On the 2-part of the Birch-Swinnerton-Dyer conjecture for elliptic curves with complex multiplication by the ring of integers of $\mathbb{Q}(\sqrt{-7})$

Takumi Yoshida

Abstract

For a modular elliptic curve $A = X_0(49)$ and its quadratic twists $A^{(M)}$, we give equivalent conditions such that the 2-Selmer group $S_2(A^{(M)}/\mathbb{Q})$ is minimal, namely it is of order 2. One of these conditions is described by the L-value $L(A^{(M)}/\mathbb{Q}, 1)$. The other conditions are described by quadratic and biquadratic residue symbol, so explicit and computable (and one can compute the density of M). Also we prove the full Birch-Swinnerton-Dyer conjecture when the equivalent conditions are satisfied. This generalizes a result by J. Coates, Y. Li, Y. Tian and S. Zhai.

1 Introduction

Let E be an elliptic curve defined over $\mathbb{Q}$, and $L(E, s)$ the complex L-series of E. For each square-free nonzero integer $M \neq 1$, we write $E^{(M)}$ for the twist of E by the quadratic extension $\mathbb{Q}(\sqrt{M})/\mathbb{Q}$. For the sake of simplicity, let $E^{(1)} = E$.

Let A be the modular curve $X_0(49)$, which we view as an elliptic curve by taking $[\infty]$ to be the origin of the group law. It is well known that A has complex multiplication by the ring of integers $\mathscr{O}_K = \mathbb{Z}[\frac{1+\sqrt{-7}}{2}]$ of the field $K = \mathbb{Q}(\sqrt{-7})$. The elliptic curve A has a minimal Weierstrass equation given by

$$y^2 + xy = x^3 - x^2 - 2x - 1.$$

We have $A(\mathbb{Q}) = \{[\infty], (2, -1)\}$. The Néron differential $\omega = dx/(2y + x)$ has the fundamental real period $\Omega_\infty = \Gamma(1/7)\Gamma(2/7)\Gamma(4/7)/2\pi\sqrt{7}$. We have

$$L(A, 1)/\Omega_\infty = \frac{1}{2}.$$

For any square-free nonzero integer M, we write ψ_M for the Grössencharacter of $A^{(M)}/K$, and $L(\bar{\psi}_M, s)$ for the corresponding Hecke L-series. Then we have $L(\bar{\psi}_M, s) = L(A^{(M)}, s)$. We define the algebraic part $L^{(alg)}(\bar{\psi}_M, 1)$ of the L-value $L(A^{(M)}, 1)$ by

$$L^{(alg)}(\bar{\psi}_M, 1) = \begin{cases} L(\bar{\psi}_M, 1)\sqrt{M}/\Omega_\infty, \text{ if } M > 0, \\ L(\bar{\psi}_M, 1)\sqrt{-M/7}/\Omega_\infty, \text{ if } M < 0, \end{cases}$$

which is a rational number.

J. Coates, M. Kim, Z. Liang and C. Zhao gave the definition of the adimissibility for positive square-free integers ([2], Definition 4.4). We slightly generalize their definition to all square-free nonzero integers.

Definition 1.1. A square-free nonzero integer M is said to be admissible (for A) if we have $M \equiv 1 \mod 4$ and $M = cp_1 \cdots p_s q_1 \cdots q_t$ $(s, t \geq 0,\ c = \pm 1)$, where p_i and q_j are primes satisfying $\left(\frac{-7}{p_i}\right) = -1$ for any $1 \leq i \leq s$, and $\left(\frac{-7}{q_j}\right) = \left(\frac{-1}{q_j}\right) = 1$ for any $1 \leq j \leq t$. For this M, we define $r(M) = s + 2t$, i.e. the number of prime ideals dividing $M\mathscr{O}_K$.

J. Coates, Y. Li, Y. Tian and S. Zhai proved in [1] Theorem 1.2 the following theorem on $A^{(M)}$ for admissible integers M.

Theorem 1.2. *Let M be an admissible integer, and assume that we have $\left(\frac{-7}{p}\right) = -1$ and $\left(\frac{-1}{p}\right) = 1$ for every prime divisor p of M. Let $S_2(A^{(M)}/\mathbb{Q})$ be the 2-Selmer group of $A^{(M)}/\mathbb{Q}$ (see (2.3)). Then, we have $\mathrm{ord}_2(L^{(alg)}(\bar{\psi}_M, 1)) = r(M) - 1$ and $\#S_2(A^{(M)}/\mathbb{Q}) = 2$. Also the full Birch-Swinnerton-Dyer conjecture is valid for the elliptic curve $A^{(M)}$ over $\mathbb{Q}$, that is,*

$$L^{(alg)}(\bar{\psi}_M, 1) = \frac{\#Ш(A^{(M)}/\mathbb{Q}) \prod_{p|M} c_p}{(\#A^{(M)}(\mathbb{Q}))^2},$$

where $Ш(A^M/\mathbb{Q})$ is the Tate-Shafarevich group of $A^{(M)}$ over $\mathbb{Q}$, and c_p is the Tamagawa number.

The aim of this paper is to generalize the above theorem by considering all admissible integers not necessarily satisfying both $\left(\frac{-7}{p}\right) = -1$ and $\left(\frac{-1}{p}\right) = 1$. We determine all adimissible integers M such that the order of 2-Selmer group $S_2(A^{(M)}/\mathbb{Q})$ is minimal, namely $\#S_2(A^{(M)}/\mathbb{Q}) = 2$, and verify the full Birch-Swinnerton-Dyer conjecture for these M (concerning the full Birch-Swinnerton-Dyer conjecture, see Remark 1.6 (3)).

Definition 1.3. Let M be an admissible integer. Define

$$\mathscr{S}_M = \left\{ d \in \mathbb{Z} \;\middle|\; \begin{array}{l} d \mid M, d \equiv 1 \mod 4 \\ \left(\frac{-1}{p}\right) = -1 \text{ for any } p \mid d \text{ with } \left(\frac{-7}{p}\right) = -1 \\ \left(\frac{M/d}{p}\right) = \left(\frac{-7}{p}\right)_4 \text{ for any } p \mid d \text{ with } \left(\frac{-7}{p}\right) = 1 \\ \left(\frac{d}{p}\right) = 1 \text{ for any } p \mid \frac{M}{d} \text{ with } \left(\frac{-7}{p}\right) = 1 \end{array} \right\},$$

and

$$\mathscr{R}_M = \left\{ D \in \mathbb{Z} \;\middle|\; \begin{array}{l} D|M, D \equiv 1 \mod 4 \\ p \mid D \text{ for any } p \mid M \text{ with } \left(\frac{-7}{p}\right) = \left(\frac{-1}{p}\right) = -1 \\ \left(\frac{-7}{p}\right)_4 = -\left(\frac{D}{p}\right) \text{ for any } p \mid \frac{M}{D} \text{ with } \left(\frac{-7}{p}\right) = \left(\frac{-1}{p}\right) = 1 \end{array} \right\},$$

where $\left(\frac{-7}{p}\right)_4$ denotes the biquadratic residue symbol when $\left(\frac{-7}{p}\right) = 1$. Define $\mathscr{T}_1 = \{1\}$, and for any admissible integer $M \neq 1$, define $\mathscr{T}_M$ inductively by

$$\mathscr{T}_M = \{D \in \mathscr{R}_M | D \neq M, \#\mathscr{T}_D \text{ is odd}\}.$$

Here, the set $\mathscr{S}_M$ is related to the Selmer group $S_2(A^{(M)}/\mathbb{Q})$ of $A^{(M)}$ over $\mathbb{Q}$. The set $\mathscr{T}_M$ is related to $\mathrm{ord}_2(L^{(alg)}(\bar{\psi}_M, 1))$.

The aim of the paper is to prove the following theorem.

Theorem 1.4. *Let M be an admissible integer, and $S_2(A^{(M)}/\mathbb{Q})$ the 2-Selmer group of $A^{(M)}/\mathbb{Q}$. Then, the following conditions are equivalent:*

(*i*) $\#S_2(A^{(M)}/\mathbb{Q}) = 2$.

(*ii*) $\mathrm{ord}_2(L^{(alg)}(\bar{\psi}_M, 1)) = r(M) - 1$.

(*iii*) $\#\mathscr{S}_M$ *is odd.*

(*iv*) $\mathscr{S}_M = \{1\}$.

(*v*) $\#\mathscr{T}_M$ *is odd.*

If these equivalent conditions are satisfied, the full Birch-Swinnerton-Dyer conjecture is valid for the elliptic curve $A^{(M)}$.

Suppose that M is the prime number, $M = p$. The condition (*iv*) in Theorem 1.4 are equivalent to the following condition:

$$\begin{aligned} \text{either } & -\left(\frac{-7}{p}\right) = \left(\frac{-1}{p}\right) = 1 \\ \text{or } & \left(\frac{-7}{p}\right) = \left(\frac{-1}{p}\right) = 1 \text{ and } \left(\frac{-7}{p}\right)_4 = -1. \end{aligned}$$

The density of the primes p which satisfy this condition is 3/8.

The next theorem gives a simple condition on admissible integers M for which one has $\#S_2(A^{(M)}/\mathbb{Q}) > 2$.

Theorem 1.5. *Let M be an admissible integer, and assume that there exists a prime divisor p of M which satisfies $\left(\frac{-7}{p}\right) = \left(\frac{-1}{p}\right) = -1$. Then, we have $\mathscr{T}_M = \emptyset$, and the equivalent conditions of Theorem 1.4 are NOT satisfied. And also we have $\#S_2(A^{(M)}/\mathbb{Q}) > 2$.*

Remark 1.6. (1) If the condition of Theorem 1.2 is satisfied, namely $-\left(\frac{-7}{p}\right) = \left(\frac{-1}{p}\right) = 1$ for every prime divisor p of M, then the condition (*iv*) holds. Thus Theorem 1.4 generalizes Theorem 1.2.

(2) We prove $\#S_2(A^{(M)}/\mathbb{Q}) \geq 2$ in Section 2, and prove $\mathrm{ord}_2(L^{(alg)}(\bar{\psi}_M, 1)) \geq r(M) - 1$ for any admissible integer M in Section 3. So the conditions (*i*) and (*ii*) are the minimal case.

(3) In [3] Theorem B, Cristian D.gonzalez-Aviles verified the full Birch-Swinnerton-Dyer conjecture for $A^{(M)}$, when the value $L^{(alg)}(\bar{\psi}_M, 1)$ is not zero. On the other hand, we can show by Theorem 1.4 that when $L^{(alg)}(\bar{\psi}_M, 1) = 0$, the condition (i) is not satisfied, thus we have
$\#S_2(A^{(M)}/\mathbb{Q}) > 2$.

(4) Let $E/\mathbb{Q}$ be an elliptic curve with complex multiplication by K satisfying $L(E, 1) \neq 0$. Then in [6], Rubin proves that the rank of $E(\mathbb{Q})$ is 0. Let Ω_E be the period for E, $Ш(E)$ the Tate-Shafarevich group, N the conductor, and c_p the Tamagawa factor for any prime $p \mid N$. Rubin also proves that, when $p \nmid \#\mathscr{O}_K^\times$, the p-part of the Birch-Swinnerton-Dyer conjecture is valid, i.e,

$$\mathrm{ord}_p\left(\frac{L(E,1)}{\Omega_E}\right) = \mathrm{ord}_p\left(\frac{\#Ш(E)\prod_{p|N} c_p}{(\#E_{tor}(\mathbb{Q}))^2}\right).$$

Therefore, in order to prove that the full Birch-Swinnerton-Dyer conjecture is valid for the elliptic curve $A^{(M)}$ when the equivalent conditions are satisfied, we only have to show that the 2-part of the Birch-Swinnerton-Dyer conjecture is valid.

Corollary 1.7. *Let $M = p_1 \dots p_s q_1 \dots q_t > 0$ be an admissible integer, where p_i and q_j are as Definition 1.1. Let $P = p_1 \dots p_s$, and assume*

$$\left(\frac{-1}{p_i}\right) = 1 \text{ for any } i,$$

$$\left(\frac{P}{q_j}\right) = -\left(\frac{-7}{q_j}\right)_4 \text{ for any } j,$$

and

$$\left(\frac{q_j}{q_k}\right) = 1 \text{ for any } j \neq k.$$

Then, the equivalent conditions (i)-(v) in Theorem 1.4 are satisfied, and consequently the full Birch-Swinnerton-Dyer conjecture is valid for $A^{(M)}/\mathbb{Q}$.

We will prove this corollary in Section 4.

Fix $s \geq 0$ and $t > 0$. By Chebotarev's density theorem, for any s and t, there exist infinitely many $(p_1, \dots, p_s, q_1, \dots, q_t)$ which satisfy the assumptions of Corollary 1.7, and thus, for these $M = p_1 \dots p_s q_1 \dots q_t$, the full Birch-Swinnerton-Dyer conjecture is valid for $A^{(M)}/\mathbb{Q}$. See Section 6 for numerical examples to which one can apply Corollary 1.7.

The main part of Theorem 1.4 is the equivalence of (i), (iii) and (iv). We will identify the 2-Selmer group $S_2(A^{(M)}/\mathbb{Q})$ with a subgroup of $K^\times/K^{\times 2}$ by Kummer theory. Then, by studying the local condition, we will prove the subgroup $S_2(A^{(M)}/\mathbb{Q}) \cap \mathbb{Q}^\times/(K^{\times 2} \cap \mathbb{Q}^\times)$ corresponds to $\mathscr{S}_M$ (Theorem 2.12), and prove the equivalence of (i), (iii) and (iv) of Theorem 1.4 (Corollary 2.13).

We will prove the equivalence of (iii) and (v) of Theorem 1.4 by using the following theorem:

Theorem 1.8. *Let $M \neq 1$ be an admissible integer. Then, the number $\sum_{D \in \mathscr{R}_M} \#\mathscr{S}_D$ is even.*

In Section 2, we identify the 2-Selmer group $S_2(A^{(M)}/\mathbb{Q})$ with a subgroup of $K^\times/K^{\times 2}$. By studying the local condition, we determine the subgroup $S_2(A^{(M)}/\mathbb{Q}) \cap \mathbb{Q}^\times/(K^{\times 2} \cap \mathbb{Q}^\times)$ of the 2-Selmer group (Proposition 2.11). Then we make a natural bijection $S_2(A^{(M)}/\mathbb{Q}) \cap \mathbb{Q}^\times/(K^{\times 2} \cap \mathbb{Q}^\times) \cong \mathscr{S}_M$ (Theorem 2.12), and prove the equivalence of (i) and (iii) of Theorem 1.4 (Corollary 2.13).

In Section 3, we define the "imprimitive" Hecke L-series $L_S(\bar{\psi}_M, 1)$ where M is a divisor of an element $\mathfrak{M} \in \mathscr{O}_K$. We recall Zhao's method (Proposition 3.1), which considers the 2-adic vauation of the sum of $L_S(\bar{\psi}_M, 1)/\Omega_\infty$, where M runs over divisors of $\mathfrak{M}$. In order to verify the relationship between the 2-adic valuation of $L^{(alg)}(\bar{\psi}_M, 1)/\Omega_\infty$ and that of $L_S(\bar{\psi}_M, 1)/\Omega_\infty$, we study the 2-adic valuation of the Euler factor of the Hecke L-series $L(\bar{\psi}_M, 1)$. Then, we prove the equivalence of (ii) and (v) of Theorem 1.4 by induction on $r(M)$ (Proposition 3.4).

In Section 4, we prove the equivalence of (iii) and (v) of Theorem 1.4 assuming Theorem 1.8, and complete the proof of Theorem 1.4.

Finally, in Section 5, we prove Theorem 1.8.

The author wishes to thank Professors Takeshi Saito and Masato Kurihara, for giving him much helpful advice and ideas and pointing out mistakes during the preparation of this paper.

2 2-Selmer groups

The aim of this section is to prove the equivalence of (i) and (iii) of Theorem 1.4. For this aim, first, we consider the cohomology group of 2-torsion points of elliptic curves and the 2-Selmer group.

Let G be a profinite group acting continuously on a free $\mathbb{Z}/4\mathbb{Z}$-module M of rank 2. Assume that for a basis a, b of M, the image of $G \to \mathrm{Aut}(M)$ is a subgroup of the group $\left\{ \begin{pmatrix} \pm 1 & 0 \\ 0 & \pm 1 \end{pmatrix}, \begin{pmatrix} 0 & \pm 1 \\ \pm 1 & 0 \end{pmatrix} \right\} \subseteq \mathrm{Aut}(M) = \mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z})$ of order 8. We identify $\bar{M} = M/2M$ with $M[2] \subseteq M$ and let H be the kernel of $G \to \mathrm{Aut}(\bar{M})$.

Lemma 2.1. *The restriction map $H^1(G, \bar{M}) \to H^1(H, \bar{M})^G = \mathrm{Hom}_G(H, \bar{M})$ is an isomorphism.*

Proof. If we have $G = H$, it is trivial. We prove this lemma when $G \neq H$. Then $\bar{M}$ is isomorphic to $\mathbb{F}_2[G/H]$ as a G/H-module. So for any $i > 0$ we have $H^i(G/H, \bar{M}) = 0$, and the lemma follows from the inflation-restriction exact sequence. □

By Lemma 2.1, we identify $H^1(G, \bar{M})$ with $H^1(H, \bar{M})^G = \mathrm{Hom}_G(H, \bar{M})$. The exact sequence $0 \to \bar{M} \to M \to \bar{M} \to 0$ defines a commutative diagram

$$\begin{array}{ccc} \bar{M}^G & \longrightarrow & H^1(G, \bar{M}) \\ \downarrow & & \downarrow \\ \bar{M} & \longrightarrow & \mathrm{Hom}(H, \mathbb{F}_2) \otimes \bar{M} \end{array}$$

of boundary morphisms. We identify $\mathbb{F}_2$ with ± 1 and let $\chi_a, \chi_b \in \mathrm{Hom}(H, \mathbb{F}_2)$ denote the character of H defining the action on a and b.

Lemma 2.2. *The lower horizontal arrow is the morphism sending $\bar{a}$ to $\chi_a \otimes a$ and $\bar{b}$ to $\chi_b \otimes b$.*

Proof. Since M is decomposed into the direct sum of $a \cdot \mathbb{Z}/4\mathbb{Z}$ and $b \cdot \mathbb{Z}/4\mathbb{Z}$ as an H-module, the lemma follows. □

Let F be a field of characteristic $\neq 2$, and E an elliptic curve over F. We assume $\dim_{\mathbb{F}_2} E[2](F) = 1$. Let $K = F(E[2])$ and $\{P, Q\} = E[2] - E[2](F)$. Let $G = \mathrm{Gal}(\bar{F}/F)$ and $M = E[4]$. We assume that we can choose a basis $P', Q' \in E[4]$ such that the image of the action $G \to \mathrm{Aut}(E[4])$ is $\left\{ \begin{pmatrix} \pm 1 & 0 \\ 0 & \pm 1 \end{pmatrix}, \begin{pmatrix} 0 & \pm 1 \\ \pm 1 & 0 \end{pmatrix} \right\} \subset \mathrm{Aut}(E[4])$. Then the assumption at the beginning of this section is satisfied. We have $H = \mathrm{Gal}(\bar{F}/K)$. We identify $\mathrm{Hom}(H, \mathbb{F}_2) \cong K^\times/K^{\times 2}, \chi \mapsto \alpha$, where $\ker(\chi) = \mathrm{Gal}(\bar{F}/K(\alpha))$. Let F' be an extension of F. If $F' \supseteq K$, we identify

$$\begin{aligned} H^1(F', E[2]) &= (F'^\times/F'^{\times 2}) \otimes E[2] \\ &= (F'^\times/F'^{\times 2})^2, \end{aligned} \tag{2.1}$$

where the second identification is defined by

$$(F'^\times/F'^{\times 2}) \otimes E[2] \to (F'^\times/F'^{\times 2})^2, \alpha \otimes P + \alpha' \otimes Q \mapsto (\alpha, \alpha').$$

If $F' \not\supseteq K$, let $K' = F'K$ be a composite field, and $\sigma \in \mathrm{Gal}(K'/F')$ the nontrivial element. Then we identify

$$\begin{aligned} H^1(F', E[2]) &= ((K'^\times/K'^{\times 2}) \otimes E[2])^{\mathrm{Gal}(\bar{F}'/F')} \\ &= K'^\times/K'^{\times 2}, \end{aligned} \tag{2.2}$$

where the second identification is

$$K'^\times/K'^{\times 2} \to ((K'^\times/K'^{\times 2}) \otimes E[2])^{\mathrm{Gal}(\bar{F}'/F')}, \alpha \mapsto \alpha \otimes P + \sigma(\alpha) \otimes Q.$$

Now assume $F = \mathbb{Q}$ and $K \not\subseteq \mathbb{R}$. We have the exact sequence of Galois modules

$$0 \longrightarrow E[2] \longrightarrow E(\overline{\mathbb{Q}}) \xrightarrow{2} E(\overline{\mathbb{Q}}) \longrightarrow 0$$

which leads to a short exact sequence

$$0 \longrightarrow E(\mathbb{Q})/2E(\mathbb{Q}) \longrightarrow H^1(\mathbb{Q}, E[2]) \longrightarrow H^1(\mathbb{Q}, E)[2] \longrightarrow 0\ .$$

This exact sequence has an analogue for $\mathbb{Q}_p$ for any prime number p and for $\mathbb{R}$. Hence we obtain the following commutative diagram with exact rows

$$\begin{array}{ccccccccc} 0 & \longrightarrow & E(\mathbb{Q})/2E(\mathbb{Q}) & \xrightarrow{\delta} & H^1(\mathbb{Q}, E[2]) & \longrightarrow & H^1(\mathbb{Q}, E)[2] & \longrightarrow & 0 \\ & & \downarrow & & \downarrow \mathrm{Res} & & \downarrow \mathrm{Res} & & \\ 0 & \longrightarrow & \prod_p E(\mathbb{Q}_p)/2E(\mathbb{Q}_p) & \xrightarrow{\prod_p \delta_p} & \prod_p H^1(\mathbb{Q}_p, E[2]) & \longrightarrow & \prod_p H^1(\mathbb{Q}_p, E)[2] & \longrightarrow & 0. \end{array}$$

where the products run over all prime numbers p and $p = \infty$ (if $p = \infty$, we define $\mathbb{Q}_\infty = \mathbb{R}$). We define the 2-Selmer group of E over $\mathbb{Q}$ by

$$S_2(E/\mathbb{Q}) = \ker\left(H^1(\mathbb{Q}, E[2]) \to \prod_p \frac{H^1(\mathbb{Q}_p, E[2])}{\mathrm{im}\delta_p}\right). \tag{2.3}$$

Through the identification (2.2), we have $S_2(E/\mathbb{Q}) \subset K^\times/K^{\times 2}$. By the identification (2.2), the cohomology group $H^1(\mathbb{R}, E[2]) = \mathbb{C}^\times/\mathbb{C}^{\times 2}$ is trivial. Thus we will consider only the case where p is a prime number. For any prime number p, write $\mathscr{O}_p$ for the ring of integers of $K_p = \mathbb{Q}_p K$, and write G_p for the Galois group $\mathrm{Gal}(K_p/\mathbb{Q}_p)$.

Lemma 2.3. (1) *If $p \neq 2$ and $K \not\subseteq \mathbb{Q}_p$, then we have $\#(\mathrm{im}\delta_p) = 2$.*

(2) *If $p \neq 2$ and $K \subseteq \mathbb{Q}_p$, then we have $\#(\mathrm{im}\delta_p) = 4$.*

(3) *Assume that E has good reduction at 2. We have $\mathrm{im}\delta_2 \subseteq (\mathscr{O}_2^\times/\mathscr{O}_2^{\times 2}) \otimes E[2]$.*

(4) *If E has good reduction at p and $p \neq 2$, then we have $\mathrm{im}\delta_p = ((\mathscr{O}_p^\times/\mathscr{O}_p^{\times 2}) \otimes E[2])^{G_p}$.*

Proof. If $p \neq 2$, we have

$$\#E(\mathbb{Q}_p)/2E(\mathbb{Q}_p) = \#E[2](\mathbb{Q}_p) = \begin{cases} 2 & (\text{if } K \not\subseteq \mathbb{Q}_p), \\ 4 & (\text{otherwise}). \end{cases}$$

If E has good reduction at $p \neq 2$, since the multiplication-by-2 map $E \to E$ over $\mathscr{O}_p$ is finite and étale, we have $\mathrm{im}\delta_p \subseteq ((\mathscr{O}_p^\times/\mathscr{O}_p^{\times 2}) \otimes E[2])^{G_p}$. If $p = 2$, the lemma follows from Proposition 3.6 in [4]. □

Let $K = \mathbb{Q}(\sqrt{-7})$ and $E = A^{(M)}$ where M is an admissible integer. We regard as $K \subseteq \mathbb{Q}_2$ by choosing a square root of -7 congruent to 3 mod 8 in $\mathbb{Q}_2$. Making a change of variables $x = X/4 + 2, y = Y/8 - X/8 - 1$, we obtain the following equation for A:

$$Y^2 = X^3 + 21X^2 + 112X.$$

Let $M \neq 1$ be any square-free integer. Then the curve $E = A^{(M)}$ has an equation

$$E : y^2 = x^3 + 21Mx^2 + 112M^2x.$$

Let $P = ((-21 + \sqrt{-7})M/2, 0), Q = ((-21 - \sqrt{-7})M/2, 0)$ be a generator of $E[2]$.

Lemma 2.4. (1) *We have $\mathbb{Q}(E[4]) = \mathbb{Q}(\sqrt{M\sqrt{-7}}, \sqrt{-1})$.*

(2) *There exists an isomorphism $E[4] \cong (\mathbb{Z}/4\mathbb{Z})^2$ of $\mathbb{Z}/4\mathbb{Z}$-module such that the image of the natural action $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}(E[4])$ is the group $\left\{\begin{pmatrix} \pm 1 & 0 \\ 0 & \pm 1 \end{pmatrix}, \begin{pmatrix} 0 & \pm 1 \\ \pm 1 & 0 \end{pmatrix}\right\} \subset \mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z})$ of order 8.*

Proof. Let

$$P' = ((-7-\sqrt{-7})M, \sqrt{M\sqrt{-7}}(\sqrt{-7}+7)),$$

and

$$Q' = ((-7+\sqrt{-7})M, \sqrt{M\sqrt{-7}}\sqrt{-1}(-\sqrt{-7}+7)).$$

Then we have $2P' = P$ and $2Q' = Q$, and we have an isomorphism $(\mathbb{Z}/4\mathbb{Z})^2 \cong E[4]$ defined by $(a,b) \mapsto aP' + bQ'$. Thus we have $\mathbb{Q}(E[4]) = \mathbb{Q}(\sqrt{M\sqrt{-7}}, \sqrt{-1})$ and the isomorphism satisfies the statement. □

By this lemma, the module $E[4]$ satisfies the assumptions at the beginning of this section. By Lemma 2.2, the map $E(K)/2E(K) \to H^1(K, E[2]) \subseteq (K^\times/K^{\times 2})^2$ maps P to $(-M\sqrt{-7}, 1)$, since $K(\sqrt{-M\sqrt{-7}}) = K(P')$. Similarly, Q is mapped to $(1, M\sqrt{-7})$.

We identify $S_2(E/\mathbb{Q})$ with

$$\ker\left(K^\times/K^{\times 2} \to \prod_p \frac{K_p^\times/K_p^{\times 2} \otimes E[2]}{\mathrm{im}\delta_p}\right).$$

Proposition 2.5. (1) *We have* $(-3,-3) \in \mathrm{im}\delta_2$.

(2) *We have* $\mathrm{im}\delta_7 = \{1, -M\sqrt{-7}\} \subseteq K_7^\times/K_7^{\times 2}$.

(3) *If* $p \mid M$ *and* $\left(\frac{-7}{p}\right) = -1$, *then we have* $\mathrm{im}\delta_p = \{1, -M\sqrt{-7}\}$ $\subseteq K_p^\times/K_p^{\times 2}$.

(4) *If* $p \mid M$ *and* $\left(\frac{-7}{p}\right) = 1$, *then we have*

$$\begin{aligned}\mathrm{im}\delta_p &= \{(1,1), (-M\sqrt{-7}, 1), (1, M\sqrt{-7}), (-M\sqrt{-7}, M\sqrt{-7})\} \\ &\subseteq (K_p^\times/K_p^{\times 2})^2.\end{aligned}$$

Proof. (2)(3) We have $P + Q \in E(\mathbb{Q}) \subseteq E(\mathbb{Q}_p)$. Thus, we have

$$\begin{aligned}\mathrm{im}\delta_p &\supseteq \delta_p\{O, P+Q\} \\ &= \{1, -M\sqrt{-7}\}.\end{aligned}$$

Since $-M\sqrt{-7}$ is a prime element of K_p, we have $-M\sqrt{-7} \neq 1$ in $K_p^\times/K_p^{\times 2}$. Therefore, by Lemma 2.3 (1), this inclusion must be an equality.

(4) If $p \mid M$ and $\left(\frac{-7}{p}\right) = 1$, then we have $P, Q \in E(K) \subseteq E(\mathbb{Q}_p)$. Thus, we have

$$\begin{aligned}\mathrm{im}\delta_p &\supseteq \delta_p\{O, P, Q, P+Q\} \\ &= \{(1,1), (-M\sqrt{-7}, 1), (1, M\sqrt{-7}), (-M\sqrt{-7}, M\sqrt{-7})\}.\end{aligned}$$

Since $\pm M\sqrt{-7}$ are prime elements of K_p, we have $\pm M\sqrt{-7} \neq 1$ in $\mathbb{Q}_p^\times/\mathbb{Q}_p^{\times 2}$. Therefore, by Lemma 2.3 (2), this inclusion must be an equality.

(1)

[I] The case $M \equiv 1 \bmod 8$.
Since $A^{(M)}$ is isomorphic to A over $\mathbb{Q}_2$, we may assume $M = 1$. Let $R = (-1, 2\sqrt{-23}) \in A(\mathbb{Q}_2)$, and we will find a point $R' = (s,t) \in A(\mathbb{Q}_2(\sqrt{-1}))$ such that $2R' = \pm R$. By duplication formula for elliptic curves, we have

$$\frac{s^4 - 2 \cdot 112 s^2 + 112^2}{4(s^3 + 21s^2 + 112s)} = -1.$$

Thus, we get

$$s^4 + 4s^3 - 140s^2 + 448s + 12544 = 0.$$

Let $f(s)$ be the left-hand side. Then we have

$$\frac{f(72 - 48\sqrt{-1} + 64x)}{8192} \equiv \sqrt{-1}x + \sqrt{-1} \bmod (1 + \sqrt{-1}).$$

Therefore, by Hensel's lemma, there exists an element $\alpha \in \mathbb{Z}_2[\sqrt{-1}]$ such that the equation $f(s) = 0$ has a solution $s = 72 - 48\sqrt{-1} + 64\alpha$. For this s, we have

$$t^2 = s^3 + 21s^2 + 112s \equiv 2^6(-873 - 12288\sqrt{-1}) \bmod 2^{11}.$$

By Hensel's lemma again, there exists $\beta \in \mathbb{Z}_2[\sqrt{-1}]$ such that this equation has a solution $t = 104\sqrt{-1} + 128\beta$. When $\sigma \in \mathrm{Gal}(\mathbb{Q}_2(\sqrt{-1})/\mathbb{Q}_2)$ is nontrivial, the x-coordinate of $R' - R'^{\sigma}$ is

$$\left(\frac{t + t^{\sigma}}{s - s^{\sigma}}\right)^2 - 21 - s - s^{\sigma} \equiv -5 \bmod 16.$$

Since $R'^{\sigma} - R'$ is an element of $A[2]$, we have $R'^{\sigma} - R' = Q$, and

$$\delta_2(2R') = (1, -1).$$

Since we have $\mathrm{im}\delta_2 \ni \delta_2(P + Q) = (-\sqrt{-7}, \sqrt{-7})$,

$$\delta_2(2R' + P + Q) = (-\sqrt{-7}, -\sqrt{-7}) = (-3, -3).$$

[II] The case $M \equiv 5 \bmod 8$.
Since $A^{(M)}$ is isomorphic to $A^{(5)}$ over $\mathbb{Q}_2$, we may assume $M = 5$. Let $R = (-60, 4\sqrt{-375}) \in A^{(5)}(\mathbb{Q}_2)$. As [I], we can prove that there exist elements $\alpha, \beta \in \mathbb{Z}_2[(\sqrt{-3} + 1)/2]$ such that $R' = (s,t) \in A^{(5)}(\mathbb{Q}_2(\sqrt{-3}))$ satisfies $2R' = \pm R$, where

$$s = 58 + 18\sqrt{-3} + 128\alpha, t = 10 - 6\sqrt{-3} + 64\beta.$$

If $\sigma \in \mathrm{Gal}(\mathbb{Q}_2(\sqrt{-3})/\mathbb{Q}_2)$ is nontrivial, then the x-coordinate of $R'^{\sigma} - R'$ is congruent to 0 modulo 32. Thus we have $R' - R'^{\sigma} = P + Q$ and then

$$\delta_2(2R') = (-3, -3).$$

□

Corollary 2.6. *For any prime number p, let* $\mathrm{Gal}(K/\mathbb{Q}) \to \mathrm{Aut}(H^1(\mathbb{Q}_p, E[2]))$ $\subset \mathrm{Aut}((K_p^\times/K_p^{\times 2})\otimes E[2])$ *be the group action defined by the natural action* $\mathrm{Gal}(K/\mathbb{Q}) \to \mathrm{Aut}(E[2])$.

(1) *If $p \neq 2, 7$, then* $\mathrm{im}\delta_p$ *is stable by the action.*

(2) *The intersection* $(\mathscr{O}_7^\times/\mathscr{O}_7^{\times 2}) \cap \mathrm{im}\delta_7$ *is trivial.*

Proof. (1) If $p \mid M$, we have $\left(\frac{-1}{p}\right) = 1$ or $\left(\frac{-7}{p}\right) = -1$ since M is admissible. In both cases, we have $-1 \in K_p^{\times 2}$, and the statement follows from Proposition 2.5 (3) and (4). If $p \nmid 14M$, the statement is clear from Lemma 2.3 (4).

(2) This is clear from Proposition 2.5 (2).

□

Proposition 2.7. *We regard the* 2*-Selmer group* $S_2(E/\mathbb{Q})$ *as a subgroup of* $K^\times/K^{\times 2}$.

(1) *All elements of* $S_2(E/\mathbb{Q})$ *are represented by divisors of* $M\sqrt{-7}$.

(2) *We have* $S_2(E/\mathbb{Q}) = \delta(E[2](\mathbb{Q}))$ *if and only if the intersection* $S_2(E/\mathbb{Q}) \cap \mathbb{Q}^\times/(K^{\times 2} \cap \mathbb{Q}^\times)$ *is trivial.*

Proof. (1) Let α be any element of $S_2(E/\mathbb{Q})$. Since $\mathscr{O}_K$ is a principal ideal domain, we may assume α is a square-free element of $\mathscr{O}_K$. By Lemma 2.3 (3) and (4), we have $\mathrm{im}\delta_p \subseteq (\mathscr{O}_p^\times/\mathscr{O}_p^{\times 2})\otimes E[2]$ for every prime p not dividing $7M$. Therefore α is a divisor of $M\sqrt{-7}$.

(2) If $S_2(E/\mathbb{Q}) \not\supseteq \delta(E[2](\mathbb{Q}))$, then there exists a square-free element $\alpha \in S_2(E/\mathbb{Q})$ which is not 1 or $-M\sqrt{-7}$, and which is a divisor of $M\sqrt{-7}$. If necessary, we replace α with the square-free element $\beta \in \mathscr{O}_K$ which satisfies $\beta \equiv -M\sqrt{-7}\alpha \mod K^{\times 2}$, we may assume $\alpha \mid M$. If α is not a rational number, there exists a prime $\mathfrak{p}$ of K which satisfies $\mathfrak{p} \mid (\alpha)$ and $\mathfrak{p} \nmid (\bar{\alpha})$. Thus $\alpha\bar{\alpha} \neq 1$ in $K^\times/K^{\times 2}$. Since M is admissible and α is a divisor of M, by next lemma (Lemma 2.8), we have $\alpha \equiv \pm 1 \mod 4$, and so $\alpha\bar{\alpha} \equiv 1 \mod 4$. By Proposition 2.5 (1) and Corollary 2.6, we have $\alpha\bar{\alpha} \in S_2(E/\mathbb{Q}) \cap \mathbb{Q}^\times/(K^{\times 2} \cap \mathbb{Q}^\times)$, and this group is nontrivial.

□

Lemma 2.8. *For any integer M, the following conditions are equivalent:*

(*i*) *The integer M is admissible.*

(*ii*) *We can write $M = \pi_1 \cdots \pi_n$, where for any i, the prime elements π_i of K satisfy $(\pi_i, \sqrt{-7}) = 1$ and $\pi_i \equiv 1 \mod 4$.*

Proof. First, suppose that $M = \pm p_1 \cdots p_s q_1 \cdots q_t$ is admissible. Then, for any i, one of the elements $\pm p_i$ is a prime element of K and is congruent to 1 modulo 4. For any j, we can write $q_j = \pi\bar{\pi}$ since $\mathscr{O}_K$ is a principal ideal domain and $\mathrm{N}_{K/\mathbb{Q}}(\alpha) > 0$ for any $\alpha \in K^\times$. Since $(\mathscr{O}_K/4\mathscr{O}_K)^\times$ is represented by ± 1 and $\pm\sqrt{-7}$,

we can assume $\pi \equiv 1$ or $\sqrt{-7} \mod 4$. If $\pi \equiv \sqrt{-7} \mod 4$, we have $q_j = \pi\bar{\pi} \equiv 7 \mod 4$, which is a contradiction. Thus $\pi \equiv \bar{\pi} \equiv 1 \mod 4$. As a result, we can write $M = c\pi_1 \cdots \pi_n$, where $c = \pm 1$ and $\pi_i \equiv 1 \mod 4$ for any i. Since $M \equiv 1 \mod 4$, we have $c = 1$, and we get (ii).

Next, suppose that (ii) is satisfied. If we have $\pi_i \in \mathbb{Q}$, the prime number $p = |\pi_i|$ satisfies $\left(\frac{-7}{p}\right) = -1$. If we have $\pi_i \notin \mathbb{Q}$, the prime number $q = \pi_i\bar{\pi}_i$ satisfies $\left(\frac{-7}{q}\right) = 1$ and $\left(\frac{-1}{q}\right) = 1$. As a result, M is admissible. □

Proposition 2.9. *Assume $p \neq 2$. Let $d \in \mathbb{Z}$ be a divisor of M. The element $dP + dQ \in H^1(\mathbb{Q}_p, E[2])$ belongs to $\mathrm{im}\delta_p$ if and only if the following conditions are satisfied:*

(i) *When $p \mid M$ and $\left(\frac{-7}{p}\right) = -1$, we have $\left(\frac{-1}{p}\right) = -1$ if $p \mid d$.*

(ii) *When $p \mid M$ and $\left(\frac{-7}{p}\right) = 1$, we have $\left(\frac{-7}{p}\right)_4 = \left(\frac{M/d}{p}\right)$ if $p \mid d$ and we have $\left(\frac{d}{p}\right) = 1$ if $p \nmid d$.*

(iii) *When $p = 7$, we have $\left(\frac{d}{7}\right) = 1$.*

When $p \mid (M/d)$ and $\left(\frac{-7}{p}\right) = -1$, or when $p \nmid 14M$, we always have $dP + dQ \in \mathrm{im}\delta_p$.

Proof. (i) When $p \mid M$ and $\left(\frac{-7}{p}\right) = -1$, the condition $dP + dQ \in \mathrm{im}\delta_p$ is satisfied if and only if

$$d = 1 \text{ or } -M\sqrt{-7} \text{ in } K_p^\times / K_p^{\times 2}$$

by our assumption and Lemma 2.5 (3). We have $d = 1$ in $K_p^\times / K_p^{\times 2}$ if and only if $p \nmid d$. If $p \mid d$, applying the following lemma (Lemma 2.10) to the element $-M\sqrt{-7}/d$, the condition $d = -M\sqrt{-7}$ in $K_p^\times / K_p^{\times 2}$ is equivalent to the condition $\left(\frac{-1}{p}\right) = -1$.

(ii) When $p \mid M$ and $\left(\frac{-7}{p}\right) = 1$, the condition $dP + dQ \in \mathrm{im}\delta_p$ is satisfied if and only if

$$d = 1 \text{ or } M\sqrt{-7} \text{ in } K_p^\times / K_p^{\times 2}$$

by Lemma 2.5 (4). If $p \nmid d$, the condition $d = 1$ in $K_p^\times / K_p^{\times 2}$ is equivalent to $\left(\frac{d}{p}\right) = 1$. Since $\left(\frac{-7}{p}\right) = 1$, we have $\left(\frac{-1}{p}\right) = 1$ because p is admissible. So if $p \mid d$, the condition $d = -M\sqrt{-7}$ in $K_p^\times / K_p^{\times 2}$ is equivalent to the condition $\left(\frac{-7}{p}\right)_4 = \left(\frac{M/d}{p}\right)$.

(iii) When $p = 7$, by Lemma 2.5 (2), the condition $dP + dQ \in \mathrm{im}\delta_7$ is satisfied if and only if

$$d = 1 \text{ in } K_7^\times / K_7^{\times 2},$$

that is, $\left(\frac{d}{7}\right) = 1$.

When $p \nmid 14M$, the prime p does not divide d, so by Lemma 2.3 (4), we have

$$dP + dQ \in ((\mathscr{O}_p^\times / \mathscr{O}_p^{\times 2}) \otimes E[2])^{G_p} = \mathrm{im}\delta_p.$$

□

Lemma 2.10. *Let q be an odd prime. Then we have*

$$\mathbb{F}_q^\times \cap \mathbb{F}_{q^2}^{\times 4} = \begin{cases} \mathbb{F}_q^{\times 2} \text{ if } q \equiv 1 \mod 4, \\ \mathbb{F}_q^\times \text{ if } q \equiv -1 \mod 4. \end{cases}$$

Proof. Identifying $\mathbb{F}_{q^2}^\times$ with $\mathbb{Z}/(q^2-1)\mathbb{Z}$, the group $\mathbb{F}_q^\times$ is identified with $(q+1)\mathbb{Z}/(q^2-1)\mathbb{Z}$. So we have

$$\begin{aligned} \mathbb{F}_q^\times \cap \mathbb{F}_{q^2}^{\times 4} &= (q+1)\mathbb{Z}/(q^2-1)\mathbb{Z} \cap 4\mathbb{Z}/(q^2-1)\mathbb{Z} \\ &= \begin{cases} 2(q+1)\mathbb{Z}/(q^2-1)\mathbb{Z} \text{ if } q \equiv 1 \mod 4, \\ (q+1)\mathbb{Z}/(q^2-1)\mathbb{Z} \text{ if } q \equiv -1 \mod 4, \end{cases} \end{aligned}$$

and the lemma follows. □

Proposition 2.11. *Let M be an admissible integer. Then, a divisor $d \in \mathbb{Z}$ of M is an element of the group $S_2(A^{(M)}/\mathbb{Q}) \cap \mathbb{Q}^\times/(K^{\times 2} \cap \mathbb{Q}^\times)$ if and only if d satisfies the following conditions:*

(*i*) *If $p \mid d$ and $\left(\frac{-7}{p}\right) = -1$, then $\left(\frac{-1}{p}\right) = -1$.*

(*ii*) *If $p \mid d$ and $\left(\frac{-7}{p}\right) = 1$, then $\left(\frac{-7}{p}\right)_4 = \left(\frac{M/d}{p}\right)$.*

(*iii*) *If $p \mid (M/d)$ and $\left(\frac{-7}{p}\right) = 1$, then $\left(\frac{d}{p}\right) = 1$.*

(*iv*) $d \equiv 1 \mod 4$.

Proof. By Proposition 2.9, we only have to show the following statement; if d satisfies all of the conditions from (*i*) to (*iii*) of Proposition 2.11, then we have $\left(\frac{d}{7}\right) = 1$ if and only if we have $d \equiv 1 \mod 4$. For any such d, since $d \mid M$, we have

$$d = c \prod_i p_i \prod_j (-q_j)$$

where $p_i \equiv 1 \mod 4$, $q_j \equiv -1 \mod 4$, and $c = \pm 1$. By (*i*), for any i, the Legendre symbol $\left(\frac{-7}{p_i}\right)$ is 1, so we have $\left(\frac{p_i}{7}\right) = 1$. Since M is admissible, so for any j, the Legendre symbol $\left(\frac{q_j}{7}\right)$ is -1, so we have $\left(\frac{-q_j}{7}\right) = 1$. As a result, we have $\left(\frac{d}{7}\right) = 1$ if and only if we have $c = 1$, i.e, $d \equiv 1 \mod 4$. □

Theorem 2.12. *Let M be an admissible integer, and we identify the 2-Selmer group $S_2(A^{(M)}/\mathbb{Q})$ with the subgroup of $K^\times/K^{\times 2}$. Let $\mathscr{S}_M$ be the same as the one introduced in Section 1. Then, the natural map from $\mathscr{S}_M$ to $S_2(A^{(M)}/\mathbb{Q}) \cap \mathbb{Q}^\times/(K^{\times 2} \cap \mathbb{Q}^\times)$ is bijective.*

Proof. This follows from Proposition 2.11. □

Corollary 2.13. *Let M be an admissible integer. Then, the following conditions are equivalent:*

(*i*) $\#S_2(A^{(M)}/\mathbb{Q}) = 2$.

(*ii*) $\#\mathscr{S}_M$ *is odd.*

(*iii*) $\mathscr{S}_M = \{1\}$.

Proof. By Proposition 2.7 (ii), the condition $\#S_2(A^{(M)}/\mathbb{Q}) = 2$ is satisfied if and only if $\dim_{\mathbb{F}_2} S_2(A^{(M)}/\mathbb{Q}) \cap \mathbb{Q}^\times/(K^{\times 2} \cap \mathbb{Q}^\times) = 0$. Therefore, the corollary follows from Theorem 2.12. □

3 2-adic valuation of $L^{(alg)}(\bar{\psi}_M, 1)$

The aim of this section is to prove the equivalence of (*ii*) and (*v*) of Theorem 1.4. In this section, first, we start by recalling Zhao's method ([1] Section 4) without proof.

Let $\pi_1, \ldots, \pi_m$ be any sequence of distinct prime elements of K such that, for all $1 \leq n \leq m$, we have $(\pi_n, \sqrt{-7}) = 1$ and $\pi_n \equiv 1 \mod 4$. Define

$$\mathfrak{M} = \pi_1 \cdots \pi_m.$$

Let $\mathfrak{D}$ be the set of all divisors of $\mathfrak{M}$, which are given by the product over all elements of any subset of $S = \{\pi_1, \ldots, \pi_m\}$. For any $M \in \mathfrak{D}$, we write $L_S(\bar{\psi}_M, s)$ for the imprimitive Hecke L-series of $\bar{\psi}_M$, where by imprimitive we mean that the Euler factors of the primes in the set S are omitted from its Euler product.

Proposition 3.1. *If $m \geq 1$, the number*

$$2^{-m} \sum_{M \in \mathfrak{D}} L_S(\bar{\psi}_M, 1)/\Omega_\infty$$

is in $\mathfrak{J} = K(\sqrt{\pi_1}, \cdots, \sqrt{\pi_m})$ and integral at all places of $\mathfrak{J}$ above 2.

Proof. By [1] Proposition 4.1 and the equation (4.5) in [1]. □

Proposition 3.2. *With the above notation and assumption, we have*

$$L(\bar{\psi}_{\mathfrak{M}}, 1)/\Omega_\infty \equiv 0 \text{ or } 2^{m-1} \mod 2^m \mathscr{O}_{\mathfrak{J}}.$$

Proof. We prove this proposition by induction on m. If $m = 0$, then we have $\mathfrak{M} = 1$ and the proposition is valid from the equation $L(A, 1)/\Omega_\infty = \frac{1}{2}$. Let $m \geq 1$. Assume that the proposition is true for any $M \in \mathfrak{D} - \{\mathfrak{M}\}$. For any $M \in \mathfrak{D} - \{\mathfrak{M}\}$, let $S_M = \{\pi \in S \mid \pi \nmid M\}$. For any $\pi \in S_M$, we have $\psi_M(\pi) = \pm\pi \equiv \pm 1 \mod 4$, so $1 - \frac{\bar{\psi}_M(\pi)}{N_{K/\mathbb{Q}}(\pi)} \equiv 0$ or $2 \mod 4$. Then

$$\begin{aligned} L_S(\bar{\psi}_M, 1)/\Omega_\infty &= L(\bar{\psi}_M, 1)/\Omega_\infty \times \prod_{\pi \in S_M} \left(1 - \frac{\bar{\psi}_M(\pi)}{N_{K/\mathbb{Q}}(\pi)}\right) \\ &\equiv 0 \text{ or } 2^{m-1} \mod 2^m \end{aligned}$$

by the induction hypothesis. By Proposition 3.1, we get

$$L_S(\bar{\psi}_{\mathfrak{M}}, 1)/\Omega_\infty \equiv 0 \text{ or } 2^{m-1} \mod 2^m.$$

As a result, the proposition is true for any $\mathfrak{M}$. □

Fix any prime element of K above 2, and write ord_2 for the order valuation at this prime element. Then, this order is the extension of the 2-adic valuation.

Lemma 3.3. *Let $0 \neq D \in \mathbb{Z}$. Choose a prime number p which is prime to $14D$, and let π be a prime element of K dividing p which satisfies $\pi \equiv 1 \mod 4$.*

(1) *We have* $\mathrm{ord}_2\left(1 - \frac{\bar{\psi}_D(\pi)}{N_{K/\mathbb{Q}}(\pi)}\right) \geq 1$.

(2) *The following conditions are equivalent:*

   (*i*) $\mathrm{ord}_2\left(1 - \frac{\bar{\psi}_D(\pi)}{N_{K/\mathbb{Q}}(\pi)}\right) \geq 2$.

   (*ii*) *The extension* $K_\pi(\sqrt{-1}, \sqrt{D\sqrt{-7}})/K_\pi$ *is trivial.*

   (*iii*) *Either* $\left(\frac{-7}{p}\right) = \left(\frac{-1}{p}\right) = 1$ *and* $\left(\frac{-7}{p}\right)_4 = \left(\frac{D}{p}\right)$ *or* $\left(\frac{-7}{p}\right) = \left(\frac{-1}{p}\right) = -1$.

Proof. (1) Define $\zeta = \pm 1$ by $\psi_D(\pi) = \zeta\pi$. Then we have

$$1 - \frac{\bar{\psi}_D(\pi)}{N_{K/\mathbb{Q}}(\pi)} = 1 - \frac{1}{\zeta\pi} \equiv \begin{cases} 0 & \mod 4 \text{ if } \zeta = 1, \\ 2 & \mod 4 \text{ if } \zeta = -1 \end{cases} \tag{3.1}$$

and the statement follows.

(2) First, we prove that (*i*) is equivalent to (*ii*). By the equation (3.1), the condition (*i*) is equivalent to $\psi_D(\pi) \equiv \pi \mod 4$, i.e, $\psi_D(\pi) \equiv 1 \mod 4$. Since $A[4]$ is a free $\mathscr{O}_K/4\mathscr{O}_K$-module of rank 1, (*i*) is further equivalent to the condition that $\psi_D(\pi)$ acts $A^{(D)}[4]$ trivially. By the definition of the Hecke character, it is also equivalent to $[\pi, K(A^{(D)}[4])/K] = id$, where $[*, K(A^{(D)}[4])/K]$ is the Artin map. Now by Lemma 2.4, we have $K(A^{(D)}[4]) = K(\sqrt{-1}, \sqrt{D\sqrt{-7}})$. Since p is prime to $14D$, the extension $K_\pi(A^{(D)}[4])/K_\pi$ is unramified. Thus $[\pi, K(A^{(D)}[4])/K] = id$ if and only if $K_\pi(A^{(D)}[4])$ and K_π are the same.

Next, we prove that (ii) is equivalent to (iii). When $\left(\frac{p}{7}\right) = 1$, then the residue field of K_π is $\mathbb{F}_p$, so (ii) is satisfied if and only if $\mathbb{F}_p\left(\sqrt{-1}, \sqrt{D\sqrt{-7}}\right) = \mathbb{F}_p$. The element $\sqrt{-1}$ belongs to $\mathbb{F}_p$ if and only if $\left(\frac{-1}{p}\right) = 1$, and the element $\sqrt{D\sqrt{-7}}$ belongs to $\mathbb{F}_p$ if and only if $\left(\frac{-7}{p}\right)_4 = \left(\frac{D}{p}\right)$, so the lemma follows in this case. When $\left(\frac{p}{7}\right) = -1$, then the residue field of K_π is $\mathbb{F}_{p^2}$, so (ii) is satisfied if and only if $\mathbb{F}_{p^2}\left(\sqrt{-1}, \sqrt{D\sqrt{-7}}\right) = \mathbb{F}_{p^2}$. By Lemma 2.10, it is equivalent to the condition that $\left(\frac{-1}{p}\right) = -1$.

□

Proposition 3.4. *Let M be an admissible integer, and $\mathscr{T}_M$ as in Definition 1.1. Then the following conditions are equivalent:*

(i) $\mathrm{ord}_2(L^{(alg)}(\bar{\psi}_M, 1)) = r(M) - 1$.

(ii) $\#\mathscr{T}_M$ *is odd.*

Proof. We prove the proposition by induction on $r(M) \geq 0$. When $r(M) = 0$, then $M = 1$. Therefore, the proposition follows from the fact that $\#\mathscr{T}_M = 1$ and that $L^{(alg)}(\bar{\psi}_M, 1) = 1/2$. Now we suppose that the proposition is true whenever $r(M) \leq n - 1$. When $r(M) = n$, let $M = \pi_1 \cdots \pi_n$ and $S = \{\pi_1, \ldots \pi_n\}$. Let $\mathfrak{D}$ be the set of divisors of M as defined at the beginning of Section 3. Then, by induction hypothesis and Lemma 3.3, we have

$$\begin{aligned}\mathscr{T}_M &= \left\{ D \in \mathscr{R}_M \middle| D \neq M, \mathrm{ord}_2(L^{(alg)}(\bar{\psi}_D, 1)) = r(D) - 1 \right\} \\ &= \left\{ D \in \mathbb{Z} \middle| \begin{array}{l} D|M, D \neq M, D \equiv 1 \bmod 4 \\ \mathrm{ord}_2(L^{(alg)}(\bar{\psi}_D, 1)) = r(D) - 1 \\ \mathrm{ord}_2\left(1 - \frac{\bar{\psi}_D(\pi)}{N_{K/\mathbb{Q}}(\pi)}\right) = 1 \\ \quad \text{for any prime elements } \pi \mid M/D \text{ with } \pi \equiv 1 \mod 4 \end{array} \right\}.\end{aligned}$$

Since we have

$$L_S(\bar{\psi}_D, 1)\sqrt{D}/\Omega_\infty = \begin{cases} L^{(alg)}(\bar{\psi}_D, 1) \prod_{\pi | M/D} \left(1 - \frac{\bar{\psi}_D(\pi)}{N_{K/\mathbb{Q}}(\pi)}\right), \text{ if } M > 0, \\ \sqrt{-7} L^{(alg)}(\bar{\psi}_D, 1) \prod_{\pi | M/D} \left(1 - \frac{\bar{\psi}_D(\pi)}{N_{K/\mathbb{Q}}(\pi)}\right), \text{ if } M < 0 \end{cases}$$

by definition, we get

$$\mathscr{T}_M = \left\{ D \in \mathbb{Z} \middle| \begin{array}{l} D \mid M, D \neq M, D \equiv 1 \bmod 4 \\ \mathrm{ord}_2(L_S(\bar{\psi}_D, 1)/\Omega_\infty) = r(M) - 1 \end{array} \right\}.$$

By Lemma 2.8, we have $\mathfrak{D} \cap \mathbb{Z} = \{D \in \mathbb{Z} | D \equiv 1 \mod 4, D \mid M\}$. Therefore, by Proposition 3.2, the number of elements of $\mathscr{T}_M$ is odd if and only if

$$\mathrm{ord}_2 \left(\sum_{D \in \mathfrak{D} \cap \mathbb{Z}, D \neq M} L_S(\bar{\psi}_D, 1)/\Omega_\infty \right) = r(M) - 1. \tag{3.2}$$

For any element $\alpha \in \mathfrak{D}$ and any prime element π of K prime to $M\sqrt{-7}$, we have $\psi_\alpha(\pi) = \bar{\psi}_{\bar{\alpha}}(\bar{\pi})$. Thus, for any complex number s, we have

$$1 - \bar{\psi}_\alpha(\pi)N_{K/\mathbb{Q}}(\pi)^{-s} = \overline{1 - \bar{\psi}_{\bar{\alpha}}(\bar{\pi})N_{K/\mathbb{Q}}(\bar{\pi})^{-\bar{s}}}.$$

Thus, we have

$$L_S(\bar{\psi}_\alpha, s) = \overline{L_S(\bar{\psi}_{\bar{\alpha}}, \bar{s})}.$$

Since $\Omega_\infty \in \mathbb{R}$, we get

$$L_S(\bar{\psi}_\alpha, 1)/\Omega_\infty = \overline{L_S(\bar{\psi}_{\bar{\alpha}}, 1)/\Omega_\infty}.$$

By Proposition 3.2, we have $L_S(\bar{\psi}_\alpha, 1)/\Omega_\infty \equiv 0$ or $2^{r(M)-1} \mod 2^{r(M)}$. We have

$$\mathrm{ord}_2(L_S(\bar{\psi}_\alpha, 1)/\Omega_\infty + L_S(\bar{\psi}_{\bar{\alpha}}, 1)/\Omega_\infty) \geq r(M). \tag{3.3}$$

By the equation (3.2) and the inequality (3.3), the number of elements of $\mathscr{T}_M$ is odd if and only if

$$\mathrm{ord}_2\left(\sum_{\alpha \in \mathfrak{D}, \alpha \neq M} L_S(\bar{\psi}_\alpha, 1)/\Omega_\infty\right) = r(M) - 1.$$

By Proposition 3.1 and Proposition 3.2, this condition is equivalent to the condition that $\mathrm{ord}_2(L^{(alg)}(\bar{\psi}_M, 1)) = r(M) - 1$. □

4 Proof of Theorem 1.4

In this section, we assume that Theorem 1.8 is true, and prove Theorem 1.4 and Thorem 1.5. Also we prove Corollary 1.7.

Proof of Theorem 1.4. We will prove the equivalence of the theorem by induction on $r(M)$. When $r(M) = 0$, then we have $M = 1$. We have $L^{(alg)}(\bar{\psi}_M, 1) = 1/2$ and $\#S_2(A^{(M)}/\mathbb{Q}) = 2$, so the theorem follows. Now we suppose that Theorem 1.4 is true for any D with $r(D) \leq n - 1$. Using the induction hypothesis and Lemma 3.3, we have

$$\mathscr{T}_M = \left\{ D \in \mathscr{R}_M \middle| D \neq M, \#S_2(A^{(D)}/\mathbb{Q}) = 2 \right\}.$$

By Corollary 2.13, we have

$$\#\mathscr{T}_M \equiv \sum_{D \in \mathscr{R}_M, D \neq M} \#\mathscr{S}_D \mod 2.$$

By Theorem 1.8, we have $\#\mathscr{S}_M \equiv \#\mathscr{T}_M \mod 2$. By Corollary 2.13 and Proposition 3.4, conditions (i)-(v) of Theorem 1.4 are equivalent.

Assume that $A^{(M)}$ satisfies these conditions. Since $L(A^{(M)}, s) \neq 0$, the p-part of Birch-Swinnerton-Dyer conjecture for any odd prime p is valid by [6]. Since $\#S_2(A^{(M)}/\mathbb{Q}) = 2$ and $\#A^{(M)}(\mathbb{Q})/2A^{(M)}(\mathbb{Q}) = 2$, the Tate-Shafarevich group

$Ш(A^{(M)}/\mathbb{Q})$ satisfies $Ш(A^{(M)}/\mathbb{Q})[2] = 0$. If we write $M = \pm p_1 \cdots p_s q_1 \cdots q_t$ as Definition 1.1, the Tamagawa factor c_p of $A^{(M)}$ at the bad prime p are given by $c_7 = 2$, $c_{p_i} = 2$ $(1 \leq i \leq s)$, and $c_{q_j} = 4$ $(1 \leq j \leq t)$. As a result, the 2-part of Birch-Swinnerton-Dyer conjecture is valid from $\mathrm{ord}_2(L^{(alg)}(\bar{\psi}_M, 1)) = r(M) - 1$. □

Proof of Theorem 1.5. We will prove that, if M satisfies the condition of Theorem 1.5, we have $\mathscr{T}_M = \emptyset$ by induction on $r(M) \geq 1$. When $r(M) = 1$, then $M = -p$ satisfies $p \equiv -1 \mod 4$ and $\left(\frac{-7}{p}\right) = -1$. Therefore we get $\mathscr{T}_M = \emptyset$.

Now assume that $p \mid M$ satisfies $p \equiv -1 \mod 4$ and $\left(\frac{-7}{p}\right) = -1$. Assume that, for any admissible integer D which satisfies $p \mid D$ and $r(D) < r(M)$, we have$\mathscr{T}_D = \emptyset$. When we have $D \in \mathscr{R}_M$ and $D \neq M$, by the definition of $\mathscr{R}_M$, we have $p \mid D$. Thus by induction hypothesis, we have $\mathscr{T}_D = \emptyset$, and $D \notin \mathscr{T}_M$. As a result, we get $\mathscr{T}_M = \emptyset$. □

Proof of Corollary 1.7. It suffices to show that $\mathscr{S}_M = \{1\}$. By the definition of $\mathscr{S}_M$, for any $d \in \mathscr{S}_M$, we have $d \mid q_1 \ldots q_t$ and $d > 0$. If $q_j \mid d$, we have $\left(\frac{M/dP}{q_j}\right) = \left(\frac{P}{q_j}\right)\left(\frac{-7}{q_j}\right)_4$. However, by our assumption on M, we have $\left(\frac{M/dP}{q_j}\right) = 1$ and $\left(\frac{P}{q_j}\right)\left(\frac{-7}{q_j}\right)_4 = -1$, which is a contradiction. Therefore, we have $\mathscr{S}_M = \{1\}$, and the condition (iv) is satisfied, and by Theorem 1.4, the corollary follows. □

5 Proof of Theorem 1.8

Let $\mathscr{N}$ denote the set of all square-free positive integers $N \neq 1$. We will prove the following proposition to show Theorem 1.8.

Proposition 5.1. *Assume that $N = p_1 \cdots p_n \in \mathscr{N}$. Let $\epsilon, \eta : \{1, \ldots, n\} \to \{\pm 1\}$ be maps, and define*

$$T_{N,(\epsilon,\eta)} = \left\{ (a,b,c) \in \mathbb{N}^3 \;\middle|\; \begin{array}{l} abc = N \\ \left(\frac{b}{p_i}\right) = \epsilon(i) \;\; \textit{if } p_i \mid a \\ \left(\frac{a}{p_i}\right) = \eta(i) \;\; \textit{if } p_i \mid b \\ \left(\frac{ab}{p_i}\right) = -\epsilon(i)\eta(i) \;\; \textit{if } p_i \mid c \end{array} \right\}.$$

Then, the number $\#T_{N,(\epsilon,\eta)}$ is even.

Proof of Theorem 1.8. Let R_+ (resp. R_-) denote the product of the prime divisors of M which is inert in K and split (resp. inert) in $\mathbb{Q}(\sqrt{-1})$. Let $N = q_1 \ldots q_n = M/R_+R_-$. Define $\epsilon_{s,t}$ and η_s for any divisor s of R_- congruent to 1 modulo 4 and for any divisor t of R_+ congruent to 1 modulo 4 by

$$\epsilon_{s,t}(i) = \left(\frac{tR_-/s}{q_i}\right)\left(\frac{-7}{q_i}\right)_4, \eta_s(i) = \left(\frac{s}{q_i}\right).$$

Then we have a map

$$\coprod_{s|R_-,t|R_+,s,t\equiv 1 \mod 4} T_{N,(\epsilon_{s,t},\eta_s)} \to \coprod_{D\in\mathscr{R}_M} \mathscr{S}_D$$

defined by

$$T_{N,(\epsilon_{s,t},\eta_s)} \ni (a,b,c) \mapsto as \in \mathscr{S}_{abtR_-}.$$

This map is bijective, since the map has the inverse map

$$\mathscr{S}_D \ni d \mapsto (a,b,c) \in T_{N,(\epsilon_{s,t},\eta_s)},$$

where $a = \gcd(N,d) > 0$, $b = \gcd(N, D/d) > 0$, $c = N/ab$, $s = d/a$, and $t = \gcd(D/d, R_+)$. By Proposition 5.1, the number $\#T_{N,(\epsilon_{s,t},\eta_s)}$ is even. Since s and t are arbitrary, the number $\sum_{D\in\mathscr{R}_M} \#\mathscr{S}_D$ is also even. □

Proof of Proposition 5.1. We prove the proposition by induction on $n \geq 1$. When $n = 1$, even numbers of $\epsilon(1), \eta(1)$, and $-\epsilon(1)\eta(1)$ are 1, so the proposition follows. Now suppose that $n \geq 2$, and assume that $\#T_{N,(\epsilon,\eta)}$ is even for all $\bar{N} \in \mathscr{N}$ with $n-1$ prime divisors. Suppose that N is any element of $\mathscr{N}$ with n prime divisors. We will prove $\#T_{N,(\epsilon,\eta)}$ is even for any ϵ, η by induction on $k = \#\{i|\epsilon(i) \neq \eta(i)\} \geq 0$.

First, we assume that $\epsilon(i) = \eta(i)$ for $i = 1, \ldots, n$. In this case, the involution $T_{N,(\epsilon,\eta)} \to T_{N,(\epsilon,\eta)}; (a,b,c) \mapsto (b,a,c)$ has no fix point since $(1,1,N) \notin T_{N,(\epsilon,\eta)}$. Therefore $\#T_{N,(\epsilon,\eta)}$ is even.

Next, we assume that the proposition is true for $k = l-1 (l \geq 1)$, and that $\#\{i|\epsilon(i) \neq \eta(i)\} = l$. Without loss of generality, we can suppose $\epsilon(n) \neq \eta(n)$. We will prove the proposition for N and (ϵ, η). Let

$$\epsilon'(i) = \begin{cases} -\epsilon(i) & (i = n), \\ \epsilon(i) & (\text{otherwise}). \end{cases}$$

Thus we have $\#\{i|\epsilon'(i) \neq \eta(i)\} = l-1$. Let $\bar{N} = N/p_n$. Let

$$T^1_{N,(\epsilon,\eta)} = \{(a,b,c) \in T_{N,(\epsilon,\eta)} | p_n \text{ divides } a\},$$

$$T^2_{N,(\epsilon,\eta)} = \{(a,b,c) \in T_{N,(\epsilon,\eta)} | p_n \text{ divides } b\},$$

and

$$T^3_{N,(\epsilon,\eta)} = \{(a,b,c) \in T_{N,(\epsilon,\eta)} | p_n \text{ divides } c\}$$

for any ϵ, η. Thus $T_{N,(\epsilon,\eta)}$ is the disjoint union of $T^1_{N,(\epsilon,\eta)}$, $T^2_{N,(\epsilon,\eta)}$, and $T^3_{N,(\epsilon,\eta)}$. Let

$$\bar{\epsilon} = \epsilon|_{\{1,\ldots,n-1\}}, \bar{\eta} = \eta|_{\{1,\ldots,n-1\}},$$

and

$$\bar{\eta}' : \{1,\ldots,n-1\} \to \{\pm 1\}, \bar{\eta}'(i) = \eta(i)\left(\frac{p_n}{p_i}\right).$$

Then, we have

$$T^1_{N,(\epsilon,\eta)} = \left\{(a,b,c) \in T_{\bar{N},(\bar{\epsilon},\bar{\eta}')} \middle| \left(\frac{b}{p_n}\right) = \epsilon(n)\right\}$$

and

$$T^1_{N,(\epsilon',\eta)} = \left\{ (a,b,c) \in T_{\bar{N},(\bar{\epsilon},\bar{\eta}')} \middle| \left(\frac{b}{p_n}\right) = -\epsilon(n) \right\}.$$

Therefore we have

$$T^1_{N,(\epsilon,\eta)} \sqcup T^1_{N,(\epsilon',\eta)} = T_{\bar{N},(\bar{\epsilon},\bar{\eta}')}.$$

By induction hypothesis on n, we have

$$\#T^1_{N,(\epsilon,\eta)} + \#T^1_{N,(\epsilon',\eta)} = \#T_{\bar{N},(\bar{\epsilon},\bar{\eta}')} \equiv 0 \pmod 2.$$

Similarly, we have

$$\#T^3_{N,(\epsilon,\eta)} + \#T^3_{N,(\epsilon',\eta)} = \#T_{\bar{N},(\bar{\epsilon},\bar{\eta})} \equiv 0 \pmod 2.$$

Also, we have $T^2_{N,(\epsilon,\eta)} = T^2_{N,(\epsilon',\eta)}$, so $\#T^2_{N,(\epsilon,\eta)} + \#T^2_{N,(\epsilon',\eta)} \equiv 0 \mod 2$. Therefore, we get $\#T_{N,(\epsilon,\eta)} + \#T_{N,(\epsilon',\eta)} \equiv 0 \mod 2$. By the induction hypothesis in k, $\#T_{N,(\epsilon,\eta)}$ is even.

As a result, $\#T_{N,(\epsilon,\eta)}$ is even for all (ϵ,η), and by induction, also it is even for all $N \in \mathscr{N}$ and (ϵ,η). □

6 Table

In this section, we give some numerical examples for which the conditions in corollary 1.4 are satisfied, so for which the full Birch-Swinnerton-Dyer conjecture holds. We made this table, referring to Table I in [2].

Table 1: The value of $L^{(alg)}(A^{(M)},1)$ and the biquadratic residue symbol.

M	$L^{(alg)}(A^{(M)},1)$	$\mathrm{ord}_2(L^{(alg)}(A^{(M)},1))$	$r(M)$	power residue symbols
29	2	1	2	$\left(\frac{-7}{29}\right)_4 = -1$
37	2	1	2	$\left(\frac{-7}{37}\right)_4 = -1$
109	2	1	2	$\left(\frac{-7}{109}\right)_4 = -1$
137	2	1	2	$\left(\frac{-7}{109}\right)_4 = -1$
145	4	2	3	$\left(\frac{-7}{29}\right)_4 = -1 = -\left(\frac{5}{29}\right)$
233	18	1	2	$\left(\frac{-7}{109}\right)_4 = -1$
265	36	2	3	$\left(\frac{-7}{53}\right)_4 = 1 = -\left(\frac{5}{53}\right)$
281	2	1	2	$\left(\frac{-7}{281}\right)_4 = -1$
337	2	1	2	$\left(\frac{-7}{337}\right)_4 = -1$
377	4	2	3	$\left(\frac{-7}{29}\right)_4 = -1 = -\left(\frac{13}{29}\right)$
389	18	1	2	$\left(\frac{-7}{389}\right)_4 = -1$
401	18	1	2	$\left(\frac{-7}{401}\right)_4 = -1$

M	$L^{(alg)}(A^{(M)},1)$	$\mathrm{ord}_2(L^{(alg)}(A^{(M)},1))$	$r(M)$	power residue symbols
545	4	2	3	$\left(\frac{-7}{109}\right)_4 = -1 = -\left(\frac{5}{109}\right)$
565	4	2	3	$\left(\frac{-7}{113}\right)_4 = 1 = -\left(\frac{5}{113}\right)$
569	2	1	2	$\left(\frac{-7}{569}\right)_4 = -1$
613	2	1	2	$\left(\frac{-7}{613}\right)_4 = -1$
617	2	1	2	$\left(\frac{-7}{617}\right)_4 = -1$
641	2	1	2	$\left(\frac{-7}{641}\right)_4 = -1$
653	2	1	2	$\left(\frac{-7}{653}\right)_4 = -1$
673	18	1	2	$\left(\frac{-7}{673}\right)_4 = -1$
701	2	1	2	$\left(\frac{-7}{701}\right)_4 = -1$
709	2	1	2	$\left(\frac{-7}{709}\right)_4 = -1$
757	2	1	2	$\left(\frac{-7}{757}\right)_4 = -1$
877	2	1	2	$\left(\frac{-7}{877}\right)_4 = -1$
965	4	2	3	$\left(\frac{-7}{193}\right)_4 = 1 = -\left(\frac{5}{193}\right)$
977	18	1	2	$\left(\frac{-7}{977}\right)_4 = -1$
985	36	2	3	$\left(\frac{-7}{197}\right)_4 = 1 = -\left(\frac{5}{197}\right)$

References

[1] J. Coates, Y. Li, Y. Tian and S. Zhai, *Quadratic twists of elliptic curves*, Proc. Lond. Math. Soc. (3) 110 (2015), no. 2 357–394. MR3335282

[2] J. Coates, M. Kim, Z. Liang and C. Zhao, *On the 2-part of the Birch-Swinnerton-Dyer conjecture for elliptic curves with complex multiplication*, Münster J. of Math. 7 (2014), no. 1 83–103. MR3271240

[3] Cristian D. González-Avilés, *On the conjecture of Birch and Swinnerton-Dyer*, Trans. Amer. Math. Soc. Vol. 349, no.10 (1997), 4181–4200. MR1390036

[4] A. Brumer and K. Kramer, *The rank of elliptic curves*, Duke Math. J. 44 (1977), no. 4, 715–743. MR0457453

[5] Joseph H. Silverman, *The Arithmetic of Elliptic Curves* second edition, Graduate Texts in Mathematics, 106. Springer, Dordrecht, 2009. xx+513 pp. ISBN: 978-0-387-09493-9 MR2514094

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

[7] J. Choi, *On the* 2*-adic valuations of central* L*-values of elliptic curves*, J. Number Theory 204 (2019), 405–422. MR3991426