscr{M}$. *For* $E = A^{(M)}$, *we have* $S_2(E) \simeq \mathcal{O}/2\mathcal{O}$ *and* $E(H) = \mathcal{O}/2\mathcal{O}$.

Moreover, it is easily seen that the root number of $E = A^{(D)}$ is -1 whenever k is odd. Hence we also have the following corollary.

Corollary 5.8. *Assume that* $k = 1$. *For* $E = A^{(D)}$, *we have* $E(H) = \mathcal{O}^h \oplus \mathcal{O}/2\mathcal{O}$. *In particular, the Mordell-Weil group* $E(H)$ *has* $\mathbb{Q}$*-rank* 1.

Finally, combining with the results of Yang [14], the proposition implies that the 2-primary subgroup of the Tate-Shafarevich group of $\mathbb{Q}$-curves can be arbitrary large.

Corollary 5.9. *Assume that* $\sqrt{q} \geq (12/\pi)D \log D$. *For* $E = A^{(D)}$, *we have*

$$\dim_{\mathbb{F}_2} Ш(E/H)_2 \geq k.$$

Proof. Indeed, Yang proved in Theorem 3.4 of [14] that if $\sqrt{q} \geq (12/\pi)D \log D$, we have $L(E/H, 1) \neq 0$. A theorem of Rubin [11] then implies that the Mordell-Weil group $E(H)$ is finite, and hence $E(H) = \mathcal{O}/2\mathcal{O}$. By Proposition 5.6 and the short exact sequence (5.3), we obtain the inequality

$$\dim_{\mathbb{F}_2}(Ш(E/H)_2)^G \geq k. \quad \square$$

We are also interested in the 2-primary subgroup of the Tate-Shafarevich group $Ш(E/H)(2)$ in Corollary 5.7 and Corollary 5.8. Unfortunately, we do not have any idea at present how to compute its order by elementary means, even though the short exact sequence (5.3) implies that

$$Ш(E/H)(2)^G = 0.$$

However, it does not mean that one always has $Ш(E/H)(2) = 0$. Indeed, Villegas [13] has computed the conjectural order of $Ш(A/H)$ predicted by the conjecture of Birch and Swinnerton-Dyer for all primes $q < 3000$, and the table at the end of his paper shows that the conjectural order of $Ш(A/H)(2)$ is non-trivial, and in fact of order at least 16, when

$$q = 431, 751, 1367, 1399, 1423, 1823, 1879, 2063, 2543, 2687, 2767.$$

Acknowledgment

The author would like to thank John Coates for suggesting this problem and giving helpful advice.

References

[1] A. Brumer, K. Kramer, The rank of elliptic curves, Duke Math. J. 44 (1997) 715–743.
[2] L. Cai, C. Li, S. Zhai, On the 2-part of the Birch and Swinnerton-Dyer conjecture for quadratic twists of elliptic curves, arXiv:1712.01271, 2017.
[3] J. Choi, J. Coates, Iwasawa theory of quadratic twists of $X_0(49)$, Acta Math. Sin. (Engl. Ser.) 34 (2018) 19–28.
[4] J. Coates, C. Goldstein, Some remarks on the main conjecture for elliptic curves with complex multiplication, Amer. J. Math. 105 (1983) 337–366.
[5] J. Coates, M. Kim, Z. Liang, C. Zhao, On the 2-part of the Birch–Swinnerton-Dyer conjecture for elliptic curves with complex multiplication, Münster J. Math. 7 (2014) 83–103.

[6] J. Coates, Y. Li, Y. Tian, S. Zhai, Quadratic twists of elliptic curves, Proc. Lond. Math. Soc. 110 (2014) 357–394.
[7] E. de Shalit, Iwasawa Theory of Elliptic Curves with Complex Multiplication, Perspectives in Mathematics, vol. 3, Academic Press, 1987.
[8] C. Goldstein, N. Schappacher, Séries d'Eisenstein et fonctions L de courbes elliptiques à multiplication complexe, J. Reine Angew. Math. 327 (1981) 184–218.
[9] B. Gross, Arithmetic on Elliptic Curves with Complex Multiplication I, Lect. Notes in Math., vol. 776, Springer-Verlag, Berlin, Heidelberg, New York, 1980.
[10] B. Gross, Minimal models for elliptic curves with complex multiplication, Compos. Math. 45 (1982) 155–164.
[11] K. Rubin, The "main conjectures" of Iwasawa theory for imaginary quadratic fields, Invent. Math. 103 (1991) 25–68.
[12] Y. Tian, X. Yuan, S. Zhang, Genus periods, genus points, and the congruent number problem, Asian J. Math. 21 (2017) 721–744.
[13] F. Villegas, On the square root of special values of certain L-series, Invent. Math. 106 (1991) 549–573.
[14] T. Yang, Nonvanishing of central Hecke L-values and rank of certain elliptic curves, Compos. Math. 117 (1999) 337–359.
[15] C. Zhao, A criterion for elliptic curves with lowest 2-power in $L(1)$, Proc. Camb. Philos. Soc. 121 (1997) 385–400.
[16] C. Zhao, A criterion for elliptic curves with second lowest 2-power in $L(1)$, Proc. Camb. Philos. Soc. 131 (2001) 385–404.
[17] C. Zhao, A criterion for elliptic curves with second lowest 2-power in $L(1)$ (II), Acta Math. Sin. 21 (2005) 961–976.