

A CLASSICAL FAMILY OF ELLIPTIC CURVES
HAVING RANK ONE AND THE 2-PRIMARY PART
OF THEIR TATE–SHAFAREVICH GROUP NON-TRIVIAL

YUKAKO KEZUKA AND YONGXIONG LI

Received: November 14, 2019

Revised: November 24, 2020

Communicated by Otmar Venjakob

ABSTRACT. We study elliptic curves of the form $x^3 + y^3 = 2p$ and $x^3 + y^3 = 2p^2$ where p is any odd prime satisfying $p \equiv 2 \pmod{9}$ or $p \equiv 5 \pmod{9}$. We first show that the 3-part of the Birch–Swinnerton-Dyer conjecture holds for these curves. Then we relate their 2-Selmer group to the 2-rank of the ideal class group of $\mathbb{Q}(\sqrt[3]{p})$ to obtain some examples of elliptic curves with rank one and non-trivial 2-part of the Tate–Shafarevich group.

2020 Mathematics Subject Classification: 14H52, 11G05, 11R29

Keywords and Phrases: Elliptic curves, complex multiplication, Tate–Shafarevich group, ideal class group

1 INTRODUCTION AND THE MAIN RESULTS

Let $n \geq 3$ be a cube free integer. The elliptic curve

$$C_n: x^3 + y^3 = n$$

is the twist of $C: x^3 + y^3 = 1$ by the cubic field $\mathbb{Q}(\sqrt[3]{n})$, where $\sqrt[3]{n}$ denotes the real root. The study of the arithmetic of C_n is very old. In particular, it is well known that C_n has no non-zero rational torsion, and thus $C_n(\mathbb{Q})$ is infinite precisely when n is the sum of two rational cubes. Let p be any odd prime satisfying

$$p \equiv 2 \pmod{9} \text{ or } p \equiv 5 \pmod{9}. \tag{1.1}$$

In [20], Satgé used the theory of Heegner points to show that C_{2p} has rank 1 when $p \equiv 2 \pmod{9}$, and C_{2p^2} has rank 1 when $p \equiv 5 \pmod{9}$. More recently, it was shown in [2] that, for all odd primes p satisfying (1.1) the 3-part of

the Birch–Swinnerton-Dyer conjecture holds for the product of the two curves $C_{2p} \times C_{2p^2}$; here, we remark that one of the curves in this product is of rank zero, while the other is of rank one.

The first main result of this paper is the proof of the 3-part of the Birch–Swinnerton-Dyer conjecture for each of the individual curves C_{2p} and C_{2p^2} for all odd primes p satisfying (1.1). More precisely, we establish the following results. Let $L(C_n, s)$ be the complex L -series of C_n over \mathbb{Q} . Since C_n has complex multiplication by the integer ring \mathcal{O}_K of $K = \mathbb{Q}(\sqrt{-3})$, the analytic continuation and functional equation of $L(C_n, s)$ are known by Deuring’s theorem. Let A be the elliptic curve with classical Weierstrass equation

$$A: y^2 = 4x^3 - 1.$$

Then fixing an embedding of K into \mathbb{C} , and noting that A also has complex multiplication by \mathcal{O}_K , the lattice L of complex periods of the differential dx/y on A is of the form $\Omega\mathcal{O}_K$, with $\Omega = 3.059908\dots$, a real number. For each integer $n \geq 3$, we then define

$$\Omega_n = \Omega/(\sqrt{3}n^{1/3}). \quad (1.2)$$

The rationality of the algebraic part $\frac{L(C_n, 1)}{\Omega_n}$ of $L(C_n, s)$ at $s = 1$ follows from a result of Birch using modular symbols, which deals with any elliptic curve over \mathbb{Q} . Moreover, Stephens strengthened this result for C_n in [24] to show that this is a rational integer.

THEOREM 1.1. *Let p be an odd prime satisfying (1.1). Then*

1. *If $p \equiv 5 \pmod{9}$, the L -values $L(C_{2p}, 1)$ and $L(C_{2^2p^2}, 1)$ are both non-zero, and the 3-part of the Birch–Swinnerton-Dyer conjecture holds for C_{2p} and $C_{2^2p^2}$. Moreover, we have the following congruence*

$$\frac{L(C_{2p}, 1)}{3\Omega_{2p}} \equiv \frac{L(C_{2^2p^2}, 1)}{3\Omega_{2^2p^2}} \equiv 1 \pmod{3}.$$

2. *If $p \equiv 2 \pmod{9}$, the L -values $L(C_{2p^2}, 1)$ and $L(C_{2^2p}, 1)$ are both non-zero, and the 3-part of the Birch–Swinnerton-Dyer conjecture holds for C_{2p^2} and C_{2^2p} . Moreover, we have the following congruence*

$$\frac{L(C_{2^2p}, 1)}{3\Omega_{2^2p}} \equiv \frac{L(C_{2p^2}, 1)}{3\Omega_{2p^2}} \equiv 1 \pmod{3}.$$

We write $\text{III}(C_n)$ for the Tate–Shafarevich group of C_n over \mathbb{Q} . Combined with the results in [2], we obtain the following corollary of Theorem 1.1.

COROLLARY 1.2. *Let p be an odd prime satisfying (1.1).*

1. *If $p \equiv 2 \pmod{9}$, the curve C_{2p} has rank 1 and $L(C_{2p}, s)$ has a simple zero at $s = 1$. Furthermore, $\text{III}(C_{2p})$ is finite and the 3-part of the Birch–Swinnerton-Dyer conjecture holds for C_{2p} .*

2. If $p \equiv 5 \pmod{9}$, the curve C_{2p^2} has rank 1 and $L(C_{2p^2}, s)$ has a simple zero at $s = 1$. Furthermore, $\text{III}(C_{2p^2})$ is finite and the 3-part of the Birch–Swinnerton-Dyer conjecture holds for C_{2p^2} .

The second main result of this paper is on the 2-part of the Tate–Shafarevich group of the curves C_{2p} and C_{2p^2} in the rank 1 case studied in Corollary 1.2. For any abelian group (scheme) \mathfrak{M} (over a base scheme S) and a positive integer m , we write $\mathfrak{M}[m]$ for the group (scheme) of m -torsion of \mathfrak{M} . We relate the 2-Selmer group of these curves to the 2-part of the ideal class group of the field $L = \mathbb{Q}(\sqrt[3]{p})$. We remark that such a relation has already been obtained in [11] for a wide class of elliptic curves without complex multiplication. We can apply the same methods to our curves on noting that their Mordell–Weil groups have trivial torsion subgroups and that for any prime number ℓ , we have $\Phi[2] = 0$, where $\Phi/\overline{\mathbb{F}}_\ell$ denotes the component group scheme of a corresponding Néron model over \mathbb{Q}_ℓ . In addition, in our case, we can use this relation to obtain examples of curves with rank 1 and non-trivial 2-part of the Tate–Shafarevich group.

Given a number field F , let $Cl(F)$ be the ideal class group of F . We call the integer $\text{rank}_2(Cl(F)) := \dim_{\mathbb{F}_2}(Cl(F)/2Cl(F))$ the 2-rank of $Cl(F)$. Here, \mathbb{F}_2 denotes the finite field of two elements.

THEOREM 1.3. *Let p be an odd prime satisfying (1.1).*

1. If $p \equiv 2 \pmod{9}$, we have $\text{rank}_2(Cl(L)) \geq 2$ if and only if $\text{III}(C_{2p})[2]$ is non-trivial. In particular, in the case $\text{rank}_2(Cl(L)) \geq 2$, the curve C_{2p} has rank 1 and has non-trivial $\text{III}(C_{2p})[2]$.
2. If $p \equiv 5 \pmod{9}$, we have $\text{rank}_2(Cl(L)) \geq 2$ if and only if $\text{III}(C_{2p^2})[2]$ is non-trivial. In particular, in the case $\text{rank}_2(Cl(L)) \geq 2$, the curve C_{2p^2} has rank 1 and has non-trivial $\text{III}(C_{2p^2})[2]$.

We remark that, although we cannot show at present that there are infinitely many primes p satisfying the condition $\text{rank}_2(Cl(L)) \geq 2$ in Theorem 1.3, there are many such p . Indeed, for $p < 1000000$, 1852/13099 of the primes $p \equiv 2 \pmod{9}$ and 1629/13068 of the primes $p \equiv 5 \pmod{9}$ satisfy the condition. Some notable numerical examples can be found in Appendix A. We note also that there are infinitely many elliptic curves over \mathbb{Q} with rank 0 and non-trivial 2-part of the Tate–Shafarevich group (see, for example, [17]). However, in the rank 1 case, it seems that one can so far only find elliptic curves over \mathbb{Q} with non-trivial 2-part of the Tate–Shafarevich group via numerical computations. Theorem 1.3 thus sheds new theoretical light on the existence of many curves with rank 1 and non-trivial 2-part of the Tate–Shafarevich group.

In the remainder of this introduction, we explain the structure of the paper and the key ideas involved. In Section 2, we will introduce the notion of ‘explicit modulo 3 Birch–Swinnerton-Dyer conjecture’ and show congruences similar to

those in Theorem 1.1 for the curves C_p and C_{p^2} . The proof of Theorem 1.1 will be given in Section 3. The main idea of the proof is an extension of Zhao's averaging method [26, 10, 15] from 2-adic to 3-adic. However, a direct application of Zhao's method only gives us the 3-adic valuation of the sum of the two algebraic L -values in Theorem 1.1, and does not give us the 3-adic valuation of the individual algebraic L -value. To overcome this difficulty, we will study the 'explicit modulo 3 Birch–Swinnerton-Dyer conjecture' introduced in Section 2 to separate the terms in the above sum. A key ingredient in establishing such an 'explicit modulo 3 Birch–Swinnerton-Dyer conjecture' is Zhang's adaptation [27] of Razar's method [16, 17] from 2-adic to 3-adic. This gives us a precise 3-adic valuation of certain rational functions on the curve A which appear naturally in a special value formula (see [6]) for $L(C_{2^i p^j}, 1)$ for $i, j \in \{0, 1, 2\}$. Combining Zhao's method, the results from Section 2 and congruences between the L -values of C_{2p} and $C_{2^2 p^2}$ (resp. C_{2p^2} and $C_{2^2 p}$) for $p \equiv 5 \pmod{9}$ (resp. $p \equiv 2 \pmod{9}$) gives us Theorem 1.1. In Section 4, we will prove Theorem 1.3 by a 2-descent argument. In Appendix A, we will give some numerical examples which satisfy the condition $\text{rank}_2(Cl(L)) \geq 2$ in Theorem 1.3.

NOTATION AND CONVENTIONS

Throughout the paper, we will have $K = \mathbb{Q}(\sqrt{-3})$ and a fixed embedding of K into \mathbb{C} . We write \mathcal{O}_K for the integer ring of K , and for every ideal $(b) = b\mathcal{O}_K$ of K , $K(b)$ will denote the ray class field over K modulo (b) . An odd prime p is always assumed satisfying the condition (1.1), and we write $H_p = K(\sqrt[3]{p})$ and $\mathcal{H}_p = K(\sqrt[3]{p}, \sqrt[3]{2})$. If $m \geq 1$ is an integer, μ_m will denote the group of m -th roots of unity. For any cube free integer $n \geq 3$, we write C_n for the elliptic curve $x^3 + y^3 = n$. Let $A : y^2 = 4x^3 - 1$ with a period lattice $L = \Omega\mathcal{O}_K$, where $\Omega = 3.059908\dots$ is a real number. For each integer $n \geq 1$, we set $\Omega_n = \frac{\Omega}{(\sqrt{3n^3})}$. Let $L(C_n, s)$ be the complex L -series of C_n over \mathbb{Q} . We call $\frac{L(C_n, 1)}{\Omega_n}$ the algebraic part of L -value of C_n at $s = 1$. As usual, \mathbb{Q}_3 will denote the field of 3-adic numbers, and \mathbb{Z}_3 the ring of 3-adic integers in \mathbb{Q}_3 . We write $\overline{\mathbb{Q}_3}$ for a fixed algebraic closure of \mathbb{Q}_3 , and $\overline{\mathbb{Z}_3}$ will denote the integer ring of $\overline{\mathbb{Q}_3}$. Given $\alpha \in \overline{\mathbb{Q}_3}$, we write $\alpha \in 3^{\epsilon_0}(\epsilon_1 + 3^{\epsilon_2}\overline{\mathbb{Z}_3})$ for three non-negative rational numbers ϵ_i ($i = 0, 1, 2$) if the number $(\alpha/3^{\epsilon_0}) - \epsilon_1$ is divisible by 3^{ϵ_1} in $\overline{\mathbb{Z}_3}$. Finally, we fix a normalized additive 3-adic valuation ord_3 on $\overline{\mathbb{Q}_3}$ such that $\text{ord}_3(3) = 1$.

2 EXPLICIT MODULO 3 BIRCH–SWINNERTON-DYER CONJECTURE FOR C_p AND C_{p^2}

We first introduce a special value formula for C_n to which we will refer frequently in the later sections of the paper. We assume from now on that n is prime to 3. Let ψ_n be the Hecke character over K associated to C_n . From an explicit description of ψ_n contained in [23], we have

$$\psi_n((\alpha)) = \left(\frac{n}{\alpha}\right)_3 \alpha \quad (2.1)$$

for every $\alpha \in \mathcal{O}_K$ which is prime to $3n$ and is congruent to 1 modulo 3. Here, $(\cdot)_3$ denotes the cubic residue symbol, and we denote by (f) the conductor of ψ_n . A precise definition of the cubic residue symbol and a detailed description of (f) can be found in [24].

Let z and s be complex variables. Given any lattice \mathcal{L} in the complex plane \mathbb{C} , the Kronecker–Eisenstein series is defined by

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

where the sum is taken over all $w \in \mathcal{L}$ except $-z$ if $z \in \mathcal{L}$. This series converges to define a holomorphic function in s on the half plane $\text{Re}(s) > \frac{3}{2}$, and it has analytic continuation to the whole complex s -plane. We define the non-holomorphic Eisenstein series by

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

It is shown in [24] that the Néron differential lattice of C_n is $\Omega_n \mathcal{O}_K$. We have the following special value formula for C_n , whose detailed proof can be found in [6, Theorem 60].

THEOREM 2.1. *Let (f) be the conductor of ψ_n , and let g be an integer in K such that g is a multiple of f . Then the value $\mathcal{E}_1^*\left(\frac{\Omega_n}{g}, \Omega_n \mathcal{O}_K\right)$ lies in $K(g)$, and we have*

$$L^{(g)}(C_n, 1) = \frac{\Omega_n}{g} \text{Tr}_{K(g)/K} \left(\mathcal{E}_1^* \left(\frac{\Omega_n}{g}, \Omega_n \mathcal{O}_K \right) \right), \tag{2.2}$$

where $\text{Tr}_{K(g)/K}$ denotes the trace map from $K(g)$ to K . Here, we denote by $L^{(g)}(C_n, s)$ the imprimitive L -series of C_n obtained by omitting the Euler factors at all primes dividing (g) , so that in particular in the case $(f) = (g)$, $L^{(g)}(C_n, s)$ is the complex L -series for C_n .

Let us say from now on that the explicit modulo 3 Birch–Swinnerton-Dyer conjecture holds for C_n if the algebraic part of its L -value at $s = 1$, when divided by the product of the Tamagawa factors, satisfies the modulo 3 congruence predicted by the Birch–Swinnerton-Dyer conjecture. When $L(C_n, 1) \neq 0$, the explicit modulo 3 Birch–Swinnerton-Dyer conjecture is stronger than the 3-part of the Birch–Swinnerton-Dyer conjecture for C_n , since the argument from Iwasawa theory due to Rubin [19] excludes both the 2-part and the 3-part of the Birch–Swinnerton-Dyer conjecture for C_n . In particular, it is not difficult to check that the congruences in Theorem 1.1 gives the explicit modulo 3 Birch–Swinnerton-Dyer conjecture for C_{2p} and $C_{2^2 p^2}$ when $p \equiv 5 \pmod{9}$ and for $C_{2^2 p}$ and C_{2p^2} when $p \equiv 2 \pmod{9}$. Indeed, the factor 3 in the denominators of the congruences in Theorem 1.1 comes from the Tamagawa factor at the prime 3 (a description of the Tamagawa factor for C_n is given in [25]). Furthermore,

by a 3-descent argument, we can show that the 3-part of the Tate–Shafarevich group of the elliptic curves in Theorem 1.1 is trivial (see Proposition 3.11). It follows from [18] that these Tate–Shafarevich groups are finite, and thus by Cassels’ theorem [3], they have square orders. Hence their orders are congruent to 1 modulo 3, as required.

In this section, we first prove

$$L(C_p, 1) \neq 0 \text{ and } L(C_{p^2}, 1) \neq 0,$$

then show that the 3-part of the Birch–Swinnerton-Dyer conjectures holds for these curves. Moreover, we will show that the explicit modulo 3 Birch–Swinnerton-Dyer conjecture holds for C_p and C_{p^2} . We remark that the non-vanishing of the L -values of these curves and the 3-part of the Birch–Swinnerton-Dyer conjecture were shown by Zhang in [27]. The main result of this section is the explicit modulo 3 Birch–Swinnerton-Dyer conjecture for the curves C_p and C_{p^2} , which we will prove by applying Zhao’s induction argument and by establishing certain congruences between the algebraic L -values of C_p and C_{p^2} .

We write D for p or p^2 . We recall that A has the periods lattice $L = \Omega\mathcal{O}_K$, and write $\wp(u)$ for the Weierstrass \wp -function associated to the lattice L . We will use the following adaptation of formula (2.2). This formula was already obtained in [24], but we give a different proof, and the style of the proof will play a key role in our later arguments.

PROPOSITION 2.2. *We have*

$$L(C_D, 1) = \frac{-\Omega}{2\sqrt{3}p} \sum_{c \in \mathfrak{C}} \left(\frac{c}{D}\right)_3 \frac{1}{\wp\left(\frac{c\Omega}{p}\right) - 1},$$

where \mathfrak{C} denotes a set of representatives of $(\mathcal{O}_K/p\mathcal{O}_K)^\times$ such that $c \in \mathfrak{C}$ implies $-c \in \mathfrak{C}$.

Proof. From [24], we know that the conductor of ψ_D divides $(3p)$ and has the same prime ideal divisors as $(3p)$. By formula (2.2), we have

$$L(C_D, 1) = \frac{\Omega_D}{-3p} \mathrm{Tr}_{K(3p)/K} \left(\mathcal{E}_1^* \left(\frac{\Omega_D}{-3p}, \Omega_D \mathcal{O}_K \right) \right). \quad (2.3)$$

We make a choice for a set of representatives of integral ideals in K whose Artin symbols give precisely the Galois group $\mathrm{Gal}(K(3p)/K)$. Note that

$$\mathrm{Gal}(K(3p)/K) \simeq (\mathcal{O}_K/3p\mathcal{O}_K)^\times / \mu_6 \simeq (\mathcal{O}_K/p\mathcal{O}_K)^\times,$$

where the inverse of the second isomorphism is given by sending $c \in (\mathcal{O}_K/p\mathcal{O}_K)^\times$ to $3c - p$. Here, we use the condition $-p \equiv 1 \pmod{3}$ and identify μ_6 with $(\mathcal{O}_K/3\mathcal{O}_K)^\times$. Therefore, the Artin symbols of $(3c - p)$ in $\mathrm{Gal}(K(3p)/K)$ give a set of representatives of $\mathrm{Gal}(K(3p)/K)$ as c runs over all

the elements of $(\mathcal{O}_K/p\mathcal{O}_K)^\times$. Thus from (2.3) and the explicit Galois action on $\mathcal{E}_1^*\left(\frac{\Omega_D}{-3p}, \Omega_D\mathcal{O}_K\right)$ described in [6], we obtain

$$\begin{aligned} L(C_D, 1) &= \frac{\Omega_D}{-3p} \sum_{c \in (\mathcal{O}_K/p\mathcal{O}_K)^\times} \mathcal{E}_1^*\left(\frac{\psi_D((3c-p))\Omega_D}{-3p}, \Omega_D\mathcal{O}_K\right) \\ &= \frac{\Omega}{-3p} \sum_{c \in (\mathcal{O}_K/p\mathcal{O}_K)^\times} \mathcal{E}_1^*\left(\frac{\psi_D((3c-p))\Omega}{-3p}, L\right) \end{aligned}$$

where $L = \Omega\mathcal{O}_K$. For the second equality, we use the homogeneity of Eisenstein series

$$\mathcal{E}_1^*(\lambda z, \lambda L) = \lambda^{-1} \mathcal{E}_1^*(z, L) \quad \lambda \in \mathbb{C}^\times$$

of degree -1 . Furthermore, by (2.1), we have

$$\psi_D((3c-p)) = \overline{\left(\frac{D}{3c-p}\right)}_3 (3c-p) = \overline{\left(\frac{c}{D}\right)}_3 (3c-p).$$

In the second equality, we use the cubic reciprocity law and the fact that $\left(\frac{3}{D}\right)_3 = 1$ (since $3, D \in \mathbb{Q}$). It follows that

$$L(C_D, 1) = \frac{\Omega}{-3p} \sum_{c \in (\mathcal{O}_K/p\mathcal{O}_K)^\times} \left(\frac{c}{D}\right)_3 \mathcal{E}_1^*\left(\frac{c\Omega}{-p} + \frac{\Omega}{3}, L\right).$$

We write $L = \mathbb{Z}u + \mathbb{Z}v$ with $\text{Im}(v/u) > 0$. We define the positive real number $A(L)$ by $A(L) = \frac{\bar{u}v - u\bar{v}}{2\pi i}$. Furthermore, we write

$$s_2(L) = \lim_{s>0, s \rightarrow 0} \sum_{w \in L \setminus \{0\}} w^{-2} |w|^{-2s}.$$

Let $\zeta(z, L)$ be the Weierstrass zeta function attached to L . Then by [6, Theorem 55], we have

$$\mathcal{E}_1^*(z, L) = \zeta(z, L) - z s_2(L) - \bar{z} A(L)^{-1}.$$

Note that by [15, pp. 390–392], we have $A(L) = \sqrt{3}\Omega^2/(2\pi)$, $s_2(L) = \frac{2}{\Omega}\zeta(\Omega/2, L) - \frac{2\pi}{\sqrt{3}\Omega^2}$ and $\zeta(\Omega/3, L) = \frac{2\pi}{3\sqrt{3}\Omega} + \frac{\sqrt{3}}{3}$. Hence the additive formula of the Weierstrass zeta function gives

$$\zeta\left(\frac{c\Omega}{-p} + \frac{\Omega}{3}, L\right) = \zeta\left(\frac{c\Omega}{-p}, L\right) + \frac{2\pi}{3\sqrt{3}\Omega} + \frac{1}{\sqrt{3}} + \frac{1}{2} \left(\frac{\wp'(c\Omega/(-p)) - \wp'(\Omega/3)}{\wp(c\Omega/(-p)) - \wp(\Omega/3)}\right).$$

From [24], we know that

$$\wp(\Omega/3) = 1, \quad \wp'(\Omega/3) = -\sqrt{3},$$

and we also have $\zeta(\Omega/2, L) = \pi/(\sqrt{3}\Omega)$ (see [15, p. 391]). Thus from all of the above, we obtain

$$L(C_D, 1) = \frac{\Omega}{-3p} \sum_c \left(\frac{c}{D}\right)_3 \left(\zeta\left(\frac{c\Omega}{-p}, L\right) + \frac{1}{2} \cdot \frac{\wp'(c\Omega/(-p)) + \sqrt{3}}{\wp(c\Omega/(-p)) - 1} + \frac{1}{\sqrt{3}} + \frac{2\pi\bar{c}}{\sqrt{3}\Omega p} \right),$$

where c runs over the elements of $(\mathcal{O}_K/p\mathcal{O}_K)^\times$. Now, since p is an odd prime, we can choose a set \mathfrak{C} of representatives of $(\mathcal{O}_K/p\mathcal{O}_K)^\times$ such that $c \in \mathfrak{C}$ implies $-c \in \mathfrak{C}$. Note that

$$\sum_{c \in \mathfrak{C}} \left(\frac{c}{p}\right)_3 = 0,$$

and that $\zeta(z, L)$ and $\wp'(z)$ are odd functions. Noting also that $\left(\frac{-1}{D}\right)_3 = 1$, we obtain

$$L(C_D, 1) = -\frac{\Omega}{2\sqrt{3}p} \sum_{c \in \mathfrak{C}} \left(\frac{c}{D}\right)_3 \frac{1}{\wp\left(\frac{c\Omega}{p}\right) - 1}$$

as required. \square

The curve A can also be written in the form

$$y^2 = x^3 - 16.$$

Now, we will construct a model \mathcal{A} of the curve A over a certain finite abelian extension of K so that \mathcal{A} has good reduction at 3. The main theoretical reason is the following theorem. The proof of the following theorem can be found in [5, Theorem 2] or [7, Theorem 2.4].

THEOREM 2.3. *Let E be an elliptic curve over K with complex multiplication by \mathcal{O}_K . Let $\mathfrak{p} = (\alpha)$ be any prime ideal of K at which E has good reduction. Denote by $E_{\mathfrak{p}}$ the subgroup of points in $E(\overline{K})$ which are contained in the kernel of the endomorphism α . Then E has good reduction everywhere over $K(E_{\mathfrak{p}})$.*

Thus we can construct a model of A over the field $\mathcal{K} = K(A_{(2-\sqrt{-3})})$, where $(2 - \sqrt{-3})$ is a prime ideal of K lying above the prime ideal $7\mathbb{Z}$ of \mathbb{Q} .

LEMMA 2.4. *Let \mathcal{K} be given as above. Then we have*

$$\mathcal{K} = K \left(\sqrt[6]{\frac{6\sqrt{-3}}{1+3\sqrt{-3}}} \right).$$

Proof. Since A has good reduction at 7, its formal group at 7 is a Lubin–Tate formal group. Therefore, the degree of \mathcal{K} over K is equal to 6, and $\text{Gal}(\mathcal{K}/K)$ is a cyclic Galois group. Since μ_6 is contained in K , by Kummer theory, we just need to find an element α in K such that $\sqrt[6]{\alpha}$ generates \mathcal{K} . One can do a direct calculation using the additive law and complex multiplication on the curve $y^2 = x^3 - 16$ to get such an α , and we leave the details to the reader. \square

Now, we make the change of variables $y = u^3Y$, $x = u^2X + r$ to the curve $y^2 = x^3 - 16$, where

$$u = \sqrt[6]{\frac{6\sqrt{-3}}{1 + 3\sqrt{-3}}} \quad \text{and} \quad r = 4\frac{u^2}{\sqrt{-3}}. \tag{2.4}$$

Then we obtain a model

$$\mathcal{A}: Y^2 = X^3 - 4\sqrt{-3}X^2 - 16X - 8 + 8\sqrt{-3} \tag{2.5}$$

of A . Note that since $\text{ord}_3(u) = \frac{1}{4}$, \mathcal{A} has good reduction at 3.

LEMMA 2.5. *If Q is a point on \mathcal{A} of order prime to 3, then either $X(Q) = 0$ or $\text{ord}_3(X(Q)) = 0$.*

Proof. The following proof is essentially an analogue of the same result in [16]. One can also find a proof in [27], but we give it here for the convenience of the reader. Denote by $\tilde{\mathcal{A}}$ the reduced curve of \mathcal{A} modulo 3, so that

$$\tilde{\mathcal{A}}: \tilde{Y}^2 = \tilde{X}^3 - \tilde{X} + 1.$$

Since \mathcal{A} has good reduction at 3, the torsion points of order prime to 3 on \mathcal{A} inject into $\tilde{\mathcal{A}}$, and if $Q_1 \neq \pm Q_2$ on \mathcal{A} , we have

$$X(Q_1) - X(Q_2) = \tilde{X}(\tilde{Q}_1) - \tilde{X}(\tilde{Q}_2) \neq 0. \tag{2.6}$$

Let $Q \neq 0$ be a point on \mathcal{A} satisfying $X(Q) = 0$. Then a direct computation shows $X(\sqrt{-3}Q) = X(2Q)$, so that Q is a $(2 - \sqrt{-3})$ - or a $(2 + \sqrt{-3})$ -torsion point. Let Q_1 be any point with $X(Q_1) \neq 0$. Then clearly $Q_1 \neq \pm Q$ since $X(Q) = X(-Q)$. Thus setting $Q_2 = Q$ in (2.6), we see that if $X(Q_1) \neq 0$ then $X(Q_1) \neq 0$, that is, $\text{ord}_3(X(Q_1)) = 0$. □

From now on, we write $(\wp(z), \wp'(z))$ for a point on $A: y^2 = 4x^3 - 1$, (x, y) for a point on the model $y^2 = x^3 - 16$ of A , and (X, Y) for a point the model \mathcal{A} whose equation is given in (2.5). The relation between the first two is given by

$$x = 4\wp(z) \quad y = 4\wp'(z). \tag{2.7}$$

Let $Q = (\wp(\frac{\Omega}{\Delta}), \wp'(\frac{\Omega}{\Delta}))$ be a point on A , where Δ is an integer prime to 3. If $c \in \mathcal{O}_K$ is prime to Δ , then since $x = u^2X + r$ and $\text{ord}_3(u) = 1/4$, Lemma 2.5 gives

$$4\wp\left(\frac{c\Omega}{\Delta}\right) = x([c]Q) \equiv r \pmod{3^{\frac{1}{2}}}. \tag{2.8}$$

Here, we denote by $[c]$ the complex multiplication by $c \in \mathcal{O}_K$. Note that r is a 3-adic unit which is independent of the point $[c]Q$, and thus $\wp\left(\frac{c\Omega}{\Delta}\right)$ is a 3-adic unit.

The following lemma will be repeatedly used in the remainder of this section and in Section 3.

LEMMA 2.6. *Let Δ be an integer prime to 3. Then we have*

1. $\wp\left(\frac{c\Omega}{\Delta}\right) - 1 \equiv 3^{\frac{1}{3}}u_1 \pmod{3^{\frac{1}{2}}}$, and
2. $\wp\left(\frac{c\Omega}{\Delta}\right)^3 - 1 \equiv 3u_1^3 \pmod{3^{\frac{7}{6}}}$

for a 3-adic unit u_1 which is independent of the point $[c]Q$. Moreover, we have $u_1^3 = (r - 1)^3/3$, where r is given in (2.4). We remark that “ $\pmod{3^\varepsilon}$ ” (for $\varepsilon > 0$) is taken in the ring of integers $\overline{\mathbb{Z}}_3$ of $\overline{\mathbb{Q}}_3$.

Proof. Noting that $x = u^2X + r$ and $\text{ord}_3(u) = \frac{1}{4}$, Lemma 2.5 gives the equality

$$x([c]Q) - 4 = x([c]Q) - 1 - 3 \equiv r - 1 \pmod{3^{\frac{1}{2}}}.$$

Recall from (2.4) that $r = 4\frac{u^2}{\sqrt{-3}}$. Thus, we have

$$r - 1 \equiv -\sqrt[3]{14}^{-1} \left(\sqrt[3]{1 - 3\sqrt{-3}} + \sqrt[3]{14} \right) \pmod{3}. \tag{2.9}$$

By considering the third power of $\sqrt[3]{1 - 3\sqrt{-3}} + \sqrt[3]{14}$, we know that $\sqrt[3]{1 - 3\sqrt{-3}} + \sqrt[3]{14}$ has 3-adic valuation equal to $\frac{1}{3}$. Therefore, defining $u_1 = \frac{r-1}{3^{\frac{1}{3}}}$ and noting that $4\wp\left(\frac{c\Omega}{\Delta}\right) = x([c]Q)$ and $4^{-1} \in 1 + 3\mathbb{Z}_3$, we obtain the first assertion.

For the second assertion, let $\omega = \frac{-1 + \sqrt{-3}}{2}$ be a primitive 3rd root of unity. Note that $\text{ord}_3(\omega^i - 1) = \frac{1}{2}$ for $i = 1, 2$, so that the first assertion gives

$$\wp\left(\frac{c\Omega}{\Delta}\right) - \omega^i \equiv \wp\left(\frac{c\Omega}{\Delta}\right) - 1 \equiv 3^{\frac{1}{3}}u_1 \pmod{3^{\frac{1}{2}}} \quad \text{for } i = 1, 2.$$

Thus

$$\begin{aligned} \wp\left(\frac{c\Omega}{\Delta}\right)^3 - 1 &= \prod_{j=0}^2 (3^{\frac{1}{3}}A_j + 3^{\frac{1}{3}}u_1) \\ &\equiv 3u_1^3 \pmod{3^{\frac{7}{6}}}. \end{aligned}$$

Here, A_j ($j = 0, 1, 2$) are 3-adic integers. The second assertion now follows. \square

THEOREM 2.7 (Zhang [27]). *Let $p \equiv 2, 5 \pmod{9}$ be an odd prime, and recall that $D = p$ or p^2 . Then*

$$L(C_D, 1) \neq 0$$

and $\text{ord}_3\left(\frac{L(C_D, 1)}{\Omega_D}\right) = 0$. Moreover, the 3-part of the Birch–Swinnerton-Dyer conjecture holds for C_D .

Proof. The following proof is contained in [27], but we give it here for the convenience of the reader. By Proposition 2.2, we have

$$\frac{2p\sqrt{3}}{\Omega}L(C_D, 1) = -\sum_{c \in \mathfrak{c}} \left(\frac{c}{D}\right)_3 \frac{1}{\wp\left(\frac{c\Omega}{p}\right) - 1}.$$

Now, we define

$$B_k = \left\{ c \in \mathfrak{C} : \left(\frac{c}{D} \right)_3 = \omega^k \right\}$$

where $k = 0, 1, 2$. We use the convention that $k + 1, k + 2$ are also in $\{0, 1, 2\}$ via taking modulo 3 in the following argument.

We define

$$S_k = \sum_{c \in B_k} \frac{1}{\wp \left(\frac{c\Omega}{p} \right) - 1}.$$

Note that $\left(\frac{\omega}{p} \right)_3 = \omega$ or ω^2 according as $p \equiv 2 \pmod 9$ or $p \equiv 5 \pmod 9$, and that $\omega \wp \left(\frac{c\Omega}{p} \right) = \wp \left(\frac{\omega c\Omega}{p} \right)$. Then

$$\omega B_k = \begin{cases} B_{k+1} & \text{if } D = p \text{ and } p \equiv 2 \pmod 9 \text{ or if } D = p^2 \text{ and } p \equiv 5 \pmod 9, \\ B_{k+2} & \text{if } D = p \text{ and } p \equiv 5 \pmod 9 \text{ or if } D = p^2 \text{ and } p \equiv 2 \pmod 9. \end{cases}$$

We just give the details of the proof in the cases $D = p$ with $p \equiv 2 \pmod 9$ and $D = p^2$ with $p \equiv 5 \pmod 9$. The other cases can be proven in the same way. In these cases, we have

$$\begin{aligned} -\frac{2p\sqrt{3}}{\Omega} L(C_D, 1) &= \sum_{c \in B_0} \left(\frac{1}{\wp \left(\frac{c\Omega}{p} \right) - 1} + \frac{\omega}{\omega \wp \left(\frac{c\Omega}{p} \right) - 1} + \frac{\omega^2}{\omega^2 \wp \left(\frac{c\Omega}{p} \right) - 1} \right) \\ &= \sum_{c \in B_0} \frac{3\wp \left(\frac{c\Omega}{p} \right)^2}{\wp \left(\frac{c\Omega}{p} \right)^3 - 1}. \end{aligned}$$

Now, by (2.8) and Lemma 2.6, we have

$$3\wp \left(\frac{c\Omega}{p} \right)^2 \equiv 3r^2 \pmod{3^{\frac{3}{2}}}, \quad \wp \left(\frac{c\Omega}{p} \right)^3 - 1 \equiv 3u_1^3 \pmod{3^{\frac{7}{6}}}.$$

Recalling that u_1 and r are independent of c , we obtain

$$-\frac{2p\sqrt{3}}{\Omega} L(C_D, 1) \equiv (r^2 u_1^{-3}) \cdot \#(B_0) \pmod{3^{\frac{1}{6}}}$$

which is a 3-adic unit, since $\#(B_0) = \frac{p^2-1}{3}$ is prime to 3 when $p \equiv 2, 5 \pmod 9$. Noting that

$$\Omega_D = \frac{\Omega}{\sqrt{3}D^{\frac{1}{3}}}$$

and D is prime to 3, we obtain $\text{ord}_3 \left(\frac{L(C_D, 1)}{\Omega_D} \right) = 0$. The theorem follows since we know that the 3-part of $\text{III}(C_D)$ is trivial by 3-descent (see [27]). \square

It follows from Theorem 2.7 of Zhang that $\frac{L(C_D, 1)}{\Omega_D} \in \mathbb{Z}_3^\times$, and we can study its value modulo 3. Now, we can prove the explicit modulo 3 Birch–Swinnerton-Dyer conjecture for C_D .

LEMMA 2.8.

1. If $p \equiv 5 \pmod{9}$, then

$$\frac{L(C_{p^2}, 1)}{2\Omega_{p^2}} \equiv \frac{L(C_p, 1)}{\Omega_p} \pmod{3}.$$

2. If $p \equiv 2 \pmod{9}$, then

$$\frac{L(C_{p^2}, 1)}{\Omega_{p^2}} \equiv \frac{L(C_p, 1)}{2\Omega_p} \pmod{3}.$$

We remark that the factor 2 in the denominators of the above congruences comes from the Tamagawa factor of C_D at 3.

Proof. We just give the details of the proof for (1), and (2) can be obtained similarly. By Proposition 2.2 and the definition of Ω_d , we have

$$\frac{L(C_{p^2}, 1)}{2\Omega_{p^2}} = -\frac{\sqrt[3]{p^2}}{4p} \sum_{c \in \mathfrak{C}} \left(\frac{c}{p^2}\right)_3 \frac{1}{\wp\left(\frac{c\Omega}{p}\right) - 1}$$

and

$$\frac{L(C_p, 1)}{\Omega_p} = -\frac{\sqrt[3]{p}}{2p} \sum_{c \in \mathfrak{C}} \left(\frac{c}{p}\right)_3 \frac{1}{\wp\left(\frac{c\Omega}{p}\right) - 1}.$$

Recall that $\omega = \frac{-1 + \sqrt{-3}}{2}$. Since $\text{ord}_3(\omega^i - \omega^j) \geq \frac{1}{2}$ for $i, j = 0, 1, 2$, we obtain

$$\text{ord}_3 \left(\left(\frac{c}{p^2}\right)_3 - \left(\frac{c}{p}\right)_3 \right) \geq \frac{1}{2}.$$

From Lemma 2.6, we know that

$$\text{ord}_3 \left(\wp\left(\frac{c\Omega}{p}\right) - 1 \right) = \frac{1}{3}.$$

We define

$$B_1 := \sum_{c \in \mathfrak{C}} \left(\frac{c}{p^2}\right)_3 \frac{1}{\wp\left(\frac{c\Omega}{p}\right) - 1}$$

and

$$B_2 := \sum_{c \in \mathfrak{C}} \left(\frac{c}{p}\right)_3 \frac{1}{\wp\left(\frac{c\Omega}{p}\right) - 1}.$$

Then

$$\text{ord}_3(B_1 - B_2) \geq \frac{1}{6}.$$

Furthermore, we define $A_1 := -\frac{\sqrt[3]{p^2}}{4p}$ and $A_2 := -\frac{\sqrt[3]{p}}{2p}$. Noting that $p \equiv 2 \pmod 3$, we have

$$\sqrt[3]{p} \equiv 2 \pmod{3^{\frac{1}{3}}},$$

and thus

$$A_1 - A_2 \equiv 0 \pmod{3^{\frac{1}{3}}}.$$

Now, by the relations

$$\frac{L(C_{p^2}, 1)}{2\Omega_{p^2}} = A_1 B_1, \quad \frac{L(C_p, 1)}{\Omega_p} = A_2 B_2$$

and the identity

$$A_1 B_1 - A_2 B_2 = (A_1 - A_2) B_1 + A_2 (B_1 - B_2),$$

we obtain that $3^{\frac{1}{6}}$ divides

$$\frac{L(C_{p^2}, 1)}{2\Omega_{p^2}} - \frac{L(C_p, 1)}{\Omega_p}.$$

Our assertion now follows on noting that these L -values are in \mathbb{Z}_3 . □

From Theorem 2.7, we know that the residue class of the two congruences in Lemma 2.8 are non-zero modulo 3. Now, we use Zhao’s induction argument to obtain the main result of this section giving the precise residue class modulo 3 in which these L -values lie.

THEOREM 2.9.

1. For $p \equiv 5 \pmod 9$, we have

$$\frac{L(C_p, 1)}{\Omega_p} \equiv \frac{L(C_{p^2}, 1)}{2\Omega_{p^2}} \equiv 1 \pmod 3.$$

Moreover, the explicit modulo 3 Birch–Swinnerton-Dyer conjecture holds for C_p and C_{p^2} .

2. For $p \equiv 2 \pmod 9$, we have

$$\frac{L(C_p, 1)}{2\Omega_p} \equiv \frac{L(C_{p^2}, 1)}{\Omega_{p^2}} \equiv 1 \pmod 3.$$

Moreover, the explicit modulo 3 Birch–Swinnerton-Dyer conjecture holds for C_p and C_{p^2} .

For simplicity, we denote by δ the period Ω_p of C_p in the following. We will just give the details for the case $p \equiv 5 \pmod{9}$, and the other case is similar. Recall that $K(3p)$ is the ray class field of K modulo $(3p)$. Then we have $\sqrt[3]{p} \in K(3p)$, and we recall that H_p is the field $K(\sqrt[3]{p})$.

For any positive divisor $d \mid (p)^2$, we know that the period relation

$$\Omega_d = \delta \sqrt[3]{(p/d)} \quad (2.10)$$

holds.

By formula 2.2, and the period relation (2.10), we have

$$\frac{L^{(3p)}(C_d, 1)}{\delta \sqrt[3]{p}} = \sum_{\sigma \in \text{Gal}(K(3p)/K)} (\sqrt[3]{d})^{\sigma-1} \frac{1}{3p} \mathcal{E}_1^* \left(\frac{\delta \sqrt[3]{p}}{3p}, \delta \sqrt[3]{p} \mathcal{O}_K \right)^\sigma.$$

Note that $\sum_d (\sqrt[3]{d})^{\sigma-1} = 3$ if σ fixes $\sqrt[3]{d}$, and $\sum_d (\sqrt[3]{d})^{\sigma-1} = 0$ otherwise. Now, summing the above formula over all $d \mid (p)^2$ and noting $\sqrt[3]{p} \in H_p$, we obtain

$$\sum_{d \mid (p)^2} \frac{L^{(3p)}(C_d, 1)}{\delta} = 3 \text{Tr}_{K(3p)/H_p} \left(\frac{1}{3p} \mathcal{E}_1^* \left(\frac{\delta}{3p}, \delta \mathcal{O}_K \right) \right). \quad (2.11)$$

First, we study the terms on the left hand side of (2.11). We write u ($= 1$ or 2) for the residue class of $\frac{L(C_p, 1)}{\Omega_p} \pmod{3}$. Then we have

LEMMA 2.10.

1. For $d = 1$, we have $\frac{L^{(3p)}(C, 1)}{\delta} = \frac{\sqrt[3]{p}(p+1)}{3p} \in (\sqrt[3]{p} + 3\overline{\mathbb{Z}}_3) = 2 + 3\frac{1}{3}\overline{\mathbb{Z}}_3$.
2. For $d = p$, we have $\frac{L^{(3p)}(C_p, 1)}{\delta} = \frac{L(C_p, 1)}{\Omega_p} \in u + 3\overline{\mathbb{Z}}_3$.
3. For $d = p^2$, we have $\frac{L^{(3p)}(C_{p^2}, 1)}{\delta} = \frac{L(C_{p^2}, 1)}{\sqrt[3]{p}\Omega_{p^2}} \in \frac{2u}{\sqrt[3]{p}} + 3\overline{\mathbb{Z}}_3$.

As for the right hand side of (2.11), we have the following standard calculation. Here, we recall that $\Omega = \delta \sqrt{3} \sqrt[3]{p}$. We will use the same set \mathfrak{C} of representatives of $\text{Gal}(K(3p)/K) \simeq (\mathcal{O}_K/p\mathcal{O}_K)^\times$ as in Proposition 2.2. We denote by V the subset of \mathfrak{C} such that $c \in V$ if and only if $\left(\frac{c}{p}\right)_3 = 1$. We see that H_p is precisely the fixed field of the subgroup generated by the Artin symbol of elements in V , and thus V gives a set of representative for $\text{Gal}(K(3p)/H_p)$. Recall that ψ_p is the Hecke character over K associated to C_p . Then

$$\begin{aligned}
 \Psi &:= 3\mathrm{Tr}_{K(3p)/H_p} \left(\frac{1}{3p} \mathcal{E}_1^* \left(\frac{\delta}{3p}, \delta \mathcal{O}_K \right) \right) \\
 &= -\frac{1}{p} \mathrm{Tr}_{K(3p)/H_p} \left(\mathcal{E}_1^* \left(\frac{\delta}{-3p}, \delta \mathcal{O}_K \right) \right) \\
 &= -\frac{1}{p\delta} \cdot \delta \sum_{c \in V} \mathcal{E}_1^* \left(\frac{\psi_p((3c-p))\delta}{-3p}, \delta \mathcal{O}_K \right) \\
 &= -\frac{1}{p\delta} \cdot \Omega \sum_{c \in V} \mathcal{E}_1^* \left(\frac{\psi_p((3c-p))\Omega}{-3p}, \Omega \mathcal{O}_K \right) \\
 &= -\frac{1}{p} \sum_{c \in V} \mathcal{E}_1^* \left(\frac{\psi_p((3c-p))\Omega}{-3p}, \Omega \mathcal{O}_K \right) \sqrt[3]{p}\sqrt{3}.
 \end{aligned}$$

Noting that, by our choice of \mathfrak{C} , we have $-c \in V$ whenever $c \in V$, the same argument as in the proof of Proposition 2.2 shows

$$\Psi = -\frac{3\sqrt[3]{p}}{2p} \sum_{c \in V} \frac{1}{\wp \left(\frac{c\Omega}{p} \right) - 1} - \frac{\sqrt[3]{p}}{p} \#(V), \tag{2.12}$$

where $\#(V) = \frac{p^2-1}{3}$.

Now, from Lemma 2.6, we know that the first term on the right hand side of (2.12) has a positive 3-adic valuation, while the second term in (2.12) is

$$-\frac{\sqrt[3]{p}}{p} \#(V) = -\frac{\sqrt[3]{p}}{p} \left(\frac{p+1}{3} \right) (p-1) \in 2\sqrt[3]{p} + 3\overline{\mathbb{Z}}_3.$$

Moreover, Lemma 2.10 and (2.11) give

$$\frac{L(C_p, 1)}{\delta} + \frac{L(C_{p^2}, 1)}{\delta} \in \sqrt[3]{p} + 3\overline{\mathbb{Z}}_3 = 2 + 3^{\frac{1}{3}}\overline{\mathbb{Z}}_3. \tag{2.13}$$

On the other hand, by (2) and (3) of Lemma 2.10, the sum in (2.13) is contained in

$$(u + 3\overline{\mathbb{Z}}_3) + \left(\frac{2u}{\sqrt[3]{p}} + 3\overline{\mathbb{Z}}_3 \right) = u \left(1 + \frac{2}{\sqrt[3]{p}} \right) + 3\overline{\mathbb{Z}}_3 = 2u + 3^{\frac{1}{3}}\overline{\mathbb{Z}}_3. \tag{2.14}$$

Here, we use the fact that

$$\sqrt[3]{p} \equiv 2 \pmod{3^{\frac{1}{3}}}$$

and $3^{\frac{1}{3}}$ exactly divides $\sqrt[3]{p} - 2$ when $p \equiv 5 \pmod{9}$. Comparing formulas (2.13) and (2.14), we obtain $u = 1$. This completes the proof of Theorem 2.9.

3 EXPLICIT MODULO 3 BIRCH–SWINNERTON-DYER CONJECTURE FOR $C_{2^i p^j}$

The goal of this section is to give the proof of Theorem 1.1. We prove this in the following steps. Firstly, we use Zhao’s induction argument to show that

the sum of algebraic part of L -values of C_{2p} and $C_{2^2p^2}$ (resp. C_{2p^2} and C_{2^2p}) is non-zero when $p \equiv 5 \pmod{9}$ (resp. $p \equiv 2 \pmod{9}$) and satisfies an explicit modulo 3 congruence. Secondly, by establishing some congruences between the algebraic L -values in the sum of the first step, we can show each term in the sum is non-zero and satisfies the explicit modulo 3 Birch–Swinnerton-Dyer conjecture. In this section, we again write D for p or p^2 . The first key result of this section is the following.

THEOREM 3.1.

1. If $p \equiv 5 \pmod{9}$, we have

$$\frac{L(C_{2p}, 1)}{\Omega_1} + \frac{L(C_{2^2p^2}, 1)}{\Omega_1} \in 3(2 + 3^{\frac{1}{3}}\overline{\mathbb{Z}}_3)$$

and

$$\frac{L(C_{2p}, 1)}{\Omega_{2p}} + \frac{L(C_{2^2p^2}, 1)}{\Omega_{2^2p^2}} \in 3(2 + 3\mathbb{Z}_3).$$

2. If $p \equiv 2 \pmod{9}$, we have

$$\frac{L(C_{2^2p}, 1)}{\Omega_1} + \frac{L(C_{2p^2}, 1)}{\Omega_1} \in 3(1 + 3^{\frac{1}{3}}\overline{\mathbb{Z}}_3)$$

and

$$\frac{L(C_{2^2p}, 1)}{\Omega_{2^2p}} + \frac{L(C_{2p^2}, 1)}{\Omega_{2p^2}} \in 3(2 + 3\mathbb{Z}_3).$$

We will only give the details for the case $p \equiv 5 \pmod{9}$, and leave the proof for the other case to the reader. Before the proof, we remark that, by a root number consideration (for details, see [12]), we know that $L(C_{2p^2}, 1) = L(C_{2^2p}, 1) = 0$ (resp. $L(C_{2p}, 1) = L(C_{2^2p^2}, 1) = 0$) when $p \equiv 5 \pmod{9}$ (resp. $p \equiv 2 \pmod{9}$). For simplicity, we write γ for Ω_{2p} in the following. Then we have the following period relation:

$$\Omega_d = \gamma \sqrt[3]{\frac{2p}{d}}. \quad (3.1)$$

We recall that $\mathcal{H}_p = K(\sqrt[3]{2}, \sqrt[3]{p})$.

LEMMA 3.2. *We have $\sqrt[3]{p}, \sqrt[3]{2} \in K(6p)$, and the degree of the field extension $[K(6p) : \mathcal{H}_p] = \frac{p^2-1}{3}$, which is prime to 3.*

Proof. Since K has class number 1, given any prime ideal $\mathfrak{q} = \alpha \mathcal{O}_K$ of \mathcal{O}_K which is prime to $6p$ and $\alpha \equiv 1 \pmod{3}$, the Artin symbol $\sigma_{\mathfrak{q}}$ of \mathfrak{q} in $\text{Gal}(K(6p)/K)$ acts on $\sqrt[3]{p}$ via

$$(\sqrt[3]{p})^{\sigma_{\mathfrak{q}}} = \left(\frac{p}{\alpha}\right)_3 \sqrt[3]{p},$$

where $(\cdot)_3$ denotes the cubic residue symbol. The Galois action on $\sqrt[3]{2}$ is given similarly. Thus, for any prime ideal \mathfrak{m} whose generator is congruent to 1

modulo $6p$, we know that $\sqrt[3]{p}, \sqrt[3]{2}$ are fixed by the Artin symbol σ_m , and the first assertion follows. For the second assertion, note that $\text{Gal}(K(6p)/K) \simeq (\mathcal{O}_K/2p\mathcal{O}_K)^\times$. Hence $[K(6p) : K(\sqrt[3]{p}, \sqrt[3]{2})] = \frac{p^2-1}{3}$, which is prime to 3 by our assumption that $p \equiv 2, 5 \pmod{9}$. \square

For each d with $0 < d \mid (2p)^2$, from (2.2), and the period relation (3.1), we have

$$\frac{L^{(6p)}(C_d, 1)}{\gamma \sqrt[3]{2p}} = \sum_{\sigma \in \text{Gal}(K(6p)/K)} \frac{1}{6p} (\sqrt[3]{d})^{\sigma-1} \left(\mathcal{E}_1^* \left(\frac{\gamma \sqrt[3]{2p}}{6p}, \gamma \sqrt[3]{2p} \mathcal{O}_K \right) \right)^\sigma.$$

Taking the sum over all $0 < d \mid (2p)^2$, we obtain the following in the same way we obtained (2.11):

$$\sum_{d \mid (2p)^2} \frac{L^{(6p)}(C_d, 1)}{\gamma \sqrt[3]{2p}} = 3^2 \text{Tr}_{K(6p)/\mathcal{H}_p} \left(\frac{1}{6p} \mathcal{E}_1^* \left(\frac{\gamma \sqrt[3]{2p}}{6p}, \gamma \sqrt[3]{2p} \mathcal{O}_K \right) \right). \tag{3.2}$$

First, we deal with terms on the left hand side of (3.2). We list the results in the following two lemmas, and leave the proofs to the reader.

LEMMA 3.3. *We have*

1. $\frac{L^{(6p)}(C_1, 1)}{\gamma \sqrt[3]{2p}} \in 3(2 + 3\overline{\mathbb{Z}}_3)$.
2. $\frac{L^{(6p)}(C_2, 1)}{\gamma \sqrt[3]{2p}} \in 3(\sqrt[3]{2^2} + 3\overline{\mathbb{Z}}_3)$.
3. $\frac{L^{(6p)}(C_4, 1)}{\gamma \sqrt[3]{2p}} \in 3\left(\frac{1}{\sqrt[3]{2^2}} + 3\overline{\mathbb{Z}}_3\right)$.

By Theorem 2.9, we have the following estimate.

LEMMA 3.4. *We have*

1. $\frac{L^{(6p)}(C_p, 1)}{\gamma \sqrt[3]{2p}} \in 3\left(\frac{2}{\sqrt[3]{p}} + 3\overline{\mathbb{Z}}_3\right)$.
2. $\frac{L^{(6p)}(C_{p^2}, 1)}{\gamma \sqrt[3]{2p}} \in 3\left(\frac{1}{\sqrt[3]{p^2}} + 3\overline{\mathbb{Z}}_3\right)$.

Moreover,

$$\frac{L^{(6p)}(C_p, 1)}{\gamma \sqrt[3]{2p}} + \frac{L^{(6p)}(C_{p^2}, 1)}{\gamma \sqrt[3]{2p}} \in 3\left(\frac{2\sqrt[3]{p} + 1}{\sqrt[3]{p^2}} + 3\overline{\mathbb{Z}}_3\right) = 3(2 + 3^{\frac{1}{3}}\overline{\mathbb{Z}}_3),$$

where we use the fact that $\text{ord}_3(\sqrt[3]{p} - 2) = \frac{1}{3}$.

LEMMA 3.5. *Define*

$$\Phi := \mathrm{Tr}_{K(6p)/\mathcal{H}_p} \left(\frac{1}{6p} \mathcal{E}_1^* \left(\frac{\gamma \sqrt[3]{2p}}{6p}, \gamma \sqrt[3]{2p} \mathcal{O}_K \right) \right).$$

Then

$$3^2 \Phi \in 3(2 + 3^{\frac{2}{3}} \overline{\mathbb{Z}}_3).$$

Proof. Since $\sqrt[3]{2p} \in \mathcal{H}_p$, we have

$$\Phi = \frac{1}{\sqrt[3]{2p}} \mathrm{Tr}_{K(6p)/\mathcal{H}_p} \left(\frac{1}{6p} \mathcal{E}_1^* \left(\frac{\gamma}{6p}, \gamma \mathcal{O}_K \right) \right).$$

We know that $\mathrm{Gal}(K(6p)/K)$ is isomorphic to

$$(\mathcal{O}_K/6p\mathcal{O}_K)^\times / \mu_6 \simeq (\mathcal{O}_K/2p\mathcal{O}_K)^\times, \quad (3.3)$$

where we identify μ_6 with $(\mathcal{O}_K/3\mathcal{O}_K)^\times$, and the isomorphism from right to left is given by sending any element c of $(\mathcal{O}_K/2p\mathcal{O}_K)^\times$ to $3c + 2p$. Here, we note that $2p \equiv 1 \pmod{3}$.

For the set of representatives $\{3c + 2p : c \in (\mathcal{O}_K/2p\mathcal{O}_K)^\times\}$ of (3.3), we know that the Artin symbol of the ideal $(3c + 2p)$ in $\mathrm{Gal}(K(6p)/K)$ fixes $\sqrt[3]{2}$ and $\sqrt[3]{p}$ if and only if

$$\left(\frac{p}{3c + 2p} \right)_3 = \left(\frac{c}{p} \right)_3 = 1$$

and

$$\left(\frac{2}{3c + 2p} \right)_3 = \left(\frac{c}{2} \right)_3 = 1$$

hold. Therefore, we can identify

$$V := \left\{ c \in (\mathcal{O}_K/2p\mathcal{O}_K)^\times : \left(\frac{c}{p} \right)_3 = \left(\frac{c}{2} \right)_3 = 1 \right\}$$

with the Galois group $\mathrm{Gal}(K(6p)/\mathcal{H}_p)$. Since $\left(\frac{-1}{c} \right)_3 = 1$, we can choose a set of representatives of V in \mathcal{O}_K such that $c \in V$ implies $-c \in V$.

Then by the action of Artin symbols on $\mathcal{E}_1^* \left(\frac{\gamma}{6p}, \gamma \mathcal{O}_K \right)$ (see the proof in [6, Theorem 60]), we have

$$\Phi = \frac{1}{6p\sqrt[3]{2p}} \sum_{c \in V} \mathcal{E}_1^* \left(\frac{\psi_{2p}((3c + 2p))\gamma}{6p}, \gamma \mathcal{O}_K \right).$$

Recalling the definition of ψ_{2p} in (2.1), it follows that

$$\Phi = \frac{1}{6p\sqrt[3]{2p}} \sum_{c \in V} \mathcal{E}_1^* \left(\frac{c\gamma}{2p} + \frac{\gamma}{3}, \gamma \mathcal{O}_K \right).$$

Now, noting that $\Omega = \gamma\sqrt{3}\sqrt[3]{2p}$ and $L = \Omega\mathcal{O}_K$, we obtain

$$\Phi = \frac{1}{2\sqrt{3p}} \sum_{c \in V} \mathcal{E}_1^* \left(\frac{c\Omega}{2p} + \frac{\Omega}{3}, L \right).$$

By a similar method as in the proof of Proposition 2.2, we have

$$\Phi = \frac{1}{4p} \sum_{c \in V} \frac{1}{\wp \left(\frac{c\Omega}{2p} \right) - 1} + \frac{1}{6p} \#(V).$$

Furthermore, from Lemma 2.6, we know

$$\text{ord}_3 \left(\wp \left(\frac{c\Omega}{2p} \right) - 1 \right) = \frac{1}{3}.$$

The lemma now follows on noting that we have $\#(V) = \frac{p^2-1}{3}$ by Lemma 3.2 and $p \equiv 5 \pmod{9}$. □

By Lemmas 3.3 and 3.4, we have

$$\mathcal{A} := \sum_{d|4} \frac{L^{(6p)}(C_d, 1)}{\gamma\sqrt[3]{2p}} \in 3(2 + \sqrt[3]{2^2} + \frac{1}{\sqrt[3]{2^2}} + 3\overline{\mathbb{Z}}_3) = 3(1 + 3^{\frac{1}{3}}\overline{\mathbb{Z}}_3)$$

and

$$\mathcal{B} := \sum_{d \neq 1, d|p^2} \frac{L^{(6p)}(C_d, 1)}{\gamma \cdot \sqrt[3]{2p}} \in 3(2 + 3^{\frac{1}{3}}\overline{\mathbb{Z}}_3).$$

Here, we use the fact

$$2 + \sqrt[3]{2^2} + (\sqrt[3]{2^2})^{-1} \in 1 + 3^{\frac{1}{3}}\overline{\mathbb{Z}}_3.$$

Now, a root number consideration combined with Lemmas 3.3, 3.4, 3.5 and formula (3.2) gives

$$\frac{L(C_{2p}, 1)}{\Omega_1} + \frac{L(C_{2^2p^2}, 1)}{\Omega_1} = 3^2\Phi - \mathcal{A} - \mathcal{B} \in 3(2 + 3^{\frac{1}{3}}\overline{\mathbb{Z}}_3), \tag{3.4}$$

where we use the fact that $\sqrt[3]{p} \cdot \gamma = \Omega_1$. Thus, the first equation of Theorem 3.1 (1) holds. The second equation follows on noting that the algebraic part of the L -values of C_{2p} and $C_{2^2p^2}$ are rational numbers and that these algebraic L -values are divisible by 3 in $\overline{\mathbb{Z}}_3$, which will be shown in (3.13). This completes the proof of Theorem 3.1.

Now, we will show that each L -value in the sum in Theorem 3.1 is non-zero. This is achieved by establishing certain congruence formulas between the algebraic L -values of C_{2p} and $C_{2^2p^2}$ (resp. C_{2^2p} and C_{2p^2}) for $p \equiv 5 \pmod{9}$ (resp. $p \equiv 2 \pmod{9}$). The main result of this section is the following.

THEOREM 3.6.

1. Assume $p \equiv 2 \pmod{9}$, then we have

$$\frac{L(C_{2^{2p}}, 1)}{3\Omega_{2^{2p}}} \equiv \frac{L(C_{2p^2}, 1)}{3\Omega_{2p^2}} \equiv 1 \pmod{3}.$$

2. Assume $p \equiv 5 \pmod{9}$, then we have

$$\frac{L(C_{2p}, 1)}{3\Omega_{2p}} \equiv \frac{L(C_{2^{2p^2}}, 1)}{3\Omega_{2^{2p^2}}} \equiv 1 \pmod{3}.$$

We will give the details of the proof for the case $p \equiv 5 \pmod{9}$, and the other case is similar.

PROPOSITION 3.7. *The element $\sqrt{3}$ is not in the field $K(6p)$.*

Proof. For the field extensions $\mathbb{Q} \subset K \subset L$, we have the following conductor-like formula:

$$\mathfrak{d}_{L/\mathbb{Q}} = \mathfrak{d}_{K/\mathbb{Q}}^{[K:\mathbb{Q}]} \cdot N_{K/\mathbb{Q}}(\mathfrak{d}_{L/K}),$$

where $\mathfrak{d}_{M/J}$ denotes the discriminant ideal of \mathcal{O}_J for an extension M/J and \mathcal{O}_J denotes the ring of integer of J . Note that $\mathbb{Q}(\sqrt{3}, \sqrt{-3})$ is a splitting field of $x^4 + 8x^2 + 4$ over \mathbb{Q} with discriminant $2^4 3^2$. Thus $K(\sqrt{3})/K$ has conductor (4), and $\sqrt{3}$ cannot be in $K(6p)$. \square

PROPOSITION 3.8. *We can choose a set of representatives \mathcal{C} of $(\mathcal{O}_K/2p\mathcal{O}_K)^\times$ in \mathcal{O}_K such that $c \in \mathcal{C}$ whenever $-c \in \mathcal{C}$, and the Artin symbol of c in $\text{Gal}(K(6p)(\sqrt{3})/K)$ fixes $\sqrt{3}$.*

Proof. By Proposition 3.7, we know the fields $K(\sqrt{3})$ and $K(6p)$ are linearly disjoint over K . Thus, given an element $\tau_1 \in \text{Gal}(K(6p)/K)$ and the identity element $\iota \in \text{Gal}(K(\sqrt{3})/K)$, the Chebotarev density theorem gives an element $c_1 \in \mathcal{O}_K$ prime to $6p$ whose Artin symbol σ_{c_1} in $\text{Gal}(K(6p)(\sqrt{3})/K)$ satisfies $\sigma_{c_1}|_{K(6p)} = \tau_1$ and $\sigma_{c_1}|_{K(\sqrt{3})} = \iota$.

Now, viewing $c_1 \in (\mathcal{O}_K/2p\mathcal{O}_K)^\times$ via the isomorphism in (3.3), we know that $-c_1$ gives another element in $\text{Gal}(K(6p)(\sqrt{3})/K)$ whose restriction to $K(\sqrt{3})$ is ι , since by class field theory the Artin symbol of $-c_1$ acts on $\sqrt{3}$ via the norm map from K to \mathbb{Q} , so must act trivially on $\sqrt{3}$ (since c_1 acts trivially on $\sqrt{3}$). In this way, we can choose the set \mathcal{C} , and the lemma follows. \square

From now on, we fix the above choice of the representatives \mathcal{C} . We denote by V_p the Galois group $\text{Gal}(K(6p)/H_p)$. We view V_p as the subset

$$V_p = \left\{ c \in \mathcal{C} : \left(\frac{c}{p} \right)_3 = 1 \right\}$$

of \mathcal{C} . Let V_{2p} the subset of \mathcal{C} giving a set of representatives of the Galois group $\text{Gal}(K(6p)/\mathcal{H}_p)$.

In the following argument, we will study the partial summation from Zhao’s method. For simplicity, we write t for 2 or 2^2 , and we will study the relations between the L -values of C_t , C_{tp} and C_{tp^2} . We need to use the key result in Theorem 2.9 on the explicit modulo 3 Birch–Swinnerton-Dyer conjecture for C_p and C_{p^2} .

Given any $0 < d \mid (p)^2$, we denote by η_t the period of C_{tp} for simplicity. Then we have the period relation

$$\Omega_{td} = \eta_t \cdot \sqrt[3]{\frac{p}{d}}. \tag{3.5}$$

For any such d , using the above period relation (3.5) and formula (2.2), we have

$$\frac{L^{(6p)}(C_{td}, 1)}{\eta_t \sqrt[3]{p}} = \frac{1}{6p} \sum_{\sigma \in \text{Gal}(K(6p)/K)} (\sqrt[3]{d})^{\sigma-1} \mathcal{E}_1^* \left(\frac{\eta_t \sqrt[3]{p}}{6p}, \eta_t \sqrt[3]{p} \mathcal{O}_K \right)^\sigma. \tag{3.6}$$

Now, taking the sum over all d dividing p^2 in (3.6), we obtain

$$\sum_{d \mid p^2} \frac{L^{(6p)}(C_{td}, 1)}{\eta_t \cdot \sqrt[3]{p}} = \frac{3}{6p} \text{Tr}_{K(6p)/H_p} \left(\mathcal{E}_1^* \left(\frac{\eta_t \sqrt[3]{p}}{6p}, \eta_t \sqrt[3]{p} \mathcal{O}_K \right) \right) \quad t = 2, 2^2.$$

First, we consider the case $t = 2$.

LEMMA 3.9. *We have*

$$\frac{L^{(6p)}(C_2, 1)}{\eta_t \sqrt[3]{p}} \in 3(2 + 3\overline{\mathbb{Z}}_3).$$

LEMMA 3.10. *We have*

$$\frac{3}{6p} \text{Tr}_{K(6p)/H_p} \left(\mathcal{E}_1^* \left(\frac{\eta_t \sqrt[3]{p}}{6p}, \eta_t \sqrt[3]{p} \mathcal{O}_K \right) \right) = \frac{3}{4p} \text{Tr}_{\mathcal{H}_p/H_p} \left(\sqrt[3]{2} \sum_{c \in V_{2p}} \frac{1}{\wp \left(\frac{c\Omega}{2p} \right) - 1} \right).$$

Proof. Recall that we use the set \mathcal{C} of representatives of $\text{Gal}(K(6p)/K)$ chosen in Proposition 3.8. We take the trace of $\mathcal{E}_1^* \left(\frac{\eta_t \sqrt[3]{p}}{6p}, \eta_t \sqrt[3]{p} \mathcal{O}_K \right)$ from $K(6p)$ to K in the following two steps: first from $K(6p)$ to \mathcal{H}_p , then from \mathcal{H}_p to H_p . Noting the Galois action on $\mathcal{E}_1^* \left(\frac{\eta_t \sqrt[3]{p}}{6p}, \eta_t \sqrt[3]{p} \mathcal{O}_K \right)$ as described in [6], the period relation

$$\eta_t \cdot \sqrt[3]{2p} \cdot \sqrt{3} = \Omega$$

and that $\sqrt{3}$ is fixed by \mathcal{C} , we obtain the following equality after taking the trace map from $K(6p)$ to \mathcal{H}_p :

$$\frac{3}{6p} \text{Tr}_{K(6p)/H_p} \left(\mathcal{E}_1^* \left(\frac{\eta_t \sqrt[3]{p}}{6p}, \eta_t \sqrt[3]{p} \mathcal{O}_K \right) \right) = \frac{\sqrt{3}}{2p} \text{Tr}_{\mathcal{H}_p/H_p} \left(\sqrt[3]{2} \sum_{c \in V_{2p}} \mathcal{E}_1^* \left(\frac{c\Omega}{2p} + \frac{\Omega}{3}, \Omega \right) \right). \tag{3.7}$$

By a similar calculation as in the proof of the Proposition 2.2, we get

$$\sum_{c \in V_{2p}} \mathcal{E}_1^* \left(\frac{c\Omega}{2p} + \frac{\Omega}{3}, \Omega \right) = \frac{\sqrt{3}}{2} \sum_{c \in V_{2p}} \frac{1}{\wp \left(\frac{c\Omega}{2p} - 1 \right)} + \frac{\#(V_{2p})}{\sqrt{3}}. \tag{3.8}$$

Note that $\mathcal{H}_p = H_p(\sqrt[3]{2})$ and $\sqrt{3}$ is fixed by \mathcal{C} . Thus applying (3.8) to (3.7) gives the lemma. \square

Next, we consider the case of $t = 2^2$. Similar to the case of $t = 2$, we have

$$\frac{L^{(6p)}(C_{2^2}, 1)}{\eta_t \sqrt[3]{p}} \in 3(1 + 3\overline{\mathbb{Z}}_3)$$

and

$$\frac{3}{6p} \text{Tr}_{K(6p)/H_p} \left(\mathcal{E}_1^* \left(\frac{\eta_t \sqrt[3]{p}}{6p}, \eta_t \sqrt[3]{p} \mathcal{O}_K \right) \right) = \frac{3}{4p} \text{Tr}_{\mathcal{H}_p/H_p} \left(\sqrt[3]{2^2} \sum_{c \in V_{2p}} \frac{1}{\wp \left(\frac{c\Omega}{2p} - 1 \right)} \right).$$

We write \mathcal{E} for the sum $\sum_{c \in V_{2p}} \frac{1}{\wp \left(\frac{c\Omega}{2p} - 1 \right)}$. Then we have

$$\frac{L^{(6p)}(C_2, 1)}{\eta_2 \sqrt[3]{p}} + \frac{L^{(6p)}(C_{2p}, 1)}{\eta_2 \sqrt[3]{p}} = \frac{3}{4p} \text{Tr}_{\mathcal{H}_p/H_p} \left(\sqrt[3]{2} \cdot \mathcal{E} \right) \tag{3.9}$$

and

$$\frac{L^{(6p)}(C_{2^2}, 1)}{\eta_{2^2} \sqrt[3]{p}} + \frac{L^{(6p)}(C_{2^2 p^2}, 1)}{\eta_{2^2} \sqrt[3]{p}} = \frac{3}{4p} \text{Tr}_{\mathcal{H}_p/H_p} \left(\sqrt[3]{2^2} \cdot \mathcal{E} \right). \tag{3.10}$$

Given any $\sigma \in \text{Gal}(\mathcal{H}_p/H_p)$, we write $\chi_2(\sigma) = (\sqrt[3]{2})^{\sigma-1}$ and $\chi_2(\sigma)^2 = (\sqrt[3]{2^2})^{\sigma-1}$. Note that these characters take values in μ_3 .

Now, dividing (3.9) by $\sqrt[3]{2}$ and (3.10) by $\sqrt[3]{2^2}$, we get

$$\frac{L^{(6p)}(C_2, 1)}{\Omega_1} + \frac{L^{(6p)}(C_{2p}, 1)}{\Omega_1} = \frac{3}{4p} \sum_{\sigma \in \text{Gal}(\mathcal{H}_p/H_p)} \chi_2(\sigma) \mathcal{E}^\sigma \tag{3.11}$$

and

$$\frac{L^{(6p)}(C_{2^2}, 1)}{\Omega_1} + \frac{L^{(6p)}(C_{2^2 p^2}, 1)}{\Omega_1} = \frac{3}{4p} \sum_{\sigma \in \text{Gal}(\mathcal{H}_p/H_p)} \chi_2(\sigma)^2 \mathcal{E}^\sigma. \tag{3.12}$$

By Lemma 2.6, we know that $\text{ord}_3(3\mathcal{E}^\sigma) = \text{ord}_3((3\mathcal{E})^\sigma) \geq \frac{2}{3}$. Thus (3.11) and (3.12) give

$$\text{ord}_3 \left(\frac{L^{(6p)}(C_{2^2 p^2}, 1)}{\Omega_1} \right) \geq 1, \quad \text{ord}_3 \left(\frac{L^{(6p)}(C_{2p}, 1)}{\Omega_1} \right) \geq 1. \tag{3.13}$$

As we mentioned after (3.4), (3.13) completes the proof Theorem 3.1. Recall that $\sqrt[3]{p} \equiv \sqrt[3]{2} \equiv 2 \pmod{3^{\frac{1}{3}}}$. Thus dividing both sides of (3.11) and (3.12) by 3 and subtracting one from the other, and noting that

$$\text{ord}_3(\chi_2(\sigma) - \chi_2(\sigma)^2) \geq \frac{1}{2} > \frac{1}{3} = \text{ord}_3\left(\wp\left(\frac{c\Omega}{2p}\right) - 1\right),$$

we see that

$$\frac{L(C_{2p}, 1)}{3\Omega_1} - \frac{L(C_{2^2p^2}, 1)}{3\Omega_1} \tag{3.14}$$

has a positive 3-adic valuation. Here, we use the fact that $\chi_2(\sigma) - \chi_2(\sigma)^2$ is fixed by the elements of $\text{Gal}(\mathcal{H}_p/H_p)$ because it takes values in K , and that $\text{ord}_3((\chi_2(\sigma) - \chi_2(\sigma)^2)^{\mathcal{E}^\sigma}) \geq \frac{1}{6}$.

By (3.13), we know that $\frac{L(C_{2p}, 1)}{3\Omega_1}$ and $\frac{L(C_{2^2p^2}, 1)}{3\Omega_1}$ lie in $\overline{\mathbb{Z}}_3$. Recall also that we have $\sqrt[3]{2p} \equiv 1 \pmod{3^{\frac{1}{3}}}$ and that the period relations $\Omega_{2p} = \frac{\Omega_1}{\sqrt[3]{2p}}$ and $\Omega_{2^2p^2} = \frac{\Omega_1}{\sqrt[3]{2^2p^2}}$. Then we know that

$$\frac{L(C_{2p}, 1)}{3\Omega_1} - \frac{L(C_{2p}, 1)}{3\Omega_{2p}} \quad \text{and} \quad \frac{L(C_{2^2p^2}, 1)}{3\Omega_1} - \frac{L(C_{2^2p^2}, 1)}{3\Omega_{2^2p^2}}$$

have positive 3-adic valuations. Now, since $\frac{L(C_{2p}, 1)}{\Omega_{2p}}, \frac{L(C_{2^2p^2}, 1)}{\Omega_{2^2p^2}} \in \mathbb{Q}$, from (3.13) and (3.14), we obtain

$$\frac{L(C_{2p}, 1)}{3\Omega_{2p}} \equiv \frac{L(C_{2^2p^2}, 1)}{3\Omega_{2^2p^2}} \pmod{3}.$$

This congruence combined with the second assertion of (1) in Theorem 3.1 shows that

$$\frac{L(C_{2p}, 1)}{3\Omega_{2p}} \equiv \frac{L(C_{2^2p^2}, 1)}{3\Omega_{2^2p^2}} \equiv 1 \pmod{3}.$$

This completes the proof of Theorem 3.6.

Next, we give a 3-descent result for $C_{2p}, C_{2^2p^2}$ (resp. C_{2p^2}, C_{2^2p}) when $p \equiv 5 \pmod{9}$ (resp. $p \equiv 2 \pmod{9}$).

PROPOSITION 3.11. *Let $C_{2^i p^j} : x^2 + y^2 = 2^i p^j$, where $i, j \in \{1, 2\}$ and $p \equiv 2, 5 \pmod{9}$. Assume in addition that $2^i p^j \equiv \pm 1 \pmod{9}$. Then the 3-part of the Tate-Shafarevich group $\text{III}(C_{2^i p^j})[3]$ of $C_{2^i p^j}$ over \mathbb{Q} is trivial.*

Proof. We write

$$E_n : y^2 z = x^3 - 2^4 3^3 n^2 z^3.$$

This is birationally equivalent to C_n , and over \mathbb{Q} it is 3-isogenous to

$$E'_n : y^2 z = x^3 + 2^4 n^2 z^3.$$

Explicitly, the isogeny $\phi: E_n \rightarrow E'_n$ is given by

$$\phi(x, y, z) = (3^{-2}(x^4 - 2^6 3^3 n^2 x z^3), 3^{-3}y(x^3 + 2^7 3^3 n^2 z^3), x^3 z)$$

and the kernel of ϕ is $\{(0, 1, 0), (0, \pm 2^2(\sqrt{-3})^3 n, 1)\}$.

By assumption, we have $n = 2^i p^j \equiv \pm 1 \pmod 9$. This happens precisely when $n = 2p, 2^2 p^2$ and $p \equiv 5 \pmod 9$ or $n = 2p^2, 2^2 p$ and $p \equiv 2 \pmod 9$. Since n has no prime divisor congruent to 1 modulo 3, hypothesis (H) of [21, Théorème 2.9] clearly holds, and thus (1) of the theorem gives us

$$\text{Sel}_\phi(E_n) = \mathbb{Z}/3\mathbb{Z} \quad \text{and} \quad \text{Sel}_{\hat{\phi}}(E'_n) = 0, \tag{3.15}$$

where $\hat{\phi}$ denotes the dual isogeny of ϕ . Here, $\text{Sel}_f(E)$ denotes the Selmer group of an elliptic curve E over \mathbb{Q} associated to an isogeny f from E to another elliptic curve E' . Recall that we have an exact sequence (see, for example, [22])

$$0 \rightarrow E'_n(\mathbb{Q})/\phi(E_n(\mathbb{Q})) \rightarrow \text{Sel}_\phi(E_n) \rightarrow \text{III}(E_n)[\phi] \rightarrow 0.$$

where $\text{III}(E_n)[\phi]$ denotes the subgroup of elements in $\text{III}(E_n)$ killed by ϕ . Now, we know that $E_n(\mathbb{Q})_{\text{tor}} = 0$, $E'_n(\mathbb{Q})_{\text{tor}} = \{(0, 1, 0), (0, \pm 2^2 D, 1)\} \simeq \mathbb{Z}/3\mathbb{Z}$, thus $\text{III}(E_n)[\phi] = 0$. We also have the following exact sequence (see, for example, [9])

$$0 \rightarrow \text{III}(E_n)[\phi] \rightarrow \text{III}(E_n)[3] \xrightarrow{\phi} \text{III}(E'_n)[\hat{\phi}] = 0,$$

where the last equality is immediate from (3.15). Thus we obtain $\text{III}(E_n)[3]$ is trivial, as required. \square

We end this section by completing the proof the 3-part of the Birch–Swinnerton-Dyer conjecture of the curves appearing in Theorem 1.1 and Corollary 1.2.

Proof of Theorem 1.1 and Corollary 1.2. We will just give the details for the curves C_{2p}, C_{2p^2} under the assumption of $p \equiv 5 \pmod 9$, and the other case is similar. By a theorem of Satgé [20] and the theorem of Gross–Zagier and Kolyvagin, we know that $L(C_{2p^2}, s)$ has a simple zero at $s = 1$, and $C_{2p^2}(\mathbb{Q})$ is of rank one. By Theorem 3.6, we know that $L(C_{2p}, 1)$ does not vanish, so it follows by the theorem of Gross–Zagier and Kolyvagin or Coates–Wiles [5] that $C_{2p}(\mathbb{Q})$ is finite. We also remark that in these cases, the Tate–Shafarevich group of C_{2p} and C_{2p^2} are finite.

From [2], we know that the 3-part Birch–Swinnerton-Dyer conjecture holds for the product curve $C_{2p} \times C_{2p^2}$. Thus

$$\begin{aligned} & \text{ord}_3 \left(\frac{L(C_{2p}, 1)L'(C_{2p^2}, 1)}{\Omega_{2p}\Omega_{2p^2} \cdot \hat{h}(P)} \right) \\ &= \text{ord}_3 (T(C_{2p})T(C_{2p^2}) \cdot \#(\text{III}(C_{2p}))\#(\text{III}(C_{2p^2}))) \end{aligned} \tag{3.16}$$

where $T(C_{2p}) = \prod_{\ell|6p} m_\ell(C_{2p})$ and $T(C_{2p^2}) = \prod_{\ell|6p} m_\ell(C_{2p^2})$ are the products of local Tamagawa numbers of C_{2p} and C_{2p^2} , respectively. Here, $m_\ell(C_n)$

denotes the local Tamagawa number of C_n at the prime ℓ . Since $C_{2p^2}(\mathbb{Q})$ is of rank one, we let P be a generator of the free part of $C_{2p^2}(\mathbb{Q})$, and denote by $\widehat{h}(P)$ the Néron–Tate height of P . Note that the local Tamagawa numbers of C_{2p} and C_{2p^2} are all equal to 1 except that $\ell = 3$, where $m_3(C_{2p}) = 3$ (see [25]). By Theorem 3.6 and Proposition 3.11, the 3-part of the Birch–Swinnerton-Dyer conjecture holds for the curve C_{2p} . Thus

$$\text{ord}_3 \left(\frac{L(C_{2p}, 1)}{\Omega_{2p}} \right) = \text{ord}_3 (T(C_{2p}) \cdot \#(\text{III}(C_{2p}))). \tag{3.17}$$

Now the 3-part of the Birch–Swinnerton-Dyer conjecture for C_{2p^2} follows from (3.16) and (3.17), and Corollary 1.2 follows as a consequence. \square

4 SOME RELATIONS BETWEEN THE 2-SELMER GROUP OF C_{2p^j} AND THE 2-CLASS GROUP OF $\mathbb{Q}(\sqrt[3]{p})$

The aim of this section is to give a proof of Theorem 1.3. Given $j \in \{1, 2\}$, the curve C_{2p^j} is a twist of C_2 by the cubic extension $\mathbb{Q}(\sqrt[3]{p^j})/\mathbb{Q}$ of discriminant prime to 2. Since a global minimal Weierstrass model of C_2 is given by $y^2 = x^3 - 27$, we know that

$$y^2 = x^3 - 27p^{2j} \quad (j = 1, 2) \tag{4.1}$$

gives a minimal model of C_{2p^j} at 2.

In the remainder of this section, we write E for C_{2p^j} for simplicity, and we work with the equation given in (4.1). We will study the relation between the 2-class group of $L = \mathbb{Q}(\sqrt[3]{p})$ and the 2-Selmer group $\text{Sel}_2(E)$. It is well known that the torsion part $E(\mathbb{Q})_{\text{tor}}$ of $E(\mathbb{Q})$ is trivial, and we identify

$$\frac{\mathbb{Q}[x]}{(x^3 - 27p^2)} = \frac{\mathbb{Q}[x]}{(x^3 - p^2)} = \frac{\mathbb{Q}[x]}{(x^3 - p)} = \frac{\mathbb{Q}[x]}{(x^3 - 27p^4)}$$

with L . To see where these fields come from, one may look at the classical proof of the weak Mordell–Weil theorem in the case $E(\mathbb{Q})[2] = 0$ (see, for example, [4, 22]). The proof of the following lemma can be found in [11].

LEMMA 4.1. *Let $\text{Res}_{L/\mathbb{Q}}\mu_2$ be the restriction of scalars of μ_2 from L to \mathbb{Q} , treated as a $G_{\mathbb{Q}}$ -module. Then we have the exact sequence*

$$0 \rightarrow E[2] \rightarrow \text{Res}_{L/\mathbb{Q}}\mu_2 \xrightarrow{\mathbb{N}} \mu_2 \rightarrow 0,$$

where all of the terms in the exact sequence are considered as $\overline{\mathbb{Q}}$ -points, and \mathbb{N} denotes the multiplication of the three components of $\text{Res}_{L/\mathbb{Q}}\mu_2$. Moreover, we have an isomorphism

$$H^1(\mathbb{Q}, E[2]) \simeq (L^\times / (L^\times)^2) \square \tag{4.2}$$

where

$$(L^\times/(L^\times)^2)_\square := \{\alpha \in L^\times/(L^\times)^2 : N(\alpha) \in (\mathbb{Q}^\times)^2\}$$

and N is the norm map from L to \mathbb{Q} .

We denote by δ the morphism which is the composition of the Kummer map

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

with the isomorphism in (4.2), which we still call the global Kummer map. Then we have the following description of δ (for a detailed proof, see [11]):

LEMMA 4.2. *The map δ is given by*

$$\delta: E(\mathbb{Q})/2E(\mathbb{Q}) \rightarrow (L^\times/(L^\times)^2)_\square, \quad P \mapsto x(P) - \beta,$$

where $x(P)$ is the x -coordinate of P and β is the image of x in $L = \mathbb{Q}[x]/(x^3 - 27p^{2j})$.

We remark that the above description of the map δ dates back to the proof of the Mordell–Weil theorem when $E(\mathbb{Q})[2] = 0$. See the book of Cassels [4] for more details. Similarly, we can state Lemmas 4.1 and 4.2 over \mathbb{Q}_q for all primes q , finite or infinite. We put $L_q = L \otimes_{\mathbb{Q}} \mathbb{Q}_q$. Then we obtain the local Kummer map δ_q , which is the composition of the Kummer map

$$E(\mathbb{Q}_q)/2E(\mathbb{Q}_q) \rightarrow H^1(\mathbb{Q}_q, E[2])$$

with the isomorphism

$$H^1(\mathbb{Q}_q, E[2]) \simeq (L_q^\times/(L_q^\times)^2)_\square,$$

where

$$(L_q^\times/(L_q^\times)^2)_\square := \{x \in L_q^\times/(L_q^\times)^2 : N(x) \in (\mathbb{Q}_q^\times)^2\}$$

and N is the norm map from L_q to \mathbb{Q}_q .

LEMMA 4.3. *The map δ_q is given by*

$$\delta_q: E(\mathbb{Q}_q)/2E(\mathbb{Q}_q) \rightarrow (L_q^\times/(L_q^\times)^2)_\square, \quad P \mapsto x(P) - \beta,$$

where β is the image of x in $L_q = \mathbb{Q}_q[x]/(x^3 - 27p^{2j})$.

To obtain a precise description of the Selmer group $\text{Sel}_2(E)$, we need to describe the image of all δ_q . We denote by \mathfrak{D} the ring of integers $\mathbb{Z}[x]/(x^3 - 27p^{2j})$ of L , and we set $\mathfrak{D}_q = \mathfrak{D} \otimes_{\mathbb{Z}} \mathbb{Z}_q$.

LEMMA 4.4. *For any prime q and for any $P \in E(\mathbb{Q}_q)$, we have*

$$\delta_q(P) \in (\mathfrak{D}_q^\times/(\mathfrak{D}_q^\times)^2)_\square$$

where $(\mathfrak{D}_q^\times/(\mathfrak{D}_q^\times)^2)_\square$ again denotes a subset of $\mathfrak{D}_q^\times/(\mathfrak{D}_q^\times)^2$ consisting of square norms.

Proof. For $q \neq 2$, this is Lemma 6 of [8]. Here, we note that since the Kodaira type of E at each prime ℓ is IV or IV*, $\Phi[2]$ is trivial, where $\Phi = \tilde{\mathcal{E}}(\overline{\mathbb{F}}_\ell)/\tilde{\mathcal{E}}^0(\overline{\mathbb{F}}_\ell)$ denotes the component group scheme of the Néron model \mathcal{E} of E over \mathbb{Q}_ℓ , and we thank the referee for pointing this out. Here, \sim denotes reduction modulo ℓ and $\tilde{\mathcal{E}}^0$ denotes the identity component. For $q = 2$, we just need to show $\text{ord}_2(x(P) - \beta)$ is even, where ord_2 denotes the normalized 2-adic valuation with $\text{ord}_2(2) = 1$. Note that

$$x^3 - 27p^{2j} \equiv (x + 1)(x^2 + x + 1) \pmod{2}. \tag{4.3}$$

We write also $3\sqrt[3]{p^{2j}}$ for the unique root in \mathbb{Z}_2 of $x^3 - 27p^{2j} = 0$ satisfying $3\sqrt[3]{p^{2j}} \equiv 1 \pmod{2}$ obtained by Hensel's lemma. Thus we have a factorisation

$$x^3 - 27p^{2j} = (x - 3\sqrt[3]{p^{2j}})(x^2 + 3\sqrt[3]{p^{2j}}x + (3\sqrt[3]{p^{2j}})^2)$$

over \mathbb{Z}_2 . Now, we have

$$2\text{ord}_2(y) = \text{ord}_2(x - 3\sqrt[3]{p^{2j}}) + \text{ord}_2(x^2 + 3\sqrt[3]{p^{2j}}x + (3\sqrt[3]{p^{2j}})^2)$$

for $x = x(P)$ and $y = y(P)$ in \mathbb{Q}_2 , so we know that the right hand side is even. If $\text{ord}_2(x) < 0$, then $\text{ord}_2(x - 3\sqrt[3]{p^{2j}}) = \text{ord}_2(x)$ and $\text{ord}_2(x^2 + 3\sqrt[3]{p^{2j}}x + (3\sqrt[3]{p^{2j}})^2) = 2\text{ord}_2(x)$, so it follows that $3\text{ord}_3(x)$ is even, and thus $\text{ord}_2(x)$ is even. If $\text{ord}_2(x) \geq 0$, noting that $x^2 + x + 1 \not\equiv 0 \pmod{2}$ in (4.3), we see that $2\text{ord}_2(y) = \text{ord}_2(x - 3\sqrt[3]{p^{2j}})$, and thus $\text{ord}_2(x - 3\sqrt[3]{p^{2j}})$ is even, as required. \square

Now, we can describe the image of δ_q .

LEMMA 4.5.

1. The image of δ_∞ is trivial.
2. If $q \neq 2, \infty$, we have

$$\text{im}(\delta_q) = (\mathfrak{O}_q^\times / (\mathfrak{O}_q^\times)^2)_\square.$$

3. The image of δ_2 is a subgroup of $(\mathfrak{O}_2^\times / (\mathfrak{O}_2^\times)^2)_\square$ of index 2, and contains the subgroup of elements in $(\mathfrak{O}_2^\times / (\mathfrak{O}_2^\times)^2)_\square$ which are congruent to 1 modulo 4.

Proof. Note that $L_\infty = \mathbb{C} \times \mathbb{R}$ and we know that $(L_\infty^\times / (L_\infty^\times)^2)_\square = 1$, thus $\text{im}(\delta_\infty)$ is trivial and (1) follows.

For (2) and (3), we know that the norm of L_q^\times in \mathbb{Q}_q^\times has index 3 by local class field theory. Thus, in the commutative diagram

$$\begin{array}{ccccccc} 0 & \longrightarrow & (\mathfrak{O}_q^\times)^2 & \longrightarrow & \mathfrak{O}_q^\times & \longrightarrow & \mathfrak{O}_q^\times / (\mathfrak{O}_q^\times)^2 \longrightarrow 0 \\ & & \downarrow & & \downarrow N & & \downarrow \lambda \\ 0 & \longrightarrow & (\mathbb{Z}_q^\times)^2 & \longrightarrow & \mathbb{Z}_q^\times & \longrightarrow & \mathbb{Z}_q^\times / (\mathbb{Z}_q^\times)^2 \longrightarrow 0 \end{array}$$

where N is the restriction of the norm map from L_q to \mathbb{Q}_q , we see that λ is surjective. Furthermore, from the exact sequence

$$0 \rightarrow (\mathfrak{D}_q^\times / (\mathfrak{D}_q^\times)^2)_\square \rightarrow \mathfrak{D}_q^\times / (\mathfrak{D}_q^\times)^2 \xrightarrow{\lambda} \mathbb{Z}_q^\times / (\mathbb{Z}_q^\times)^2 \rightarrow 0,$$

we obtain

$$\#(\mathfrak{D}_q^\times / (\mathfrak{D}_q^\times)^2)_\square = \frac{\#(\mathfrak{D}_q^\times / (\mathfrak{D}_q^\times)^2)}{\#(\mathbb{Z}_q^\times / (\mathbb{Z}_q^\times)^2)}.$$

Note that $\#(\mathbb{Z}_q^\times / (\mathbb{Z}_q^\times)^2) = 2$ or 2^2 according as $q \neq 2$ or $q = 2$. Suppose $x^3 - 27p^{2j}$ is a product of ℓ irreducible polynomials modulo q . For $q \neq 2$, we have $\#(\mathfrak{D}_q^\times / (\mathfrak{D}_q^\times)^2) = 2^\ell$. For $q = 2$, note that we have $\mathfrak{D}_2^\times = \mathbb{Z}_2^\times \times \mathbb{Z}_2[\gamma]^\times$ where γ is a root of the irreducible polynomial $x^2 + 3\sqrt[3]{p^{2j}}x + (3\sqrt[3]{p^{2j}})^2 \in \mathbb{Z}_2[x]$ from the proof of Lemma 4.4. Note also that $(1 + 2\mathbb{Z}_2[\gamma])^2$ is a subgroup of $1 + 4\mathbb{Z}_2[\gamma]$ of index 2. Thus we have $\#(\mathfrak{D}_2^\times / (\mathfrak{D}_2^\times)^2) = 2^{2+3} = 2^5$. It follows that $\#(\mathfrak{D}_q^\times / (\mathfrak{D}_q^\times)^2)_\square = 2^{\ell-1}$ or 2^3 according as $q \neq 2$ or $q = 2$. On the other hand, a direct computation shows that

$$\#(E(\mathbb{Q}_q)[2]) = 2^{\ell-1}.$$

Furthermore, since $E(\mathbb{Q}_q)$ has a subgroup isomorphic to \mathbb{Z}_q of finite index, we have $\#(E(\mathbb{Q}_q)/2E(\mathbb{Q}_q)) = \#(E(\mathbb{Q}_q)[2]) = 2^{\ell-1}$ or $2 \cdot \#E(\mathbb{Q}_q)[2] = 2^2$ according as $q \neq 2$ or $q = 2$. Therefore (2) follows, and it remains to show that $\text{im}(\delta_2)$ contains the subgroup $(1 + 4\mathfrak{D}_2 / (\mathfrak{D}_2^\times)^2)_\square = (1 + 4\mathbb{Z}_2[\gamma] / (\mathbb{Z}_2[\gamma]^\times)^2)$ of order 2. Let \widehat{E} be the formal group of E over \mathbb{Z}_2 given by (4.1). Let $P \in \widehat{E}(2\mathbb{Z}_2)$, and write $t = -\frac{x}{y}$ for the uniformizer of \widehat{E} . Then we have

$$x(P) = t^{-2} + O(t^2)$$

since $a_1 = a_2 = a_3 = 0$. Then

$$\delta_2(P) = x(P) - \beta = t^{-2} - \beta + O(t^2) \equiv 1 - \beta t^2 \pmod{(L_2^\times)^2},$$

where the last equality is obtained by noting that $t \in 2\mathbb{Z}_2$ and that the units in \mathfrak{D}_2 congruent to 1 modulo 16 lie in $(\mathfrak{D}_2^\times)^2$. Now, take $P \in \widehat{E}(2\mathbb{Z}_2)$ corresponding to $t = 2u \in 2\mathbb{Z}_2 \setminus 4\mathbb{Z}_2$. Then $\delta_2(P) \equiv 1 - 4\gamma u^2$ clearly lies in the non-trivial class of $(1 + 4\mathbb{Z}_2[\gamma] / (\mathbb{Z}_2[\gamma]^\times)^2)$. This concludes the proof of Lemma 4.5. \square

We can now state a relation between the 2-Selmer group $\text{Sel}_2(E)$ of E and the 2-class group of $L = \mathbb{Q}(\sqrt[3]{p})$. Write $\epsilon(E/\mathbb{Q})$ for the global root number of E/\mathbb{Q} . Recall from the introduction that $\text{rank}_2(Cl(F)) := \dim_{\mathbb{F}_2}(Cl(F)/2Cl(F))$ denotes the 2-rank of $Cl(F)$.

PROPOSITION 4.6. *Let $k = \text{rank}_2(Cl(L))$. Then*

$$\dim_{\mathbb{F}_2} \text{Sel}_2(E) = \begin{cases} k & \text{if } \epsilon(E/\mathbb{Q}) = (-1)^k, \\ k + 1 & \text{if } \epsilon(E/\mathbb{Q}) = (-1)^{k+1}. \end{cases}$$

Proof. Since we may follow the methods in [11], we will only state the key ideas in the argument. We define two subgroups

$$N_1 = \{\alpha \in L^\times / (L^\times)^2 : L(\sqrt{\alpha})/L \text{ is unramified}\}$$

and

$$N_2 = \{\alpha \in L^\times / (L^\times)^2 : \alpha > 0, (\alpha) = I^2, I \subset L \text{ is a fractional ideal}\}$$

of $(L^\times / (L^\times)^2)_\square$. Then from the description of the local Kummer map given in (4.5), we see that the 2-Selmer group $\text{Sel}_2(E)$ satisfies

$$N_1 \subseteq \text{Sel}_2(E) \subseteq N_2.$$

Furthermore, by Kummer theory, we have

$$N_1 \simeq \text{Hom}(\text{Gal}(M/L), \mu_2)$$

where M is the maximal abelian extension of exponent two unramified everywhere, so that $\text{Gal}(M/L) = Cl(L)[2]$. Note that $\#(Cl(L)[2]) = \#(Cl(L)/2Cl(L))$, since $Cl(L)$ is a finite group. Thus we have

$$\#(N_1) = 2^k \text{ where } \dim_{\mathbb{F}_2} Cl(L)[2] = k.$$

By Dirichlet’s unit theorem, the free part of the group \mathcal{O}_L^\times of units in L has rank one. Let u_L be a generator. By choosing $-u_L$ or u_L , we may assume $u_L > 0$, and by choosing u_L or u_L^{-1} , we may assume $u_L > 1$. Now, we define a map

$$N_2 \rightarrow Cl(L)[2] \quad \alpha \mapsto [I]$$

where I is a fractional ideal of L such that $I^2 = (\alpha)$ and $[I]$ denotes its ideal class in $Cl(L)$. This map is surjective, and the kernel of this map is given by $u_L^{\mathbb{Z}}/u_L^{2\mathbb{Z}} \simeq \mathbb{Z}/2\mathbb{Z}$. Hence we have

$$\dim_{\mathbb{F}_2} N_2 = k + 1.$$

From all of the above considerations and the 2-parity conjecture proved in [13], we obtain the assertion of Proposition 4.6. This also concludes the proof of Theorem 1.3. □

A NUMERICAL EXAMPLES

Let $p \equiv 2, 5 \pmod 9$ be an odd prime number. Let $L = \mathbb{Q}(\sqrt[3]{p})$, and write $Cl(L)$ for the ideal class group of L . We ran a numerical test for primes $p < 1000000$, and obtained that 1629 out of 13068 primes $p \equiv 5 \pmod 9$, and 1852 out of 13099 primes $p \equiv 2 \pmod 9$ satisfy condition

$$\text{rank}_2(Cl(L)) = \dim_{\mathbb{F}_2} (Cl(L)/2Cl(L)) \geq 2 \tag{A.1}$$

from Theorem 1.3. The following lists are small hand-picked samples of primes p such that $Cl(L)$ satisfies (A.1), including all the cases when the Tate–Shafarevich group of C_{2p} (resp. C_{2p^2}) is strictly bigger than $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ for $p \equiv 5 \pmod{9}$ (resp. $p \equiv 2 \pmod{9}$) and $p < 1000000$. All the numerical results were obtained using the computer algebra packages *Magma* [1] and *PARI/GP* [14].

$p \equiv 5 \pmod{9}$	$Cl(L)$	$\text{III}(C_{2p})[2]$
113	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$
3209	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/68\mathbb{Z}$	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$
9941	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$
15053	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/14\mathbb{Z}$	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$
17573	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/374\mathbb{Z}$	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$
18257	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/170\mathbb{Z}$	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$
24197	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/20\mathbb{Z}$	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$
32009	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/16\mathbb{Z}$	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$
35969	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/140\mathbb{Z}$	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$
40577	$\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/28\mathbb{Z}$	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$
41981	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/26\mathbb{Z}$	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$
46229	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$
54869	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/1190\mathbb{Z}$	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$
61169	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/50\mathbb{Z}$	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$
61547	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/314\mathbb{Z}$	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$
73013	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$
81077	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$
97943	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/10\mathbb{Z}$	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$
166667	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/14\mathbb{Z}$	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$
169007	$\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/124\mathbb{Z}$	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$
195581	$\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/184\mathbb{Z}$	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$
206489	$\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/20\mathbb{Z}$	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$
483017	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$
635909	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$
805073	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$
964589	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$

$p \equiv 2 \pmod{9}$	$Cl(L)$	$\text{III}(C_{2p^2})[2]$
443	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$
857	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/28\mathbb{Z}$	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$
4799	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/20\mathbb{Z}$	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$
5987	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/64\mathbb{Z}$	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$
9011	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$
9749	$\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/16\mathbb{Z}$	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$
13043	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$
17579	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/230\mathbb{Z}$	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$
26111	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/52\mathbb{Z}$	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$
31547	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/50\mathbb{Z}$	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$
36263	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/70\mathbb{Z}$	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$
47387	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$
58727	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/32\mathbb{Z}$	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$
60149	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/74\mathbb{Z}$	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$
65063	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$
78437	$\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$
79967	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/40\mathbb{Z}$	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$
96329	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/22\mathbb{Z}$	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$
99371	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$
125003	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/700\mathbb{Z}$	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$
167087	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/656\mathbb{Z}$	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$
266663	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$
402131	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$
424163	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$
521831	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$
916103	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$

ACKNOWLEDGEMENT

The authors would like to thank John Coates for his comments on this work. The second author would like to thank Ye Tian for the suggestion given during his PhD to study the Birch–Swinnerton-Dyer conjecture for the individual curves in the product of curves. Finally, the authors are very grateful to the referee whose valuable comments lead to an improvement of the quality of this paper.

The first author is supported by the SFB 1085 “Higher invariants” at the University of Regensburg, funded by the Deutsche Forschungsgemeinschaft (DFG), the second author is supported by NSFC-11901332.

REFERENCES

- [1] W. Bosma, J. Cannon, C. Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. 24 (1997), 235–265.
- [2] L. Cai, J. Shu, Y. Tian, *Cube sum problem and an explicit Gross–Zagier formula*, Amer. J. Math. 139 (2017), no. 3, 785–816.
- [3] J. Cassels, *Arithmetic on curves of genus 1. IV. Proof of the Hauptvermutung*, J. Reine Angew. Math. 211 (1962), 95–112.
- [4] J. Cassels, *Lectures on elliptic curves*, London Mathematical Society Student Texts, 24. Cambridge University Press, Cambridge, 1991. vi+137 pp. ISBN 0-521-41517-9; 0-521-42530-1.
- [5] J. Coates, A. Wiles, *On the conjecture of Birch and Swinnerton-Dyer*, Invent. Math. 39 (1977), 223–251.
- [6] J. Coates, *Lectures on the Birch–Swinnerton-Dyer conjecture*, ICCM Not. 1 (2013), no. 2, 29–46.
- [7] J. Coates, Y. Li, *Non-vanishing theorems for central L-values of some elliptic curves with complex multiplication*, Proc. Lond. Math. Soc. (3) 121 (2020), no. 6, 1531–1578.
- [8] B. Gross, J. Parson, *On the local divisibility of Heegner points*, Number Theory, Analysis and Geometry, 215–241, Springer, New York, 2012.
- [9] Y. Hu, H. Yin, J. Shu, *An explicit Gross-Zagier formula related to the Sylvester conjecture*, Trans. Amer. Math. Soc. 372 (2019), no. 10, 6905–6925.
- [10] Y. Kezuka, *On the p-part of the Birch–Swinnerton-Dyer conjecture for elliptic curves with complex multiplication by the ring of integers of $\mathbb{Q}(\sqrt{-3})$* , Math. Proc. Cambridge Philos. Soc. 164 (2018), no. 1, 67–98.

- [11] C. Li, *2-Selmer groups, 2-class groups and rational points on elliptic curves*, Trans. Amer. Math. Soc. 371 (2019), no. 7, 4631–4653.
- [12] E. Liverance, *A formula for the root number of a family of elliptic curves*, J. Number Theory 51 (1995), no. 2, 288–305.
- [13] P. Monsky, *Generalizing the Birch-Stephens theorem. I. Modular curves*, Math. Z. 221 (1996), no. 3, 415–420.
- [14] The PARI Group, PARI/GP version 2.11.1, Univ. Bordeaux, 2018, <http://pari.math.u-bordeaux.fr/>.
- [15] D. Qiu, X. Zhang, *Elliptic curves with CM by $\sqrt{-3}$ and 3-adic valuations of their L-series*, Manuscripta Math. 108 (2002), no. 3, 385–397.
- [16] M. Razar, *The non-vanishing of $L(1)$ for certain elliptic curves with no first descents*, Amer. J. Math. 96 (1974), 104–126.
- [17] M. Razar, *A relation between the two-component of the Tate-Shafarevich group and $L(1)$ for certain elliptic curves*, Amer. J. Math. 96 (1974), 127–144.
- [18] K. Rubin, *Tate-Shafarevich groups and L-functions of elliptic curves with complex multiplication*, Invent. Math. 89 (1987), no. 3, 527–559.
- [19] K. Rubin, *The “main conjectures” of Iwasawa theory for imaginary quadratic fields*, Invent. Math. 103 (1991), no. 1, 25–68.
- [20] P. Satgé, *Un analogue du calcul de Heegner*, Invent. Math. 87 (1987), no. 2, 425–439.
- [21] P. Satgé, *Groupes de Selmer et corps cubiques*, J. Number Theory 23 (1986), no. 3, 294–317.
- [22] J. 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.
- [23] J. Silverman, *Advanced topics in the arithmetic of elliptic curves*, Graduate Texts in Mathematics, 151. Springer-Verlag, New York, 1994. xiv+525 pp. ISBN 0-387-94328-5.
- [24] N. Stephens, *The diophantine equation $X^3+Y^3 = DZ^3$ and the conjectures of Birch and Swinnerton-Dyer*, J. Reine Angew. Math. 231 (1968), 121–162.
- [25] D. Zagier, G. Kramarz, *Numerical investigations related to the L-series of certain elliptic curves*, J. Indian Math. Soc. (N.S.) 52 (1987), 51–69 (1988).

- [26] C. Zhao, *A criterion for elliptic curves with second lowest 2-power in $L(1)$* , Math. Proc. Cambridge Philos. Soc. 131 (2001), no. 3, 385–404.
- [27] S. Zhang, *The nonvanishing of $L(1)$ for the L -series of some elliptic curves*, Adv. in Math. (China) 24 (1995), no. 5, 439–443.

Yukako Kezuka
Fakultät für Mathematik
Universität Regensburg
93049 Regensburg
Germany
yukako.kezuka@ur.de

Yongxiong Li
Yau Mathematical Sciences Center
Tsinghua University
Beijing
China
liyx_1029@tsinghua.edu.cn

