ON THE QUADRATIC TWIST OF ELLIPTIC CURVES WITH FULL 2-TORSION

ZHANGJIE WANG AND SHENXING ZHANG

Contents

Abstract. Let $E : y^2 = x(x - a^2)(x + b^2)$ be an elliptic curve with full 2-torsion group, where a and b are coprime integers and $2(a^2 + b^2)$ is a square. Assume that the 2-Selmer group of E has rank two. We characterize all quadratic twists of E with Mordell-Weil rank zero and 2-primary Shafarevich-Tate groups $(\mathbb{Z}/2\mathbb{Z})^2$, under certain conditions. We also obtain a distribution result of these elliptic curves.

1. Introduction

A positive integer n is called *a congruent number* if and only if it is the area of a right rational triangle. This is equivalently to say, the congruent elliptic curve $y^2 = x^3 - n^2 x$ has positive Mordell-Weil rank. The classical descent method provides a way to construct non-congruent numbers, see [Fen96, LT00, OZ14, OZ15]. In

Date: April 24, 2026.
2020 *Mathematics Subject Classification.* Primary 11G05; Secondary 11R11, 11R29, 11N99.
Key words and phrases. Shafarevich-Tate groups; full 2-torsion; Cassels pairing; Gauss genus theory; equidistribution property; residue symbols.

[Wan16], the first author used Cassels pairing to characterize all congruent elliptic curves $y^2 = x^3 - n^2 x$ with Mordell-Weil rank zero and second minimal 2-primary Shafarevich-Tate group, where all prime divisors of n are congruent to 1 modulo 4.

Fujiwara in [Fuj98] defined the generalized concept, a θ-congruent number by considering rational triangles with an angle θ. For such a triangle, $\cos\theta = s/r$ is a rational number, $s, r \in \mathbb{Z}, r > 0, \gcd(r, s) = 1$. A positive integer n is called *θ-congruent* if $n\sqrt{r^2 - s^2}$ is the area of a rational triangle with an angle θ. This is equivalently to say, the elliptic curve

$$y^2 = x(x + (r+s)n)(x - (r-s)n)$$

has positive Mordell-Weil rank. The goal of this paper is to generalize the result in [Wan16] to non-θ-congruent case. More precisely, we will show that for certain n, n is non-congruent with second minimal 2-primary Shafarevich-Tate group, if and only if n is non-θ-congruent with second minimal 2-primary Shafarevich-Tate group, where both of $\sqrt{2}\sin(\theta/2)$ and $\sqrt{2}\cos(\theta/2)$ are rational.

Let (a, b, c) be a primitive triple of positive integers such that $a^2 + b^2 = 2c^2$. By elementary number theory, this is equivalent to say,

$$a = |\alpha^2 - 2\alpha\beta - \beta^2|, \quad b = |\alpha^2 + 2\alpha\beta - \beta^2|, \quad c = \alpha^2 + \beta^2$$

for some coprime integers α, β with different parities. Denote by

$$E : y^2 = x(x - a^2)(x + b^2)$$

an elliptic curve with full 2-torsion group, and

$$E^{(n)} : y^2 = x(x - a^2 n)(x + b^2 n)$$

a quadratic twist of E, where n is a positive square-free integer. If

$$\sin\left(\frac{\theta}{2}\right) = \frac{a}{\sqrt{2}c}, \quad \cos\left(\frac{\theta}{2}\right) = \frac{b}{\sqrt{2}c} \quad \text{and} \quad \tan\left(\frac{\theta}{2}\right) = \frac{a}{b},$$

then $\cos\theta = \frac{b^2 - a^2}{b^2 + a^2}$. Therefore, n is non-θ-congruent if and only if $\operatorname{rank}_{\mathbb{Z}} E^{(n)} = 0$.

1.1. **Rank zero twists.** When $n > 1$, denote by $\mathcal{A}$ the ideal class group of $K = \mathbb{Q}(\sqrt{-n})$ and

$$h_{2^m}(n) := \dim_{\mathbb{F}_2} \mathcal{A}^{2^{m-1}}/\mathcal{A}^{2^m}$$

its 2^m-rank for a positive integer m. Denote by $\operatorname{Sel}_2\big(E^{(n)}/\mathbb{Q}\big)$ the 2-Selmer group of $E^{(n)}$ over $\mathbb{Q}$.

Theorem 1.1 (=Theorems 4.2 and 4.4)**.** *Assume that* $\operatorname{Sel}_2(E/\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^2$. *Let* $n \equiv 1 \bmod 8$ *be a positive square-free integer coprime to abc where each prime factor of n is a quadratic residue modulo every prime factor of abc.*

(A) *If all prime factors of n are congruent to* ± 1 *modulo* 8*, then the following are equivalent:*

(1) $\operatorname{rank}_{\mathbb{Z}} E^{(n)}(\mathbb{Q}) = 0$ *and* $\text{Ш}(E^{(n)}/\mathbb{Q})[2^\infty] \cong (\mathbb{Z}/2\mathbb{Z})^2$*;*
(2) $h_4(n) = 1$ *and* $h_8(n) = 0$*.*

(B) *If all prime factors of n are congruent to* 1 *modulo* 4*, then the following are equivalent:*

(1) $\operatorname{rank}_{\mathbb{Z}} E^{(n)}(\mathbb{Q}) = 0$ *and* $\text{Ш}(E^{(n)}/\mathbb{Q})[2^\infty] \cong (\mathbb{Z}/2\mathbb{Z})^2$*;*
(2) $h_4(n) = 1$ *and* $h_8(n) \equiv \frac{d-1}{4} \bmod 2$*.*

Here d is the odd part of $d_0 \mid 2n$ such that the ideal class $[(d_0, \sqrt{-n})]$ is the non-trivial element in $\mathcal{A}[2] \cap \mathcal{A}^2$.

Remark 1.2. (1) When $(a, b) = (1, 1), (7, 23), (23, 47), (119, 167), (167, 223), (287, 359)$, we have $\mathrm{Sel}_2(E/\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^2$.

(2) In Theorem 1.1(B), if $h_4(n) = 1$, then the non-trivial element in $\mathcal{A}[2] \cap \mathcal{A}^2$ is $[(d_0, \sqrt{-n})]$ for some positive divisor d_0 of $2n$. If d_0' is another positive divisor of $2n$ such that $[(d_0, \sqrt{-n})] = [(d_0', \sqrt{-n})]$, then $d_0 d_0' = n$ or $4n$. See §2.1.

We will first show that $E^{(n)}_{\mathrm{tor}}(\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^2$ in §2.2. In §3, we will study the local solvability of homogeneous spaces and then express the 2-Selmer group as the kernel of the generalized Monsky matrix $\mathcal{M}_n$. Then we will give the proof of Theorem 1.1 in §4. The strategy is similar to [Wan16].

1.2. **Distribution.** We will also study the distribution of n satisfying the equivalent condition in Theorem 1.1(B), which generalizes the result in [Wan17]. Denote by

- $C_k(x)$ the set of positive square-free integers $n \leqslant x$ with exactly k prime factors;
- $\mathscr{Q}_k(x)$ the set of $n \in C_k(x)$ coprime to abc such that each prime factor of $n \equiv 1 \bmod 8$ is a quadratic residue modulo every prime factor of abc and congruent to 1 modulo 4;
- $\mathscr{P}_k(x)$ the set of all $n \in \mathscr{Q}_k(x)$ such that Theorem 1.1(B)(2) holds.

We will use the standard symbols in analytic number theory: "$\sim, \ll, O(\cdot), o(\cdot), \mathrm{Li}(x)$", which can be found in [IR90]. It's a classical result, due to Landau in [Lan18, Kapitel XIII, § 56], that

$$\#C_k(x) \sim \frac{x(\log\log x)^{k-1}}{(k-1)!\log x}. \tag{1.1}$$

Theorem 1.3. *Assume that* $\mathrm{Sel}_2(E/\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^2$. *Then*

$$\#\mathscr{P}_k(x) \sim 2^{-k\ell-k-2}\left(u_k + (2^{-1} - 2^{-k})u_{k-1}\right) \cdot \#C_k(x),$$

where ℓ is the number of different prime factors of abc and

$$u_k := \prod_{1 \leqslant i \leqslant k/2} (1 - 2^{1-2i}).$$

We will use the method in [CO89] to show the equidistribution property of residue symbols in § 5.3 and then use this to prove Theorem 1.3 in § 6.

Remark 1.4. If one wants to study the distribution of n satisfying the equivalent condition in Theorem 1.1(A), one needs a characterization of $h_8(n)$ in terms of residue symbols similar to [JY11].

1.3. **Notations.**

- $n = p_1 \cdots p_k$ the prime decomposition of n.
- $abc = q_1^{t_1} \cdots q_\ell^{t_\ell}$ the prime decomposition of abc.
- $\gcd(m_1, \ldots, m_t)$ the greatest common divisor of integers $m_1, \ldots, m_t$.
- $\mathrm{Sel}_2'(E^{(n)}) = \mathrm{Sel}_2(E^{(n)})/E^{(n)}(\mathbb{Q})[2]$ the pure 2-Selmer group of $E^{(n)}$, see (2.4).
- D_Λ the homogeneous space associated to a rational triple (d_1, d_2, d_3), see (2.2).
- $(\alpha, \beta)_v$ the Hilbert symbol, $\alpha, \beta \in \mathbb{Q}_v^\times$.

- $[\alpha,\beta]_v$ the additive Hilbert symbol, i.e., the image of $(\alpha,\beta)_v$ under the isomorphism $\{\pm 1\} \xrightarrow{\sim} \mathbb{F}_2$.
- $\left(\frac{\alpha}{\beta}\right) = \prod_{p\mid\beta}(\alpha,\beta)_p$ the Jacobi symbol with $p \mid \beta$ counted with multiplicity, where $\gcd(\alpha,\beta)=1$ and $\beta>0$.
- $\left[\frac{\alpha}{\beta}\right]$ the additive Jacobi symbol, i.e., the image of $\left(\frac{\alpha}{\beta}\right)$ under the isomorphism $\{\pm 1\} \xrightarrow{\sim} \mathbb{F}_2$.
- $\mathcal{D}(K)$ the set of positive square-free divisors of $2n$.
- $\mathbf{0} = (0,\dots,0)^{\mathrm{T}}$ and $\mathbf{1} = (1,\dots,1)^{\mathrm{T}}$.
- $\mathbf{I}$ the identity matrix and $\mathbf{O}$ the zero matrix.
- $\mathbf{A} = \mathbf{A}_n$ a matrix associated to n, see (3.2).
- $\mathbf{R}_n$ the Rédei matrix of $K = \mathbb{Q}(\sqrt{-n})$, see (2.1).
- $\mathbf{D}_u = \mathrm{diag}\Big\{\Big[\frac{u}{p_1}\Big],\dots,\Big[\frac{u}{p_k}\Big]\Big\}$.
- $\mathbf{b}_u = \mathbf{D}_u\mathbf{1} = \Big(\Big[\frac{u}{p_1}\Big],\dots,\Big[\frac{u}{p_k}\Big]\Big)$.
- $\mathbf{M}_n$ the Monsky matrix associated to n, see (3.3).
- $\mathcal{M}_n$ the generalized Monsky matrix associated to $E^{(n)}$, see (3.4).
- $I = \sqrt{-1}$.
- $\mathcal{P}$ the set of primary primes of $\mathbb{Z}[I]$ with positive imaginary part.
- $\left(\frac{\alpha}{\lambda}\right)_2$ the quadratic residue symbol over $\mathbb{Z}[I]$, see (5.1).
- $\left(\frac{\alpha}{\lambda}\right)_4$ the quartic residue symbol over $\mathbb{Z}[I]$, see (5.2).
- $\left(\frac{a}{d}\right)_4 := \left(\frac{a}{\lambda}\right)_4$ the rational quartic residue symbol, see (5.3).
- $\Lambda(\mathfrak{a})$ the von Mangoldt function, see (5.4).
- χ_0 the trivial character modulo a given integral ideal, see § 5.2.
- $\psi(x,\chi) = \sum_{\mathbf{N}\mathfrak{a}\leqslant x}\chi(\mathfrak{a})\Lambda(\mathfrak{a})$, see (5.5).
- $C_k(x,\alpha,\mathbf{B}), C_k'(x,\alpha,\mathbf{B}), T_k(x), T_k'(x)$ sets associated to $x,\alpha,\mathbf{B}$, see § 5.3.
- $\binom{k}{2} = k(k-1)/2$ the binomial coefficient.

2. Preliminaries

2.1. **Gauss genus theory.** In this subsection, we will recall Gauss genus theory, which can be found in [Wan16, § 3] for details. For our purpose, assume that $n = p_1\cdots p_k \equiv 1 \bmod 4$. Denote by $\mathcal{A}$ the ideal class group of $K = \mathbb{Q}(\sqrt{-n})$. Denote by $\mathcal{D}(K)$ the set of positive square-free divisors of $2n$. The classical Gauss genus theory tells that

$$\mathcal{A}[2] = \big\{[(d,\sqrt{-n})] : d \in \mathcal{D}(K)\big\} \quad \text{and} \quad h_2(n) = \dim_{\mathbb{F}_2}\mathcal{A}[2] = k.$$

Denote by $p_{k+1} = 2$ and define the Rédei matrix

$$\mathbf{R}_n = \big([p_j,-n]_{p_i}\big)_{i,j} \in M_{k\times(k+1)}(\mathbb{F}_2). \tag{2.1}$$

Proposition 2.1 ([Rei34]). *We have*

$$\begin{array}{rcccl} \mathrm{Ker}\,\mathbf{R}_n & \xleftarrow{\sim} & \mathcal{D}(K)\cap \mathbf{N}_{K/\mathbb{Q}}K^\times & \longrightarrow & \mathcal{A}[2]\cap\mathcal{A}^2 \\ \big(v_{p_1}(d),\dots,v_{p_{k+1}}(d)\big) & \longleftarrow & d & \longmapsto & [(d,\sqrt{-n})], \end{array}$$

where the second arrow is a two-to-one onto homomorphism with kernel $\{1,n\}$. *Hence* $h_4(n) = k - \mathrm{rank}\,\mathbf{R}_n$.

Proposition 2.2 ([Wan16, Proposition 3.6]). *For any $2^r d \in \mathcal{D}(K) \cap \mathbf{N}_{K/\mathbb{Q}} K^\times$ with odd d, let (α, β, γ) be a primitive triple of positive integers satisfying*

$$d\alpha^2 + \frac{n}{d}\beta^2 = 2^r \gamma^2.$$

Then $[(2^r d, \sqrt{-n})] \in \mathcal{A}^4$ if and only if

$$\mathbf{b}_\gamma = \left(\left[\frac{\gamma}{p_1}\right], \dots, \left[\frac{\gamma}{p_k}\right]\right)^{\mathrm{T}} \in \operatorname{Im} \mathbf{R}_n.$$

2.2. **Torsion subgroup.**

Proposition 2.3. *For any positive square-free integer n, $E^{(n)}_{\mathrm{tor}}(\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^2$.*

We need the following lemma.

Lemma 2.4 ([Ono96]). *Let $\mathcal{E} : y^2 = x(x-a)(x+b)$ be an elliptic curve with $a, b \in \mathbb{Z}$.*

1. *$\mathcal{E}(\mathbb{Q})$ has a point of order 4 if and only if one of the three pairs $(-a, b), (a, a+b)$ and $(-b, -a-b)$ consists of squares of integers.*
2. *$\mathcal{E}(\mathbb{Q})$ has a point of order 3 if and only if there exist integers d, u, v such that $\gcd(u, v) = 1$, $d^2u^3(u+2v) = -a, d^2v^3(v+2u) = b$ and $u/v \notin \{-2, -1/2, -1, 1, 0\}$.*

Proof of Proposition 2.3. Since $E^{(n)}$ has full rational 2-torsion, $E^{(n)}_{\mathrm{tor}}(\mathbb{Q})$ contains a subgroup isomorphic to $(\mathbb{Z}/2\mathbb{Z})^2$. By Mazur's classification theorem [Maz77, Maz78], one has

$$E^{(n)}_{\mathrm{tor}}(\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2N\mathbb{Z}$$

for some $N \in \{1, 2, 3, 4\}$. We only need to show that $E^{(n)}(\mathbb{Q})$ contains no point of order 4 or 3.

Since the three pairs in Lemma 2.4(1) are $(-a^2n, b^2n), (a^2n, 2c^2n)$ and $(-b^2n, -2c^2n)$, $E^{(n)}(\mathbb{Q})$ contains no point of order 4.

Assume that there are integers d, u, v such that $\gcd(u, v) = 1$,

$$d^2u^3(u+2v) = -a^2n \quad \text{and} \quad d^2v^3(v+2u) = b^2n.$$

Clearly, $d^2 = 1$ and $n = \gcd(u+2v, v+2u) = \gcd(3, u-v) = 1$ or 3. Since a and b are odd, so is u, v. We may assume that $v > 0$, then $u < 0$. Since $n \mid (u+2v, v+2u)$, we may write $v = \alpha^2, u = -\beta^2$. Then $(\alpha^2 - 2\beta^2)/n$ and $(2\alpha^2 - \beta^2)/n$ are squares, which is impossible by modulo 8. Hence $E^{(n)}(\mathbb{Q})$ contains no point of order 3 by Lemma 2.4(2). □

2.3. **Cassels pairing.** As shown in [Cas98], the 2-Selmer group $\mathrm{Sel}_2\big(E^{(n)}\big)$ can be identified with

$$\Big\{\Lambda = (d_1, d_2, d_3) \in \big(\mathbb{Q}^\times/\mathbb{Q}^{\times 2}\big)^3 : D_\Lambda(\mathbb{A}_\mathbb{Q}) \neq \emptyset, d_1d_2d_3 \equiv 1 \bmod \mathbb{Q}^{\times 2}\Big\},$$

where D_Λ is a genus one curve defined by

$$\begin{cases} H_1: & -b^2nt^2 + d_2u_2^2 - d_3u_3^2 = 0, \\ H_2: & -a^2nt^2 + d_3u_3^2 - d_1u_1^2 = 0, \\ H_3: & 2c^2nt^2 + d_1u_1^2 - d_2u_2^2 = 0. \end{cases} \tag{2.2}$$

Under this identification, the points $O, (a^2n, 0), (-b^2n, 0), (0, 0)$ and non-torsion $(x, y) \in E^{(n)}(\mathbb{Q})$ correspond to

$$(1,1,1),\ (2,2n,n),\ (-2n,2,-n),\ (-n,n,-1) \tag{2.3}$$

and $(x - a^2n, x + b^2n, x)$ respectively.

Cassels in [Cas98] defined an alternating bilinear pairing $\langle -, - \rangle$ on the $\mathbb{F}_2$-vector space

$$\mathrm{Sel}_2'\big(E^{(n)}\big) := \mathrm{Sel}_2\big(E^{(n)}\big)/E^{(n)}(\mathbb{Q})[2]. \tag{2.4}$$

We will write it additively. For any $\Lambda \in \mathrm{Sel}_2\big(E^{(n)}\big)$, choose $P = (P_v) \in D_\Lambda(\mathbb{A}_\mathbb{Q})$. Since H_i is locally solvable everywhere, there exists $Q_i \in H_i(\mathbb{Q})$ by Hasse-Minkowski principle. Let L_i be a linear form in three variables such that $L_i = 0$ defines the tangent plane of H_i at Q_i. Then for any $\Lambda' = (d_1', d_2', d_3') \in \mathrm{Sel}_2\big(E^{(n)}\big)$, define

$$\langle \Lambda, \Lambda' \rangle = \sum_v \langle \Lambda, \Lambda' \rangle_v \in \mathbb{F}_2, \quad \text{where} \quad \langle \Lambda, \Lambda' \rangle_v = \sum_{i=1}^3 \big[L_i(P_v), d_i'\big]_v.$$

This pairing is independent of the choice of P and Q_i, and is trivial on $E^{(n)}(\mathbb{Q})[2]$.

Lemma 2.5 ([Cas98, Lemma 7.2])**.** *The local Cassels pairing $\langle \Lambda, \Lambda' \rangle_p = 0$ if*

- *$p \nmid 2\infty$,*
- *the coefficients of H_i and L_i are all integral at p for $i = 1, 2, 3$, and*
- *modulo D_Λ and L_i by p, they define a curve of genus 1 over $\mathbb{F}_p$ together with tangents to it.*

Lemma 2.6. *The following are equivalent:*

1. *$\mathrm{rank}_\mathbb{Z} E^{(n)}(\mathbb{Q}) = 0$ and $Ш(E^{(n)}/\mathbb{Q})[2^\infty] \cong (\mathbb{Z}/2\mathbb{Z})^{2t}$;*
2. *$\mathrm{Sel}_2'\big(E^{(n)}\big) \cong (\mathbb{Z}/2\mathbb{Z})^{2t}$ and the Cassels pairing on $\mathrm{Sel}_2'\big(E^{(n)}\big)$ is non-degenerate.*

Proof. Note that $E^{(n)}(\mathbb{Q})[2] = (\mathbb{Z}/2\mathbb{Z})^2$ by Proposition 2.3. The proof is similar to [Wan16, p. 2157]. □

By this lemma, the proof of our main result can be reduced to the calculations of the 2-Selmer group and the Cassels pairing on it.

3. 2-descent method

In this section, we will study the local solvability of homogeneous spaces and then express the 2-Selmer group as the null space of a matrix defined over $\mathbb{F}_2$.

3.1. Homogeneous spaces.

Lemma 3.1. *Let n be a positive square-free integer prime to $2abc$ and $\Lambda = (d_1, d_2, d_3)$, where d_1, d_2, d_3 are square-free integers.*

1. *If $p \nmid 2abcn$, then $D_\Lambda(\mathbb{Q}_p) \neq \emptyset$ if and only if $p \nmid d_1d_2d_3$.*
2. *If $D_\Lambda(\mathbb{Q}_2) \neq \emptyset$, then d_1 and d_2 have the same parity.*
3. *If both of d_1 and d_2 are odd, then $D_\Lambda(\mathbb{Q}_2) \neq \emptyset$ if and only if either $4 \mid d_1 - 1, 8 \mid d_1 - d_2$ or $4 \mid d_1 + n, 8 \mid d_1 - d_2 + 2n$.*
4. *$D_\Lambda(\mathbb{R}) \neq \emptyset$ if and only if $d_2 > 0$.*

Proof. Certainly, $\gcd(d_1, d_2, d_3) = 1$. Since we are dealing with homogeneous equations, we may assume that u_1, u_2, u_3 and t are p-adic integers and at least one of them is a p-adic unit.

(1) This follows from the classical descent theory (see [Sil09, Theorem X.1.1, Corollary X.4.4]).

(2) Suppose that $D_\Lambda(\mathbb{Q}_2) \neq \emptyset$. If $2 \mid d_1, 2 \nmid d_2$, then $2 \mid d_3$. We have $2 \mid u_2$ by H_3 and $2 \mid t$ by H_1. Then $2 \mid u_3$ by H_1 and $2 \mid u_1$ by H_2, which is impossible. The case $2 \nmid d_1, 2 \mid d_2$ is similar. Hence d_1 and d_2 have the same parity.

(3) If $D_\Lambda(\mathbb{Q}_2) \neq \emptyset$, then both of u_1, u_2 are odd by H_3 and exactly one of t and u_3 is even by H_2. If t is even and u_3 is odd, then $4 \mid d_1 - d_3, 8 \mid d_1 - d_2$ by H_2 mod 4 and H_3 mod 8. Note that if $8 \mid d_1 - d_2$, then $d_3 \equiv d_1 d_2 \equiv 1 \bmod 8$. If t is odd and u_3 is even, then $4 \mid d_1 + n, 8 \mid d_1 - d_2 + 2n$ by H_2 mod 4 and H_3 mod 8.

Conversely, if $4 \mid d_1 - 1, 8 \mid d_1 - d_2$, then $d_3 \equiv d_1 d_2 \equiv 1 \bmod 8$. Take

- $t = 0, u_1 = \sqrt{1/d_1}, u_2 = \sqrt{1/d_2}, u_3 = \sqrt{1/d_3}$ if $8 \mid d_1 - 1$;
- $t = 2, u_1 = 1, u_2 = \sqrt{(d_1 + 8c^2 n)/d_2}, u_3 = \sqrt{(d_1 + 4a^2 n)/d_3}$ if $8 \mid d_1 - 5$.

If $4 \mid d_1 + n, 8 \mid d_1 - d_2 + 2n$, take

- $t = 1, u_1 = \sqrt{-a^2 n/d_1}, u_2 = \sqrt{b^2 n/d_2}, u_3 = 0$ if $8 \mid d_1 + n$;
- $t = 1, u_1 = \sqrt{(4d_3 - a^2 n)/d_1}, u_2 = \sqrt{(4d_3 + b^2 n)/d_2}, u_3 = 2$ if $8 \mid d_1 + n + 4$.

(4) Suppose that $D_\Lambda(\mathbb{R}) \neq \emptyset$. If $d_2 < 0$, then $d_3 < 0$ by H_1. Thus $d_1 > 0$ by $d_1 d_2 d_3 \in \mathbb{Q}^{\times 2}$ but $d_1 < 0$ by H_2, which is impossible. Hence $d_2 > 0$. The other direction is trivial. □

Assume that n is a positive square-free integer prime to $2abc$. By Lemma 3.1 and (2.3), any element of the pure 2-Selmer group $\mathrm{Sel}_2'(E^{(n)})$ has a unique representative $\Lambda = (d_1, d_2, d_3)$, where d_1, d_2, d_3 are positive square-free integers dividing $nabc$. In the rest of this article, Λ is always assumed to be in this form and we will write $\Lambda = (d_1, d_2, d_3) \in \mathrm{Sel}_2'(E^{(n)})$ for simplicity.

Lemma 3.2. *Let n be a positive square-free integer prime to $2abc$ and $\Lambda = (d_1, d_2, d_3)$. Let p be a prime factor of n. Then $D_\Lambda(\mathbb{Q}_p) \neq \emptyset$ if and only if*

- $\left(\frac{d_1}{p}\right) = \left(\frac{d_2}{p}\right) = 1$, *if* $p \nmid d_1, p \nmid d_2$;
- $\left(\frac{2d_1}{p}\right) = \left(\frac{2n/d_2}{p}\right) = 1$, *if* $p \nmid d_1, p \mid d_2$;
- $\left(\frac{-2n/d_1}{p}\right) = \left(\frac{2d_2}{p}\right) = 1$, *if* $p \mid d_1, p \nmid d_2$;
- $\left(\frac{-n/d_1}{p}\right) = \left(\frac{n/d_2}{p}\right) = 1$, *if* $p \mid d_1, p \mid d_2$.

Proof. Assume that $p \nmid d_1 d_2$, then $p \nmid d_3$. If $D_\Lambda(\mathbb{Q}_p) \neq \emptyset$, then $\left(\frac{d_2 d_3}{p}\right) = \left(\frac{d_1 d_3}{p}\right) = 1$ by H_2 and H_3. That's to say, $\left(\frac{d_1}{p}\right) = \left(\frac{d_2}{p}\right) = 1$. Conversely, if $\left(\frac{d_1}{p}\right) = \left(\frac{d_2}{p}\right) = 1$, then $\left(0, \sqrt{1/d_1}, \sqrt{1/d_2}, \sqrt{1/d_3}\right) \in D_\Lambda(\mathbb{Q}_p)$. The rest of the cases can be proved similarly as in the congruent elliptic curve case, see [HB94, Appendix]. □

Lemma 3.3. *Let n be a positive square-free integer prime to $2abc$ and $\Lambda = (d_1, d_2, d_3)$. Let p be a prime factor of abc.*

(1) *If $p \mid a$, then $D_\Lambda(\mathbb{Q}_p) \neq \emptyset$ if and only if one of the following cases holds:*

- $p \nmid d_2, p \nmid d_1, \left(\frac{d_2}{p}\right) = 1$;
- $p \nmid d_2, p \mid d_1, \left(\frac{d_2}{p}\right) = \left(\frac{n}{p}\right) = 1$.

(2) *If $p \mid b$, then $D_\Lambda(\mathbb{Q}_p) \neq \emptyset$ if and only if one of the following cases holds:*

- $p \nmid d_1, p \nmid d_2, \left(\frac{d_1}{p}\right) = 1$;
- $p \nmid d_1, p \mid d_2, \left(\frac{d_1}{p}\right) = \left(\frac{-n}{p}\right) = 1$.

(3) *If $p \mid c$, then $D_\Lambda(\mathbb{Q}_p) \neq \emptyset$ if and only if one of the following cases holds:*

- $p \nmid d_3, p \nmid d_1, \left(\frac{d_3}{p}\right) = 1$;
- $p \nmid d_3, p \mid d_1, \left(\frac{d_3}{p}\right) = \left(\frac{n}{p}\right) = 1$.

Proof. Let p be a prime factor of a.

Suppose that $D_\Lambda(\mathbb{Q}_p) \neq \emptyset$. If $p \mid d_2$, then p divides exactly one of d_1 and d_3. We may assume that $p \mid d_1$ and $p \nmid d_3$. Then p divides u_3, t by H_2, H_3 and then u_2, u_1 by H_1, H_2. So $p \mid \gcd(t, u_1, u_2, u_3)$, which will cause a contradiction. Hence $p \nmid d_2$.

Suppose that $p \nmid d_1, p \nmid d_3$. If $D_\Lambda(\mathbb{Q}_p) \neq \emptyset$, then $\left(\frac{d_1 d_3}{p}\right) = \left(\frac{d_2}{p}\right) = 1$ by H_2. Conversely, if $\left(\frac{d_2}{p}\right) = 1$, then we may take

$$\begin{aligned} u_1 &= d_2/\gcd(d_1, d_2), \\ u_3^2 &= d_2 + a^2 n t^2/d_3 \equiv d_2 \bmod p, \\ u_2^2 &= d_3 + 2c^2 n t^2/d_2, \end{aligned}$$

where $t \in \mathbb{Z}_p$ such that $d_3 + 2c^2 n t^2/d_2$ is a square in $\mathbb{Z}_p$. In fact, if $-2nd_3$ is quadratic residue modulo p, then we may take $t = \sqrt{-\frac{d_2 d_3}{2c^2 n}}$ and $u_2 = 0$; if $-2nd_1$ is not a quadratic residue modulo p, then there exists $t \in \{0, 1, \dots, (p-1)/2\}$ such that $d_3 + 2c^2 n t^2/d_2 \bmod p$ is a nonzero square. Hence $D_\Lambda(\mathbb{Q}_p)$ is non-empty.

Suppose that $p \mid d_1, p \mid d_3$. If $D_\Lambda(\mathbb{Q}_p) \neq \emptyset$, then $\left(\frac{d_2 n}{p}\right) = 1$ by H_1 and $\left(\frac{d_2}{p}\right) = 1$ by H_2. Conversely, if $\left(\frac{d_2}{p}\right) = \left(\frac{n}{p}\right) = 1$, then we may take $t = 1$ and

$$\begin{aligned} u_1 &= d_2/\gcd(d_1, d_2), \\ u_3^2 &= d_2 + a^2 n/d_3 \equiv d_2 \bmod p, \\ u_2^2 &= d_3 + 2c^2 n/d_2 \equiv b^2 n/d_2 \bmod p. \end{aligned}$$

Hence $D_\Lambda(\mathbb{Q}_p)$ is non-empty.

The rest cases can be proved similarly. □

Lemma 3.4. *Let n be a positive square-free integer prime to $2abc$ and $\Lambda = (d_1, d_2, d_3)$. If $D_\Lambda(\mathbb{Q}_v) \neq \emptyset$ for all places $v \neq 2$, then $D_\Lambda(\mathbb{Q}_2)$ is also non-empty.*

Proof. Since $D_\Lambda(\mathbb{Q}_v) \neq \emptyset$ for all places $v \neq 2$, each H_i is locally solvable at $v \neq 2$. By the product formula of Hilbert symbols, H_i is locally solvable at 2. In other words,

$$[nd_2, d_2 d_3]_2 = [-nd_1, d_3 d_1]_2 = [2nd_2, d_1 d_2]_2 = 0.$$

Then $[nd_2, d_1]_2 = [-nd_1, d_2]_2 = 0$.

- If $d_1 \equiv d_2 \bmod 4$, then $[-n, d_1]_2 = [n, d_2]_2 = [2, d_1d_2]_2 = 0$, which forces $4 \mid d_1 - 1$ and $8 \mid d_1 - d_2$.
- If $d_1 \equiv -d_2 \bmod 4$, then $[n, d_1]_2 = [-n, -d_1]_2 = 0$ and $n \equiv -d_1 \equiv d_2 \bmod 4$. Since $[2, d_1d_2]_2 = [2nd_2, d_1d_2]_2 = 0$, we have $d_1d_2 \equiv -1 \bmod 8$. In other words, $4 \mid d_1 + n$ and $8 \mid d_1 - d_2 + 2n$.

Hence $D_\Lambda(\mathbb{Q}_2) \neq \emptyset$ by Lemma 3.1(3). □

3.2. **Matrix representation.** By the results in the previous subsection, we can express the pure 2-Selmer group $\mathrm{Sel}'_2(E^{(n)})$ as the kernel of a matrix. For our purpose, we assume that n is prime to abc and each prime factor of n is a quadratic residue modulo every prime factor of abc.

Denote by $n = p_1 \cdots p_k$ and

$$a = q_1^{t_1} \cdots q_{\ell_1}^{t_{\ell_1}}, \quad b = q_{\ell_1+1}^{t_{\ell_1+1}} \cdots q_{\ell_2}^{t_{\ell_2}}, \quad c = q_{\ell_2+1}^{t_{\ell_2+1}} \cdots q_\ell^{t_\ell} \tag{3.1}$$

the prime decompositions respectively, where all $t_i > 0$ and $0 \leqslant \ell_1 \leqslant \ell_2 \leqslant \ell$. Let $\Lambda = (d_1, d_2, d_3) \in \mathrm{Sel}'_2(E^{(n)})$ where d_1, d_2, d_3 are positive square-free integers dividing $nabc$. By Lemma 3.3, we have $\gcd(a, d_2) = \gcd(b, d_1) = \gcd(c, d_3) = 1$. In other words, $d_1 \mid nac, d_2 \mid nbc$ and $d_3 \mid nab$. So we may write

$$\begin{aligned} d_1 &= p_1^{x_1} \cdots p_k^{x_k} \cdot q_1^{z_1} \cdots q_{\ell_1}^{z_{\ell_1}} \cdot q_{\ell_2+1}^{z_{\ell_2+1}} \cdots q_\ell^{z_\ell}, \\ d_2 &= p_1^{y_1} \cdots p_k^{y_k} \cdot q_{\ell_1+1}^{z_{\ell_1+1}} \cdots q_{\ell_2}^{z_{\ell_2}} \cdot q_{\ell_2+1}^{z_{\ell_2+1}} \cdots q_\ell^{z_\ell}, \\ d_3 &\equiv p_1^{x_1+y_1} \cdots p_k^{x_k+y_k} \cdot q_1^{z_1} \cdots q_{\ell_1}^{z_{\ell_1}} \cdot q_{\ell_1+1}^{z_{\ell_1+1}} \cdots q_{\ell_2}^{z_{\ell_2}} \bmod \mathbb{Q}^{\times 2}. \end{aligned}$$

Denote by

$$\mathbf{x} = (x_1, \ldots, x_k)^{\mathrm{T}}, \quad \mathbf{y} = (y_1, \ldots, y_k)^{\mathrm{T}} \in \mathbb{F}_2^k,$$

and

$$\mathbf{z} = (z_1, \ldots, z_{\ell_1}, z_{\ell_1+1}, \ldots, z_{\ell_2}, z_{\ell_2+1}, \ldots, z_\ell)^{\mathrm{T}} \in \mathbb{F}_2^\ell.$$

Denote by

$$\begin{pmatrix} \mathbf{F}_1 & \mathbf{F}_2 & \mathbf{F}_3 \\ \mathbf{F}_4 & \mathbf{F}_5 & \mathbf{F}_6 \\ \mathbf{F}_7 & \mathbf{F}_8 & \mathbf{F}_9 \end{pmatrix} = \big([q_j, q_i]_{q_i}\big)_{i,j} \in M_\ell(\mathbb{F}_2),$$

where $\mathbf{F}_1 \in M_{\ell_1}(\mathbb{F}_2)$ and $\mathbf{F}_5 \in M_{\ell_2-\ell_1}(\mathbb{F}_2)$. Denote by

$$\mathcal{M}_1 = \begin{pmatrix} & \mathbf{F}_2 & \mathbf{F}_3 \\ \mathbf{F}_4 & & \mathbf{F}_6 \\ \mathbf{F}_7 & \mathbf{F}_8 & \\ & \Delta & \end{pmatrix} \in M_{(\ell+\ell_2-\ell_1)\times\ell}(\mathbb{F}_2),$$

where

$$\Delta = \mathrm{diag}\Big(\Big[\frac{-1}{q_{\ell_1+1}}\Big], \cdots, \Big[\frac{-1}{q_{\ell_2}}\Big]\Big).$$

Lemma 3.5. *Notations as above. The map* $(d_1, d_2, d_3) \mapsto \mathbf{z}$ *induces an isomorphism*

$$\mathrm{Sel}'_2(E) \xrightarrow{\sim} \mathrm{Ker}\, \mathcal{M}_1.$$

Proof. In the language of linear algebra, Lemma 3.3 tells that

(1) $(\mathbf{O}, \mathbf{F}_2, \mathbf{F}_3)\mathbf{z} = \mathbf{0}$;
(2) $(\mathbf{F}_4, \mathbf{O}, \mathbf{F}_6)\mathbf{z} = \mathbf{0}$ and $\Delta(z_{\ell_1+1}, \ldots, z_{\ell_2})^{\mathrm{T}} = \mathbf{0}$;
(3) $(\mathbf{F}_7, \mathbf{F}_8, \mathbf{O})\mathbf{z} = \mathbf{0}$.

The result then follows from Lemmas 3.1(4) and 3.4 by noting that $n = 1$. □

Denote by

$$\mathbf{D}_u = \operatorname{diag}\left\{ \left[\frac{u}{p_1}\right], \cdots, \left[\frac{u}{p_k}\right] \right\} \in M_k(\mathbb{F}_2),$$

$$\mathbf{A} = \mathbf{A}_n = \left([p_j, -n]_{p_i}\right)_{i,j} \in M_k(\mathbb{F}_2) \tag{3.2}$$

and

$$(\mathbf{G}_1, \mathbf{G}_2, \mathbf{G}_3) = \left([q_j, -n]_{p_i}\right)_{i,j} \in M_{k\times\ell}(\mathbb{F}_2),$$

where $\mathbf{G}_1 \in M_{k\times\ell_1}(\mathbb{F}_2)$ and $\mathbf{G}_2 \in M_{k\times(\ell_2-\ell_1)}(\mathbb{F}_2)$. Denote the Monsky matrix by

$$\mathbf{M}_n = \begin{pmatrix} \mathbf{A} + \mathbf{D}_{-2} & \mathbf{D}_2 \\ \mathbf{D}_2 & \mathbf{A} + \mathbf{D}_2 \end{pmatrix} \tag{3.3}$$

and the generalized Monsky matrix by

$$\mathcal{M}_n = \begin{pmatrix} \mathbf{M}_n & \mathbf{G} \\ & \mathcal{M}_1 \end{pmatrix}, \quad \text{where} \quad \mathbf{G} = \begin{pmatrix} \mathbf{G}_1 & & \mathbf{G}_3 \\ & \mathbf{G}_2 & \mathbf{G}_3 \end{pmatrix}. \tag{3.4}$$

See [HB94, Appendix].

Proposition 3.6. *Notations as above. The map* $(d_1, d_2, d_3) \mapsto \begin{pmatrix} \mathbf{x} \\ \mathbf{y} \\ \mathbf{z} \end{pmatrix}$ *induces an isomorphism*

$$\mathrm{Sel}_2'\big(E^{(n)}\big) \xrightarrow{\sim} \operatorname{Ker} \mathcal{M}_n.$$

Proof. This follows from Lemmas 3.1(4), 3.2, 3.3, 3.4 and 3.5 with $\left(\frac{n}{q}\right) = 1$. □

4. Second minimal Shafarevich-Tate group

In this section, we will prove Theorem 1.1 by calculating the Cassels pairing. Let $n = p_1 \cdots p_k \equiv 1 \bmod 8$ be a positive square-free integer prime to abc where each p_i is a quadratic residue modulo every prime factor of abc.

4.1. **Proof of Theorem 1.1(A).**

Lemma 4.1. *Assume that each* $p_i \equiv \pm 1 \bmod 8$*. Let* $\mathbf{d} = (s_1, \cdots, s_k)^{\mathrm{T}}$ *be a column vector in* $\mathbb{F}_2^k$ *and* $d = p_1^{s_1} \cdots p_k^{s_k}$.

1. $\mathbf{d} \in \operatorname{Ker}(\mathbf{A} + \mathbf{D}_{-1})$ *if and only if* $\mathbf{d} + \left[\frac{-1}{d}\right]\mathbf{1} \in \operatorname{Ker} \mathbf{A}^{\mathrm{T}}$.
2. *Assume that* $\mathrm{Sel}_2(E/\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^2$*. Then* $\dim_{\mathbb{F}_2} \mathrm{Sel}_2'\big(E^{(n)}\big) = 2$ *if and only if* $h_4(n) = 1$*. In which case,* $\mathrm{Sel}_2'\big(E^{(n)}\big)$ *is generated by* $(2, 2, 1)$ *and* $(d, 1, d)$*, where* $\operatorname{Ker}(\mathbf{A} + \mathbf{D}_{-1}) = \{\mathbf{0}, \mathbf{d}\}$.

Proof. (1) We may rearrange the ordering of the prime factors p_i such that $p_1 \equiv \cdots \equiv p_{k'} \equiv -1 \bmod 8$ and $p_{k'+1} \equiv \cdots \equiv p_k \equiv 1 \bmod 8$. Then $\mathbf{b}_{-1} = \begin{pmatrix} \mathbf{1}' \\ \mathbf{0} \end{pmatrix}$, where $\mathbf{1}' \in \mathbb{F}_2^{k'}$. By the quadratic reciprocity law, one can show that

$$\mathbf{A}^{\mathrm{T}} = \mathbf{A} + \mathbf{D}_{-1} + \mathbf{b}_{-1}\mathbf{b}_{-1}^{\mathrm{T}}.$$

Since $n \equiv 1 \bmod 8$, k' is even and $\mathbf{b}_{-1}^{\mathrm{T}}\mathbf{1} = \mathbf{1}^{\mathrm{T}}\mathbf{b}_{-1} = \mathbf{b}_{-1}^{\mathrm{T}}\mathbf{b}_{-1} = k' = 0 \in \mathbb{F}_2$. Since $\mathbf{A}\mathbf{1} = \mathbf{0}$, we have

$$\mathbf{A}^{\mathrm{T}}\mathbf{1} = (\mathbf{A} + \mathbf{D}_{-1} + \mathbf{b}_{-1}\mathbf{b}_{-1}^{\mathrm{T}})\mathbf{1} = \mathbf{b}_{-1}$$

and

$$\mathbf{A}^{\mathrm{T}}(\mathbf{I}+\mathbf{1}\mathbf{b}_{-1}^{\mathrm{T}}) = \mathbf{A}^{\mathrm{T}} + \mathbf{b}_{-1}\mathbf{b}_{-1}^{\mathrm{T}} = \mathbf{A} + \mathbf{D}_{-1}.$$

Hence $\mathbf{d} \in \mathrm{Ker}\,(\mathbf{A}+\mathbf{D}_{-1})$ if and only if

$$(\mathbf{I}+\mathbf{1}\mathbf{b}_{-1}^{\mathrm{T}})\mathbf{d} = \mathbf{d} + (\mathbf{b}_{-1}^{\mathrm{T}}\mathbf{d})\mathbf{1} = \mathbf{d} + \left[\frac{-1}{d}\right]\mathbf{1} \in \mathrm{Ker}\,\mathbf{A}^{\mathrm{T}}.$$

(2) Since $\dim_{\mathbb{F}_2} \mathrm{Sel}_2'(E) = 0$, we have $\mathrm{Ker}\,\mathcal{M}_1 = 0$ by Lemma 3.5. By Proposition 3.6, $\dim_{\mathbb{F}_2} \mathrm{Sel}_2'\big(E^{(n)}\big) = 2$ if and only if the rank of

$$\mathbf{M}_n = \mathrm{diag}\{\mathbf{A}+\mathbf{D}_{-1}, \mathbf{A}\}$$

is $2k-2$. By (1), we have $\mathrm{rank}\,\mathbf{A} = \mathrm{rank}\,(\mathbf{A}+\mathbf{D}_{-1})$ and then

$$\dim_{\mathbb{F}_2} \mathrm{Sel}_2'\big(E^{(n)}\big) = 2 \iff \mathrm{rank}\,\mathbf{A} = k-1.$$

Note that the Rédei matrix of $\mathbb{Q}(\sqrt{-n})$ is $\mathbf{R}_n = (\mathbf{A}, \mathbf{0})$. Then $h_4(n) = 1$ if and only if $\mathrm{rank}\,\mathbf{A} = k-1$ by Proposition 2.1.

If $\mathrm{rank}\,\mathbf{A} = k-1$, then $\mathrm{Ker}\,\mathbf{A} = \{\mathbf{0}, \mathbf{1}\}$. Hence

$$\mathrm{Ker}\,\mathcal{M}_n = \left\{ \begin{pmatrix}\mathbf{0}\\ \mathbf{0}\\ \mathbf{0}\end{pmatrix}, \begin{pmatrix}\mathbf{0}\\ \mathbf{1}\\ \mathbf{0}\end{pmatrix}, \begin{pmatrix}\mathbf{d}\\ \mathbf{0}\\ \mathbf{0}\end{pmatrix}, \begin{pmatrix}\mathbf{d}\\ \mathbf{1}\\ \mathbf{0}\end{pmatrix} \right\}.$$

In other words, $\mathrm{Sel}_2'\big(E^{(n)}\big)$ is generated by $(1, n, n)$ and $(d, 1, d)$. Conclude the result by the fact that $(1, n, n) - (2, 2, 1) = (2, 2n, n)$ corresponds to a torsion, see (2.3). ☐

Theorem 4.2. *Assume that* $\mathrm{Sel}_2(E/\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^2$. *Let n be a positive square-free integer prime to abc where each prime factor of n is a quadratic residue modulo every prime factor of abc. If $n \equiv 1 \bmod 8$ and all of its prime factors are congruent to ± 1 modulo 8, then the following are equivalent:*

(1) $\mathrm{rank}_{\mathbb{Z}} E^{(n)}(\mathbb{Q}) = 0$ *and* $Ш(E^{(n)}/\mathbb{Q})[2^\infty] \cong (\mathbb{Z}/2\mathbb{Z})^2$;
(2) $h_4(n) = 1$ *and* $h_8(n) = 0$.

Proof. By Lemma 2.6, (1) is equivalent to say, $\mathrm{Sel}_2'\big(E^{(n)}\big)$ has dimension 2 and the Cassels pairing on it is non-degenerate. By Lemma 4.1(2), $\dim_{\mathbb{F}_2} \mathrm{Sel}_2'\big(E^{(n)}\big) = 2$ if and only if $h_4(n) = 1$.

Since all prime factors of n are congruent to ± 1 modulo 8, 2 is a norm and there exists a primitive triple (α, β, γ) of positive integers such that

$$\alpha^2 + n\beta^2 = 2\gamma^2.$$

It's easy to see that all of α, β, γ are odd.

Assume that $h_4(n) = 1$. Then by Lemma 4.1(2), $\mathrm{Sel}_2'\big(E^{(n)}\big)$ is generated by $\Lambda = (2, 2, 1)$ and $\Lambda' = (d, 1, d)$. Recall that D_Λ is

$$\begin{cases} H_1: & -b^2nt^2 + 2u_2^2 - u_3^2 = 0,\\ H_2: & -a^2nt^2 + u_3^2 - 2u_1^2 = 0,\\ H_3: & c^2nt^2 + u_1^2 - u_2^2 = 0.\end{cases}$$

Choose

$$Q_1 = (\beta, b\gamma, b\alpha) \in H_1(\mathbb{Q}), \qquad L_1 = bn\beta t - 2\gamma u_2 + \alpha u_3,$$
$$Q_3 = (0, 1, 1) \in H_3(\mathbb{Q}), \qquad L_3 = u_1 - u_2.$$

By Lemma 2.5, we have

$$\langle \Lambda, \Lambda' \rangle = \sum_{p \mid 2nabc} \big[L_1 L_3(P_p), d\big]_p$$

for any $P_p \in D_\Lambda(\mathbb{Q}_p)$. Since $\left(\frac{p_i}{q}\right) = 1$ for any prime $q \mid abc$, we have $\left(\frac{d}{q}\right) = 1$ and $\langle \Lambda, \Lambda' \rangle_q = 0$.

For $p \mid n$, $\alpha^2 \equiv 2\gamma^2 \bmod p$. We may take $\sqrt{2} \in \mathbb{Q}_p$ such that $\sqrt{2}\gamma \equiv \alpha \bmod p$. Take $P_p = (t, u_1, u_2, u_3) = (0, 1, -1, \sqrt{2})$, then

$$L_1 L_3(P_p) = 2(2\gamma + \sqrt{2}\alpha) \equiv 8\gamma \bmod p$$

and

$$\langle \Lambda, \Lambda' \rangle_p = \big[L_1 L_3(P_p), d\big]_p = [\gamma, d]_p.$$

Note that $n(b\beta)^2 - (a\alpha)^2 = 2(b^2\gamma^2 - c^2\alpha^2) \equiv 0 \bmod 16$, so we may take $\sqrt{n} \in \mathbb{Q}_2$ such that $b\beta\sqrt{n} \equiv a\alpha \bmod 8$. Take $P_2 = (1, 0, c\sqrt{n}, -a\sqrt{n})$, then

$$L_1 L_3(P_2) = -c\sqrt{n}(bn\beta - 2c\gamma\sqrt{n} - a\alpha\sqrt{n}) = 2c^2 n\gamma + cn(a\alpha - b\beta\sqrt{n})$$

and

$$\langle \Lambda, \Lambda' \rangle_2 = \big[L_1 L_3(P_2), d\big]_2 = [2c^2 n\gamma, d]_2 = [\gamma, d]_2 = \left[\frac{-1}{d}\right]\left[\frac{-1}{\gamma}\right].$$

Since $\alpha^2 \equiv -n\beta^2 \bmod \gamma$, we have $\left(\frac{-1}{\gamma}\right) = \left(\frac{n}{\gamma}\right) = \left(\frac{\gamma}{n}\right)$. Hence

$$\langle \Lambda, \Lambda' \rangle = \sum_{p \mid n} \langle \Lambda, \Lambda' \rangle_p + \langle \Lambda, \Lambda' \rangle_2 = \left[\frac{\gamma}{d}\right] + \left[\frac{-1}{d}\right]\left[\frac{\gamma}{n}\right].$$

Since $\mathbf{R}_n = (\mathbf{A}, \mathbf{0})$, we have $\mathcal{A}[2] \cap \mathcal{A}^2 = \big\{[(1)], [(2, \sqrt{-n})]\big\}$. Since $\operatorname{Ker} \mathbf{A}^{\mathrm{T}} = \left\{\mathbf{0}, \mathbf{d} + \left[\frac{-1}{d}\right]\mathbf{1}\right\}$ by Lemma 4.1(1), we have

$$\operatorname{Im} \mathbf{R}_n = \operatorname{Im} \mathbf{A} = \left\{\mathbf{u} : \mathbf{u}^{\mathrm{T}}\left(\mathbf{d} + \left[\frac{-1}{d}\right]\mathbf{1}\right) = 0\right\}.$$

By Proposition 2.2, $[(2, \sqrt{-n})] \in \mathcal{A}^4$ if and only if

$$\mathbf{b}_\gamma = \left(\left[\frac{\gamma}{p_1}\right], \dots, \left[\frac{\gamma}{p_k}\right]\right)^{\mathrm{T}} \in \operatorname{Im} \mathbf{R}_n,$$

if and only if

$$\langle \Lambda, \Lambda' \rangle = \left[\frac{\gamma}{d}\right] + \left[\frac{-1}{d}\right]\left[\frac{\gamma}{n}\right] = \mathbf{b}_\gamma^{\mathrm{T}}\left(\mathbf{d} + \left[\frac{-1}{d}\right]\mathbf{1}\right) = 0.$$

In conclusion, the Cassels pairing is non-degenerate if and only if $h_8(n) = 0$. □

4.2. **Proof of Theorem 1.1(B).**

Lemma 4.3. *Assume that each $p_i \equiv 1 \bmod 4$ and $\mathrm{Sel}_2(E/\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^2$. Let $\mathbf{d} = (s_1, \cdots, s_k)^{\mathrm{T}}$ be a column vector in $\mathbb{F}_2^k$ and $d = p_1^{s_1} \cdots p_k^{s_k}$.*

1. *$\dim_{\mathbb{F}_2} \mathrm{Sel}_2'\big(E^{(n)}\big) = 2$ if and only if $h_4(n) = 1$. In which case, $\operatorname{rank} \mathbf{A} = k-2$ or $k-1$.*
2. *If $h_4(n) = 1$ and $\operatorname{rank} \mathbf{A} = k-2$, then $\mathrm{Sel}_2'\big(E^{(n)}\big)$ is generated by $(d, d, 1)$ and $(-1, 1, -1)$, where $\operatorname{Ker} \mathbf{A} = \{\mathbf{0}, \mathbf{1}, \mathbf{d}, \mathbf{d} + \mathbf{1}\}$. Moreover, $d \equiv 5 \bmod 8$.*

(3) *If* $h_4(n) = 1$ *and* $\operatorname{rank}\mathbf{A} = k-1$, *then* $\operatorname{Sel}_2'\big(E^{(n)}\big)$ *is generated by* $(2d, 2d, 1)$ *and* $(-1, 1, -1)$, *where* $\mathbf{A}\mathbf{d} = \mathbf{b}_2$.

Proof. Similar to the proof of Lemma 4.1(2), we have $\operatorname{Ker}\mathcal{M}_1 = 0$. It suffices to show that $\operatorname{rank}\mathbf{M}_n = 2k-2$ if and only if the Rédei matrix $\mathbf{R}_n = (\mathbf{A}, \mathbf{b}_2)$ has rank $k-1$ by Proposition 2.1. Since $\mathbf{A}\mathbf{1} = \mathbf{0}$, we have $\operatorname{rank}\mathbf{A} \leqslant k-1$. If $\operatorname{rank}\mathbf{M}_n = 2k-2$, then

$$2k-2 = \operatorname{rank}\begin{pmatrix}\mathbf{A}+\mathbf{D}_2 & \mathbf{D}_2\\ \mathbf{D}_2 & \mathbf{A}+\mathbf{D}_2\end{pmatrix} = \operatorname{rank}\begin{pmatrix}\mathbf{A} & \mathbf{D}_2\\ & \mathbf{A}\end{pmatrix} \leqslant k + \operatorname{rank}\mathbf{A}$$

and $\operatorname{rank}\mathbf{A} \geqslant k-2$. If $\operatorname{rank}\mathbf{R}_n = k-1$, then clearly $\operatorname{rank}\mathbf{A} \geqslant k-2$.

Suppose that $\operatorname{rank}\mathbf{A} = k-2$. If $\operatorname{rank}\mathbf{M}_n = 2k-2$, then $\mathbf{b}_2 \notin \operatorname{Im}\mathbf{A}$. Otherwise assume that $\mathbf{A}\mathbf{a} = \mathbf{b}_2$, then

$$\operatorname{Ker}\mathbf{M}_n \supseteq \left\{\begin{pmatrix}\mathbf{u}\\ \mathbf{u}\end{pmatrix}, \begin{pmatrix}\mathbf{u}+\mathbf{a}\\ \mathbf{u}+\mathbf{a}+\mathbf{1}\end{pmatrix} : \mathbf{u} \in \operatorname{Ker}\mathbf{A}\right\}$$

has at least 8 elements, which is impossible. Therefore, $\operatorname{rank}\mathbf{R}_n = \operatorname{rank}(\mathbf{A}, \mathbf{b}_2) = k-1$. Conversely, if $\operatorname{rank}\mathbf{R}_n = k-1$, then $\mathbf{b}_2 \notin \operatorname{Im}\mathbf{A}$. Since $n \equiv 1 \bmod 8$, we have $\mathbf{1}^{\mathrm{T}}\mathbf{b}_2 = 0$. Note that $\mathbf{A}$ is symmetric, we have

$$\operatorname{Im}\mathbf{A} = \big\{\mathbf{u} : \mathbf{1}^{\mathrm{T}}\mathbf{u} = \mathbf{d}^{\mathrm{T}}\mathbf{u} = 0\big\},$$

$\mathbf{d}^{\mathrm{T}}\mathbf{b}_2 = 1$ and $\mathbf{1}^{\mathrm{T}}\mathbf{D}_2(\mathbf{d}+\mathbf{1}) = \mathbf{1}^{\mathrm{T}}\mathbf{D}_2\mathbf{d} = \mathbf{b}_2^{\mathrm{T}}\mathbf{d} = 1$. Hence $\mathbf{D}_2\mathbf{1}, \mathbf{D}_2\mathbf{d}, \mathbf{D}_2(\mathbf{d}+\mathbf{1}) \notin \operatorname{Im}\mathbf{A}$. If $\begin{pmatrix}\mathbf{x}\\ \mathbf{y}\end{pmatrix} \in \operatorname{Ker}\mathbf{M}_n$, then $\mathbf{x}+\mathbf{y} \in \operatorname{Ker}\mathbf{A}$ and $\mathbf{D}_2(\mathbf{x}+\mathbf{y}) = \mathbf{A}\mathbf{x}$. This forces $\mathbf{x}+\mathbf{y} = \mathbf{0}$ and $\mathbf{x} = \mathbf{y} \in \operatorname{Ker}\mathbf{A}$. Hence $\#\operatorname{Ker}\mathbf{M}_n = \#\operatorname{Ker}\mathbf{A} = 4$ and $\operatorname{rank}\mathbf{M}_n = 2k-2$. In this case,

$$\operatorname{Ker}\mathcal{M}_n = \left\{\begin{pmatrix}\mathbf{0}\\ \mathbf{0}\\ \mathbf{0}\end{pmatrix}, \begin{pmatrix}\mathbf{1}\\ \mathbf{1}\\ \mathbf{0}\end{pmatrix}, \begin{pmatrix}\mathbf{d}\\ \mathbf{d}\\ \mathbf{0}\end{pmatrix}, \begin{pmatrix}\mathbf{d}+\mathbf{1}\\ \mathbf{d}+\mathbf{1}\\ \mathbf{0}\end{pmatrix}\right\}.$$

In other words, $\operatorname{Sel}_2'\big(E^{(n)}\big)$ is generated by $(n, n, 1)$ and $(d, d, 1)$. Since $\mathbf{d}^{\mathrm{T}}\mathbf{b}_2 = 1$, we have $\left(\frac{2}{d}\right) = 1$ and $d \equiv 5 \bmod 8$.

Suppose that $\operatorname{rank}\mathbf{A} = k-1$. Then $\operatorname{Ker}\mathbf{A} = \{\mathbf{0}, \mathbf{1}\}$ and $\operatorname{Im}\mathbf{A} = \big\{\mathbf{u} : \mathbf{1}^{\mathrm{T}}\mathbf{u} = 0\big\}$. Since $n \equiv 1 \bmod 8$, we have $\mathbf{1}^{\mathrm{T}}\mathbf{b}_2 = 0$ and $\mathbf{b}_2 \in \operatorname{Im}\mathbf{A}$. Thus $\operatorname{rank}\mathbf{R}_n = k-1$, $h_4(n) = 1$ and

$$\operatorname{Ker}\mathcal{M}_n = \left\{\begin{pmatrix}\mathbf{0}\\ \mathbf{0}\\ \mathbf{0}\end{pmatrix}, \begin{pmatrix}\mathbf{1}\\ \mathbf{1}\\ \mathbf{0}\end{pmatrix}, \begin{pmatrix}\mathbf{d}\\ \mathbf{d}+\mathbf{1}\\ \mathbf{0}\end{pmatrix}, \begin{pmatrix}\mathbf{d}+\mathbf{1}\\ \mathbf{d}\\ \mathbf{0}\end{pmatrix}\right\}.$$

In this case, $\operatorname{Sel}_2'\big(E^{(n)}\big)$ is generated by $(n, n, 1)$ and (d, nd, n).

Conclude the result by the fact that $(n, n, 1) - (-1, 1, -1) = (-n, n, -1)$ and $(d, nd, n) - (2d, 2d, 1) = (2, 2n, n)$ correspond torsions, see (2.3). □

Theorem 4.4. *Assume that* $\operatorname{Sel}_2(E/\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^2$. *Let n be a positive square-free integer prime to abc where each prime factor of n is a quadratic residue modulo every prime factor of abc. If* $n \equiv 1 \bmod 8$ *and all of its prime factors are congruent to* 1 *modulo* 4, *then the following are equivalent:*

(1) $\operatorname{rank}_{\mathbb{Z}} E^{(n)}(\mathbb{Q}) = 0$ *and* $\text{Ш}(E^{(n)}/\mathbb{Q})[2^\infty] \cong (\mathbb{Z}/2\mathbb{Z})^2$;

(2) $h_4(n) = 1$ *and* $h_8(n) \equiv \frac{d-1}{4} \bmod 2$.

Here d is the odd part of $d_0 \mid 2n$ such that the ideal class $[(d_0, \sqrt{-n})]$ is the non-trivial element in $\mathcal{A}[2] \cap \mathcal{A}^2$.

Proof. By Lemma 2.6, (1) is equivalent to say, $\mathrm{Sel}_2'(E^{(n)})$ has dimension 2 and the Cassels pairing on it is non-degenerate. By Lemma 4.3(1), $\dim_{\mathbb{F}_2} \mathrm{Sel}_2'(E^{(n)}) = 2$ if and only if $h_4(n) = 1$. Assume that $h_4(n) = 1$.

(1) The case $\operatorname{rank} \mathbf{A} = k - 2$. By Lemma 4.3(2) and Proposition 2.1, we have $\mathbf{b}_2 \notin \operatorname{Im} \mathbf{A}$ and $\mathcal{D}(K) \cap \mathbf{N}_{K/\mathbb{Q}} K^\times = \{1, n, d, n/d\}$ with $d = d_0 \equiv 5 \bmod 8$. Denote by $d' = n/d \equiv 5 \bmod 8$. Since d is a norm, there exists a primitive triple (α, β, γ) of positive integers such that

$$d\alpha^2 + d'\beta^2 = \gamma^2.$$

If α is odd, then β is even and the triple

$$(\alpha', \beta', \gamma') = \left(\left| \frac{(d-d')\alpha}{2} + d'\beta \right|, \left| \frac{(d-d')\beta}{2} - d\alpha \right|, \frac{(d+d')\gamma}{2} \right)$$

is another primitive solution with even α'. Thus we may assume that α is even. Then all of $\alpha/2, \beta, \gamma$ are odd since $d' \equiv 5 \bmod 8$.

By Lemma 4.3(2), $\mathrm{Sel}_2'(E^{(n)})$ is generated by $\Lambda = (d, d, 1)$ and $\Lambda' = (-1, 1, -1)$. Recall that D_Λ is

$$\begin{cases} H_1: & -b^2nt^2 + du_2^2 - u_3^2 = 0, \\ H_2: & -a^2nt^2 + u_3^2 - du_1^2 = 0, \\ H_3: & 2c^2d't^2 + u_1^2 - u_2^2 = 0. \end{cases}$$

Choose

$$\begin{aligned} Q_1 &= (\beta, b\gamma, bd\alpha) \in H_1(\mathbb{Q}), & L_1 &= bd'\beta t - \gamma u_2 + \alpha u_3, \\ Q_3 &= (0, 1, 1) \in H_3(\mathbb{Q}), & L_3 &= u_1 - u_2. \end{aligned}$$

By Lemma 2.5, we have

$$\langle \Lambda, \Lambda' \rangle = \sum_{p \mid 2nabc\infty} \big[L_1L_3(P_p), -1 \big]_p$$

for any $P_p \in D_\Lambda(\mathbb{Q}_p)$. For each $p \mid n$, we have $p \equiv 1 \bmod 4$ and then $\langle \Lambda, \Lambda' \rangle_p = 0$. Since for any $q \mid c$, we have $-a^2 = b^2 - 2c^2 \equiv b^2 \bmod q$, we have $q \equiv 1 \bmod 4$ and then $\langle \Lambda, \Lambda' \rangle_q = 0$.

Take $P_\infty = (t, u_1, u_2, u_3) = (0, 1, -1, \sqrt{d})$, then

$$L_1L_3(P_\infty) = 2(\gamma + \alpha\sqrt{d}) > 0$$

and

$$\langle \Lambda, \Lambda' \rangle_\infty = \big[L_1L_3(P_\infty), -1 \big]_\infty = 0.$$

Take $P_2 = (2, \sqrt{1 - 8c^2d'}, 1, \sqrt{d - 4b^2n})$ where $u_1 \equiv 3 \bmod 8$. Note that $bd'\beta + \alpha u_3/2$ is even. We have

$$L_1L_3(P_2) = (u_1 - 1)(2bd'\beta + \alpha u_3 - \gamma)$$

and

$$\langle \Lambda, \Lambda' \rangle_2 = \big[L_1L_3(P_2), -1 \big]_2 = [2, -1]_2 + [-\gamma, -1]_2 = \left[\frac{-1}{\gamma} \right] + 1.$$

Since $d\alpha^2 \equiv -d'\beta^2 \bmod \gamma$, we have $\left(\frac{-1}{\gamma} \right) = \left(\frac{n}{\gamma} \right) = \left(\frac{\gamma}{n} \right)$ and $\langle \Lambda, \Lambda' \rangle_2 = \left[\frac{\gamma}{n} \right] + 1$.

For $q \mid ab$, take $P_q = (0, 1, -1, \sqrt{d})$. Since $\gamma^2 - d\alpha^2 = d'\beta^2$, we may choose $\sqrt{d}$ such that $q \mid (\gamma - \alpha\sqrt{d})$ if $q \mid \beta$. Then

$$L_1L_3(P_q) = 2(\gamma + \alpha\sqrt{d}) \in \mathbb{Z}_q^\times$$

and

$$\langle \Lambda, \Lambda' \rangle_q = \big[L_1L_3(P_q), -1\big]_q = 0.$$

Hence

$$\langle \Lambda, \Lambda' \rangle = \langle \Lambda, \Lambda' \rangle_2 = \left[\frac{\gamma}{n}\right] + 1.$$

Since $\mathbf{R}_n = (\mathbf{A}, \mathbf{b}_2)$, we have $\mathcal{A}[2] \cap \mathcal{A}^2 = \big\{[(1)], [(d, \sqrt{-n})]\big\}$. Since $\mathbf{b}_2 \notin \operatorname{Im}\mathbf{A}$ and $\mathbf{A}\mathbf{1} = \mathbf{0}$, we have

$$\operatorname{Im}\mathbf{R}_n = \big\{\mathbf{u} : \mathbf{1}^{\mathrm{T}}\mathbf{u} = 0\big\}.$$

By Lemma 2.2, $[(d, \sqrt{-n})] \in \mathcal{A}^4$ if and only if

$$\mathbf{b}_\gamma = \Big(\left[\frac{\gamma}{p_1}\right], \dots, \left[\frac{\gamma}{p_k}\right]\Big)^{\mathrm{T}} \in \operatorname{Im}\mathbf{R}_n,$$

if and only if

$$\langle \Lambda, \Lambda' \rangle = \left[\frac{\gamma}{n}\right] + 1 = \mathbf{1}^{\mathrm{T}}\mathbf{b}_\gamma + 1 = 1.$$

In conclusion, the Cassels pairing is non-degenerate if and only if $h_8(n) = 1 = \left[\frac{2}{d}\right]$.

(2) The case $\operatorname{rank}\mathbf{A} = k - 1$. By Lemma 4.3(3) and Proposition 2.1, we have $\mathbf{b}_2 \in \operatorname{Im}\mathbf{A}$ and $\mathcal{D}(K) \cap \mathbf{N}_{K/\mathbb{Q}}K^\times = \{1, n, 2d, 2n/d\}$. Denote by $d' = n/d$. Since $d_0 = 2d$ is a norm, there exists a primitive triple (α, β, γ) of positive integers such that

$$d\alpha^2 + d'\beta^2 = 2\gamma^2.$$

It's easy to see that all of α, β, γ are odd.

By Lemma 4.3(3), $\mathrm{Sel}_2'\big(E^{(n)}\big)$ is generated by $\Lambda = (2d, 2d, 1)$ and $\Lambda' = (-1, 1, -1)$. Recall that D_Λ is

$$\begin{cases} H_1: & -b^2nt^2 + 2du_2^2 - u_3^2 = 0, \\ H_2: & -a^2nt^2 + u_3^2 - 2du_1^2 = 0, \\ H_3: & c^2d't^2 + u_1^2 - u_2^2 = 0. \end{cases}$$

Choose

$$Q_1 = (\beta, b\gamma, bd\alpha) \in H_1(\mathbb{Q}), \qquad L_1 = bd'\beta t - 2\gamma u_2 + \alpha u_3,$$
$$Q_3 = (0, 1, 1) \in H_3(\mathbb{Q}), \qquad L_3 = u_1 - u_2.$$

Similar to the case $\operatorname{rank}\mathbf{A} = k - 2$, we have

$$\langle \Lambda, \Lambda' \rangle = \sum_{p \mid 2ab\infty} \big[L_1L_3(P_p), -1\big]_p$$

for any $P_p \in D_\Lambda(\mathbb{Q}_p)$.

For $p = \infty$, take $P_\infty = (0, 1, -1, \sqrt{2d})$. Then

$$L_1L_3(P_\infty) = 2(2\gamma + \alpha\sqrt{2d}) > 0$$

and

$$\langle \Lambda, \Lambda' \rangle_\infty = \big[L_1L_3(P_\infty), -1\big]_\infty = 0.$$

For $p = 2$, take $P_2 = (t, u_1, u_2, u_3)$ where

$$t = 1, \ u_1 = 2\left[\frac{2}{d}\right], \ u_2^2 = c^2d' + u_1^2, \ u_3^2 = a^2n + 2du_1^2$$

with $\gamma u_2 \equiv 1 \bmod 4$. Since

$$\begin{aligned}
&(bd'\beta + \alpha u_3)(bd'\beta - \alpha u_3) = b^2 {d'}^2 \beta^2 - \alpha^2(a^2 n + 2du_1^2)\\
=&b^2 d'(2\gamma^2 - d\alpha^2) - \alpha^2(a^2 n + 2du_1^2) = 2b^2 d'\gamma^2 - \alpha^2(2c^2 n + 2du_1^2)\\
=&2\big((bd'\gamma)^2 - n\alpha^2 u_2^2\big)/d' \equiv 0 \bmod 16,
\end{aligned}$$

we may choose u_3 such that $8 \mid bd'\beta + \alpha u_3$. Then

$$\begin{aligned}
\langle \Lambda, \Lambda' \rangle_2 =&\big[L_1 L_3(P_2), -1\big]_2 = \big[(u_1 - u_2)(bd'\beta + \alpha u_3 - 2\gamma u_2), -1\big]_2\\
=&\big[-2\gamma u_2(u_1 - u_2), -1\big]_2 = [2, -1]_2 + \big[u_2 - u_1, -1\big]_2\\
=&[\gamma, -1]_2 + [1 - u_1\gamma, -1]_2\\
=&\Big[\frac{-1}{\gamma}\Big] + \Big[1 - 2\Big[\frac{2}{d}\Big], -1\Big]_2 = \Big[\frac{-1}{\gamma}\Big] + \Big[\frac{2}{d}\Big].
\end{aligned}$$

Since $d\alpha^2 \equiv -d'\beta^2 \bmod \gamma$, we have $\Big(\frac{-1}{\gamma}\Big) = \Big(\frac{n}{\gamma}\Big) = \Big(\frac{\gamma}{n}\Big)$ and $\langle \Lambda, \Lambda' \rangle_2 = \Big[\frac{\gamma}{n}\Big] + \Big[\frac{2}{d}\Big]$.

For $q \mid a$, take $P_q = (1, 0, u_2, a\sqrt{n})$ where $u_2^2 = c^2 d'$. Since

$$\begin{aligned}
&(bd'\beta - 2\gamma u_2)(bd'\beta + 2\gamma u_2) = b^2 {d'}^2 \beta^2 - 4c^2 d'\gamma^2\\
\equiv&2c^2 d'(d'\beta^2 - 2\gamma^2) = -2c^2 n\alpha^2 \bmod q,
\end{aligned}$$

we may choose u_2 such that $q \mid bd'\beta + 2\gamma u_2$ if $q \mid \alpha$. If $q \mid bd'\beta \pm 2\gamma u_2$, then $q \mid \beta$, which contradicts to the primitivity of (α, β, γ). Therefore, $q \nmid bd'\beta - 2\gamma u_2$. If $q \nmid \alpha$, clearly we have $q \nmid bd'\beta \pm 2\gamma u_2$. Then

$$L_1 L_3(P_q) = -u_2(bd'\beta - 2\gamma u_2 + a\alpha\sqrt{n}) \in \mathbb{Z}_q^\times$$

and

$$\langle \Lambda, \Lambda' \rangle_q = \big[L_1 L_3(P_q), -1\big]_q = 0.$$

Similarly, $\langle \Lambda, \Lambda' \rangle_q = 0$ for $q \mid b$. Hence

$$\langle \Lambda, \Lambda' \rangle = \langle \Lambda, \Lambda' \rangle_2 = \Big[\frac{\gamma}{n}\Big] + \Big[\frac{2}{d}\Big].$$

Since $\mathbf{R}_n = (\mathbf{A}, \mathbf{b}_2)$, we have $\mathcal{A}[2] \cap \mathcal{A}^2 = \big\{[(1)], [(2d, \sqrt{-n})]\big\}$. Since $\mathbf{b}_2 \in \operatorname{Im} \mathbf{A}$, we have

$$\operatorname{Im} \mathbf{R}_n = \operatorname{Im} \mathbf{A} = \big\{\mathbf{u} : \mathbf{1}^{\mathrm{T}} \mathbf{u} = 0\big\}.$$

By Lemma 2.2, $[(2d, \sqrt{-n})] \in \mathcal{A}^4$ if and only if

$$\mathbf{b}_\gamma = \Big(\Big[\frac{\gamma}{p_1}\Big], \dots, \Big[\frac{\gamma}{p_k}\Big]\Big)^{\mathrm{T}} \in \operatorname{Im} \mathbf{R}_n,$$

if and only if

$$\langle \Lambda, \Lambda' \rangle = \Big[\frac{\gamma}{n}\Big] + \Big[\frac{2}{d}\Big] = \mathbf{1}^{\mathrm{T}} \mathbf{b}_\gamma + \Big[\frac{2}{d}\Big] = \Big[\frac{2}{d}\Big].$$

In conclusion, the Cassels pairing is non-degenerate if and only if $h_8(n) = \Big[\frac{2}{d}\Big]$. □

5. Equidistribution of residue symbols

In this and next sections, we will prove Theorem 1.3.

5.1. **Residue symbols.**

Definition 5.1. Denote by $I=\sqrt{-1}$ and $\mathbb{Z}[I]$ the ring of Gaussian integers.
(1) A prime element λ of $\mathbb{Z}[I]$ is called *Gaussian* if it is not a rational prime.
(2) An integer $\lambda\in\mathbb{Z}[I]$ is called *primary* if $\lambda\equiv 1 \bmod (2+2I)$.

Recall the quadratic and quartic residue symbols on $\mathbb{Z}[I]$, referring to [Hec81, p. 196] and [IR90]. Denote by $\mathbf{N}=\mathbf{N}_{\mathbb{Q}(I)/\mathbb{Q}}$ the norm from $\mathbb{Q}(I)$ to $\mathbb{Q}$. For any $\alpha\in\mathbb{Z}[I]$ and prime element λ prime to $1+I$, define

$$\left(\frac{\alpha}{\lambda}\right)_2\in\{0,\pm1\}\quad\text{such that}\quad\left(\frac{\alpha}{\lambda}\right)_2\equiv\alpha^{\frac{\mathbf{N}\lambda-1}{2}}\bmod\lambda. \tag{5.1}$$

For any element λ prime to $1+I$ with a prime decomposition $\lambda=\prod_{i=1}^k\lambda_k$, define $\left(\frac{\alpha}{\lambda}\right)_2=\prod_{i=1}^k\left(\frac{\alpha}{\lambda_i}\right)_2$.

For any $\alpha\in\mathbb{Z}[I]$ and primary prime λ, define

$$\left(\frac{\alpha}{\lambda}\right)_4\in\{0,\pm1,\pm I\}\quad\text{such that}\quad\left(\frac{\alpha}{\lambda}\right)_4\equiv\alpha^{\frac{\mathbf{N}\lambda-1}{4}}\bmod\lambda. \tag{5.2}$$

For any primary element λ with a primary prime decomposition $\lambda=\prod_{i=1}^k\lambda_k$, define $\left(\frac{\alpha}{\lambda}\right)_4=\prod_{i=1}^k\left(\frac{\alpha}{\lambda_i}\right)_4$. Let λ and λ' be two coprime primary primes. Then we have the quartic reciprocity law

$$\left(\frac{\lambda}{\lambda'}\right)_4=\left(\frac{\lambda'}{\lambda}\right)_4(-1)^{\frac{\mathbf{N}\lambda-1}{4}\cdot\frac{\mathbf{N}\lambda'-1}{4}}.$$

Certainly, $\left(\frac{\alpha}{\lambda}\right)_2=\left(\frac{\alpha}{\lambda}\right)_4^2$.

Let p be a rational prime such that $p\equiv 1\bmod 4$. Let a be a rational integer such that $\left(\frac{a}{p}\right)=1$. By abuse of notations, we define

$$\left(\frac{a}{p}\right)_4:=\left(\frac{a}{\lambda}\right)_4, \tag{5.3}$$

where λ is a primary prime such that $\mathbf{N}\lambda=p$. For any rational integer $d=p_1\cdots p_k$ with $p_i\equiv 1\bmod 4$, define $\left(\frac{a}{d}\right)_4=\prod_{i=1}^k\left(\frac{a}{p_i}\right)_4$.

5.2. **Analytic results.**

Let F be a number field with degree n, Δ the discriminant of F and $\mathcal{O}$ the ring of integers of F. Denote by $\mathbf{N}=\mathbf{N}_{F/\mathbb{Q}}$ the norm from F to $\mathbb{Q}$.

For an ideal $\mathfrak{f}$ of $\mathcal{O}$, denote by $I(\mathfrak{f})$ the group of fractional ideals prime to $\mathfrak{f}$ and $P_{\mathfrak{f}}$ the subgroup consisting of principal fractional ideals $(\gamma)=\gamma\mathcal{O}$ with totally real $\gamma\equiv 1\bmod\mathfrak{f}$. A character χ of $I(\mathfrak{f})/P_{\mathfrak{f}}$ is called a *character modulo* $\mathfrak{f}$. It can be viewed as a character on $I(\mathfrak{f})$. If $\mathfrak{a}$ is a fractional ideal not coprime to $\mathfrak{f}$, define $\chi(\mathfrak{a})=0$. Denote by

$$\Lambda(\mathfrak{a})=\begin{cases}\log\mathbf{N}\mathfrak{p} & \text{if } \mathfrak{a}=\mathfrak{p}^m \text{ with } m\geqslant 1;\\ 0 & \text{otherwise}\end{cases} \tag{5.4}$$

the *von Mangoldt function*. Define

$$\psi(x,\chi)=\sum_{\mathbf{N}\mathfrak{a}\leqslant x}\chi(\mathfrak{a})\Lambda(\mathfrak{a}). \tag{5.5}$$

Denote by χ_0 the principal character on $I(\mathfrak{f})/P_{\mathfrak{f}}$.

Proposition 5.2 ([IK04, p. 112, Exercise 7])**.** *If $\chi \neq \chi_0$ is a character modulo $\mathfrak{f}$ and $1 \leqslant T \leqslant x$, then*

$$\psi(x,\chi) = -\sum_{|\mathrm{Im}\,\rho|\leqslant T} \frac{x^\rho - 1}{\rho} + O\big(T^{-1} x \log x \log(x^n \mathbf{N}\mathfrak{f})\big).$$

Here ρ runs over all the zeros of $L(s,\chi)$ with $0 \leqslant \mathrm{Re}\,\rho \leqslant 1$.

Similar to the classical process on the estimation of $\psi(x,\chi)$ as in [Dav80, § 19], we derive the following explicit formula

$$\psi(x,\chi) = -\frac{x^{\beta'}}{\beta'} + R(x,T) \tag{5.6}$$

with

$$R(x,T) \ll x \log^2(x\mathbf{N}\mathfrak{f}) \exp\left(-\frac{c_1 \log x}{\log(T\mathbf{N}\mathfrak{f})}\right) + T^{-1} x \log x \cdot \log(x^n \mathbf{N}\mathfrak{f}) + x^{\frac{1}{4}} \log x.$$

We also use the estimation on the number of zeroes in [Lan18, Satz LXXI]. Here c_1 is a positive constant and the term $-\frac{x^{\beta'}}{\beta'}$ occurs only if χ is a real character such that $L(s,\chi)$ has a zero β' satisfying

$$\beta' > 1 - \frac{c_2}{\log \mathbf{N}\mathfrak{f}}$$

with c_2 a positive constant.

We recall the Siegel Theorem as in [Fog61, Theorem] and [Fog63, Satz].

Proposition 5.3. *Let χ be a character modulo an integral $\mathfrak{f}$ and $D = |\Delta|\mathbf{N}\mathfrak{f} > 1$.*

(1) *There is a positive constant $c_3 = c_3(n)$ such that in the region*

$$\mathrm{Re}\,(s) > 1 - \frac{c_3}{\log D(2 + |\mathrm{Im}\,s|)} > \frac{3}{4}$$

there is no zero of $L(s,\chi)$ in the case of a complex χ. For at most one real χ', there may be a simple zero β' of $L(s,\chi')$ in this region.

(2) *For any $\varepsilon > 0$, there exists a positive constant $c_4 = c_4(n,\varepsilon)$ such that*

$$1 - \beta' > c_4(n,\varepsilon) D^{-\varepsilon}.$$

We recall the Page Theorem as a special case of [HR95, § 3, Theorem A].

Proposition 5.4. *For any $Z \geqslant 2$ and a suitable constant c_5, there is at most one real primitive character χ modulo $\mathfrak{f}$ with $\mathbf{N}\mathfrak{f} \leqslant Z$ such that $L(s,\chi)$ has a real zero β satisfying*

$$\beta > 1 - \frac{c_5}{\log Z}.$$

5.3. **Equidistribution of residue symbols.** Recall that $abc = q_1^{t_1} \cdots q_\ell^{t_\ell}$ is the prime decomposition of abc. Let $\alpha = (\alpha_1, \cdots, \alpha_k)$ be a vector with $\alpha_i \in \{1, 5, 9, 13\}$ and $\alpha_1 \cdots \alpha_k \equiv 1 \bmod 8$. Let $\mathbf{B} = (B_{ij})_{k\times k} \in M_k(\mathbb{F}_2)$ be a symmetric matrix with rank $k-2$ such that $\mathbf{B1} = \mathbf{0}$. Then $\mathrm{Ker}\,\mathbf{B} = \{\mathbf{0}, \mathbf{1}, \mathbf{d}, \mathbf{d}+\mathbf{1}\}$ for some vector $\mathbf{d} = (s_1, \cdots, s_k)^{\mathrm{T}}$ with $s_k = 0$.

Denote by $C_k(x, \alpha, \mathbf{B})$ the set of all $n = p_1 \cdots p_k$ satisfying

- $n \leqslant x$ and $p_1 < \cdots < p_k$;
- $p_i \equiv \alpha_i \bmod 16$ for all $1 \leqslant i \leqslant k$;
- $\left[\dfrac{p_j}{p_i}\right] = B_{ij}$ for all $1 \leqslant i < j \leqslant k$;

- $\left(\dfrac{p_i}{q_j}\right) = 1$ for all $1 \leqslant i \leqslant k$ and $1 \leqslant j \leqslant \ell$;
- $\left(\dfrac{d'}{d}\right)_4 \left(\dfrac{d}{d'}\right)_4 = -1$, where $d = p_1^{s_1} \cdots p_k^{s_k}$ and $d' = n/d$,

and denote by $C'_k(x, \alpha, \mathbf{B})$ the set of all $\eta = \lambda_1 \cdots \lambda_k$ satisfying

- $\mathbf{N}\eta \leqslant x$ and $\mathbf{N}\lambda_1 < \cdots < \mathbf{N}\lambda_k$;
- $\lambda_i \in \mathcal{P}$ and $\mathbf{N}\lambda_i \equiv \alpha_i \bmod 16$ for all $1 \leqslant i \leqslant k$;
- $\left[\dfrac{\mathbf{N}\lambda_j}{\mathbf{N}\lambda_i}\right] = B_{ij}$ for all $1 \leqslant i < j \leqslant k$;
- $\left(\dfrac{\mathbf{N}\lambda_i}{q_j}\right) = 1$ for all $1 \leqslant i \leqslant k$ and $1 \leqslant j \leqslant \ell$;
- $\left(\dfrac{\delta'}{\delta}\right)_2 = -1$, where $\delta = \lambda_1^{s_1} \cdots \lambda_k^{s_k}$ and $\delta' = \eta/\delta$.

Here, $\mathcal{P}$ is the set of primary primes in $\mathbb{Z}[I]$ with positive imaginary part.

In this section, we will give an estimation of the number of $C_k(x, \alpha, \mathbf{B})$.

Lemma 5.5. *There is a bijection*

$$C'_k(x, \alpha, \mathbf{B}) \longrightarrow C_k(x, \alpha, \mathbf{B}), \quad \eta \mapsto \mathbf{N}\eta.$$

Proof. For any $\eta = \lambda_1 \cdots \lambda_k \in C'_k(x, \alpha, \mathbf{B})$, denote by $p_i = \mathbf{N}\lambda_i$. By the quartic reciprocity law, we have

$$\left(\frac{p_i}{p_j}\right)_4 \left(\frac{p_j}{p_i}\right)_4 = \left(\frac{\lambda_i\overline{\lambda_i}}{\lambda_j}\right)_4 \left(\frac{\lambda_j\overline{\lambda_j}}{\lambda_i}\right)_4 = \left(\frac{\lambda_i}{\lambda_j}\right)_4 \left(\frac{\overline{\lambda_i}}{\lambda_j}\right)_4 \left(\frac{\lambda_j}{\lambda_i}\right)_4 \left(\frac{\overline{\lambda_j}}{\lambda_i}\right)_4$$
$$= \left(\frac{\lambda_j}{\lambda_i}\right)_4 \left(\frac{\lambda_j}{\overline{\lambda_i}}\right)_4 \left(\frac{\lambda_j}{\lambda_i}\right)_4 \left(\frac{\overline{\lambda_j}}{\lambda_i}\right)_4 = \left(\frac{\lambda_j}{\lambda_i}\right)_2 \overline{\left(\frac{\overline{\lambda_j}}{\lambda_i}\right)_4} \left(\frac{\overline{\lambda_j}}{\lambda_i}\right)_4 = \left(\frac{\lambda_j}{\lambda_i}\right)_2.$$

Therefore,

$$\left(\frac{d'}{d}\right)_4 \left(\frac{d}{d'}\right)_4 = \left(\frac{\delta'}{\delta}\right)_2 = -1,$$

where $d = \mathbf{N}\delta$ and $d' = \mathbf{N}\delta'$. Hence $\mathbf{N}\eta \in C_k(x, \alpha, \mathbf{B})$.

For any rational prime $p \equiv 1 \bmod 4$, there is exactly one primary prime in $\mathcal{P}$ with norm p. This gives the surjectivity. The injectivity is trivial. □

Denote by $T_k(x)$ the set of all $n = p_1 \cdots p_{k-1}$ satisfying

- $n \leqslant x$ and $p_1 < \cdots < p_{k-1}$;
- $p_i \equiv \alpha_i \bmod 16$ for all $1 \leqslant i \leqslant k-1$;
- $\left[\dfrac{p_j}{p_i}\right] = B_{ij}$ for all $1 \leqslant i < j \leqslant k-1$;
- $\left(\dfrac{p_i}{q_j}\right) = 1$ for all $1 \leqslant i \leqslant k-1$ and $1 \leqslant j \leqslant \ell$,

and denote by $T'_k(x)$ the set of all $\eta = \lambda_1 \cdots \lambda_{k-1}$ satisfying

- $\mathbf{N}\eta \leqslant x$ and $\mathbf{N}\lambda_1 < \cdots < \mathbf{N}\lambda_{k-1}$;
- $\lambda_i \in \mathcal{P}$ and $\mathbf{N}\lambda_i \equiv \alpha_i \bmod 16$ for all $1 \leqslant i \leqslant k-1$;
- $\left[\dfrac{\mathbf{N}\lambda_j}{\mathbf{N}\lambda_i}\right] = B_{ij}$ for all $1 \leqslant i < j \leqslant k-1$;
- $\left(\dfrac{\mathbf{N}\lambda_i}{q_j}\right) = 1$ for all $1 \leqslant i < k$ and $1 \leqslant j \leqslant \ell$.

The independence property of Legendre symbols in [Rho09] implies that

$$\#T_k(x) \sim 2^{-(\ell+3)(k-1)-\binom{k-1}{2}} \cdot \#C_{k-1}(x), \tag{5.7}$$

where $C_k(x)$ is the set of all positive square-free integers $n \leqslant x$ with exactly k prime factors.

Lemma 5.6. *There is a bijection*

$$T'_k(x) \longrightarrow T_k(x), \quad \eta \mapsto \mathbf{N}\eta.$$

Proof. For any rational prime $p \equiv 1 \bmod 4$, there is exactly one primary prime in $\mathcal{P}$ with norm p. This proves the surjectivity. The injectivity is trivial. ☐

Theorem 5.7. *Notations as above with $k > 1$. We have*

$$\#C_k(x, \alpha, \mathbf{B}) \sim 2^{-k\ell-3k-1-\binom{k}{2}} \cdot \#C_k(x),$$

where $C_k(x)$ is the set of all positive square-free integers $n \leqslant x$ with exactly k prime factors.

Proof. Similar to [CO89], we consider the comparison map

$$f : C'_k(x, \alpha, \mathbf{B}) \longrightarrow T'_k(x), \quad \lambda_1 \cdots \lambda_k \mapsto \lambda_1 \cdots \lambda_{k-1}.$$

Let Q_1 be the product of all primary primes $\mu \in \mathcal{P}$ dividing abc, and Q_2 the product of all prime $q \mid abc$ with $q \equiv 3 \bmod 4$. For any $\eta = \lambda_1 \cdots \lambda_{k-1} \in T'_k(x)$, denote by $\mathfrak{c}_\eta = 16\mathbf{N}(\eta Q_1)Q_2\mathbb{Z}[I]$. It's easy to see that if β satisfies

- $\mathbf{N}\beta \equiv \alpha_k \bmod 16$;
- $\left[\dfrac{\mathbf{N}\beta}{\mathbf{N}\lambda_i}\right] = B_{ik}$ for all $1 \leqslant i \leqslant k-1$;
- $\left(\dfrac{\mathbf{N}\beta}{q_j}\right) = 1$ for all $1 \leqslant j \leqslant \ell$;
- $\left(\dfrac{\beta}{\delta}\right)_2 = -\left(\dfrac{\eta/\delta}{\delta}\right)_2$, where $\delta = \lambda_1^{s_1} \cdots \lambda_k^{s_k}$,

then so is $\beta' \equiv \beta \bmod 16\mathbf{N}(\eta Q_1)Q_2$. Denote by

$$\mathscr{A}_\eta \subseteq (\mathbb{Z}[I]/\mathfrak{c}_\eta)^\times$$

the classes of such β. Then η lies in the image of f if and only if there exists $\theta \in \mathcal{P}$ such that $\mathbf{N}\lambda_{k-1} < \mathbf{N}\theta \leqslant x/\mathbf{N}\eta$ and $\theta \bmod \mathfrak{c}_\eta \in \mathscr{A}_\eta$ by noting that $s_k = 0$.

Lemma 5.8. *Let $\chi_1, \chi_2 : G \to \mathbb{F}_2$ be two different non-trivial quadratic characters on a finite group G. Then the size of $\chi_1^{-1}(i) \cap \chi_2^{-1}(j)$ is $\#G/4$ for any $i, j \in \mathbb{F}_2$.*

Proof. Note that the assumption implies that $\#G \geqslant 2$. The sizes of $\chi_1^{-1}(i)$ and $\chi_2^{-1}(j)$ are $\#G/2$. Since $\chi_1 \neq \chi_2$, these two sets always have a common element, which means that $(\chi_1, \chi_2) : G \to \mathbb{F}_2^2$ is surjective. The result then follows. ☐

Lemma 5.9. *Assume that $\pi \in \mathcal{P}$ and $p = \mathbf{N}\pi$. Then $\left(\dfrac{x}{\pi}\right)_2$ and $\left(\dfrac{\mathbf{N}x}{p}\right)$ are different non-trivial quadratic characters on $\big(\mathbb{Z}[I]/p\mathbb{Z}[I]\big)^\times$.*

Proof. Since $\mathbf{N} : \big(\mathbb{Z}[I]/p\mathbb{Z}[I]\big)^\times \to (\mathbb{Z}/p\mathbb{Z})^\times$ is surjective, $\left(\dfrac{\mathbf{N}x}{p}\right)$ is non-trivial. Let $\gamma \in \mathbb{Z}[I]$ be an element such that $\pi\gamma \equiv 1 \bmod \overline{\pi}$. Let $x = \overline{\pi\gamma} + \alpha\pi\gamma$ for some $\alpha \in \mathbb{Z}$ coprime to p. Then

$$\left(\frac{x}{\pi}\right)_2 = \left(\frac{\overline{\pi\gamma}}{\pi}\right)_2 = 1.$$

Denote by $A = (\pi\gamma)^2 + (\overline{\pi\gamma})^2$. Then $\mathbf{N}(x) \equiv \alpha A \bmod p$ and

$$\left(\frac{\mathbf{N}x}{p}\right) = \left(\frac{\alpha A}{p}\right).$$

Hence $\left(\frac{x}{\pi}\right)_2 \neq \left(\frac{\mathbf{N}x}{p}\right)$ by taking $\left(\frac{\alpha}{p}\right) = -\left(\frac{A}{p}\right)$. □

Lemma 5.10. *Let $\varphi(\eta)$ be the cardinality of $G = (\mathbb{Z}[I]/\mathfrak{c}_\eta)^\times$. Then*

$$\#\mathscr{A}_\eta = 2^{-k-\ell-4}\varphi(\eta).$$

Proof. By the Chinese Remainder Theorem, we have a natural isomorphism

$$G \cong \left(\frac{\mathbb{Z}[I]}{16\mathbb{Z}[I]}\right)^\times \times \prod_{i=1}^{k-1}\left(\frac{\mathbb{Z}[I]}{\mathbf{N}\lambda_i\mathbb{Z}[I]}\right)^\times \times \prod_{\mu\mid Q_1}\left(\frac{\mathbb{Z}[I]}{\mathbf{N}\mu\mathbb{Z}[I]}\right)^\times \times \prod_{q\mid Q_2}\left(\frac{\mathbb{Z}[I]}{q\mathbb{Z}[I]}\right)^\times$$
$$\beta \mapsto (\beta_0, \beta_1, \cdots, \beta_{k-1}, \beta'_\mu, \beta'_q).$$

Then $\beta \in \mathscr{A}_\eta$ if and only if

(1) $\beta_0 \equiv 1 \bmod 2+2I$ and $\mathbf{N}\beta_0 \equiv \alpha_k \bmod 16$;
(2) $\left[\frac{\mathbf{N}\beta_i}{\mathbf{N}\lambda_i}\right] = B_{ik}$ for all $1 \leqslant i \leqslant k-1$;
(3) $\left(\frac{\mathbf{N}\beta'_\mu}{\mathbf{N}\mu}\right) = 1$ for all $\mu \mid Q_1$;
(4) $\left(\frac{\mathbf{N}\beta'_q}{q}\right) = 1$ for all $q \mid Q_2$;
(5) $\prod_{s_i=1}\left(\frac{\beta_i}{\lambda_i}\right)_2 = -\left(\frac{\eta/\delta}{\delta}\right)_2$.

(1) selects $\frac{1}{4}\times\frac{1}{4}$ number of elements in $\left(\mathbb{Z}[I]/16\mathbb{Z}[I]\right)^\times$. Note that $\left(\mathbb{Z}[I]/\lambda_i\mathbb{Z}[I]\right)^\times \cong (\mathbb{Z}/\mathbf{N}\lambda_i\mathbb{Z})^\times$, each conditions in (2)–(4) select half as many elements in each corresponding component.

To treat (5), we choose $\beta_1, \cdots, \beta_{k-1}$ as follows. Since $s_k = 0$, there is some $s_j = 1$ for $1 \leqslant j \leqslant k-1$. For $i = 1, 2, \cdots, j-1, j+1, \cdots, k-1$, we choose $\beta_i \in \left(\mathbb{Z}[I]/N\lambda_i\mathbb{Z}[I]\right)^\times$ satisfying (2), and there are half number of $\left(\mathbb{Z}[I]/N\lambda_i\mathbb{Z}[I]\right)^\times$ choices. With above chosen $\beta_1, \cdots, \beta_{j-1}, \beta_{j+1}, \cdots, \beta_{k-1}$, applying Lemmas 5.8 and 5.9 to $\pi = \lambda_j$, (5) and $\left[\frac{\mathbf{N}\beta_j}{\mathbf{N}\lambda_j}\right] = B_{jk}$ selects $\frac{1}{4}$ number of elements in $\left(\mathbb{Z}[I]/N\lambda_j\mathbb{Z}[I]\right)^\times$. Hence

$$\frac{\#\mathscr{A}_\eta}{\varphi(\eta)} = \frac{1}{16} \times \frac{1}{2^{k-1}} \times \frac{1}{2^\ell} \times \frac{1}{2} = 2^{-k-\ell-4}.$$ □

For any $\eta \in T'_k(x)$, denote by $h(\eta)$ the number of primes $\theta \in \mathcal{P}$ such that $\mathbf{N}\lambda_{k-1} < \mathbf{N}\theta \leqslant x/\mathbf{N}\eta$ and $\theta \bmod \mathfrak{c}_\eta \in \mathscr{A}_\eta$. Then we have

$$\#C'_k(x, \alpha, \mathbf{B}) = \sum_{\eta \in T'_k(x)} h(\eta). \tag{5.8}$$

Denote by

$$M_1 = (\log x)^{100} \quad \text{and} \quad M_2 = \exp\left(\frac{\log x}{(\log\log x)^{100}}\right).$$

We will use

$$\sum_{\mathbf{N}\eta\in S}^{*}$$

to denote a summation over $\eta \in T'_k(x)$ with $\mathbf{N}\eta \in S$.

Lemma 5.11. *We have*

$$\begin{aligned}\sum_{20<\mathbf{N}\eta\leqslant M_1}^{*} \mathrm{Li}(x/\mathbf{N}\eta) &= o\Big(\frac{x(\log\log x)^{k-1}}{\log x}\Big),\\ \sum_{M_2<\mathbf{N}\eta\leqslant x^{\frac{k-1}{k}}}^{*} \mathrm{Li}(x/\mathbf{N}\eta) &= o\Big(\frac{x(\log\log x)^{k-1}}{\log x}\Big),\\ \sum_{M_1<\mathbf{N}\eta\leqslant M_2}^{*} \mathrm{Li}(x/\mathbf{N}\eta) &\sim \frac{\#T'_k(x)}{k-1}\log\log x.\end{aligned}$$

Proof. The proof is similar to [CO89, Lemma 3.1]. □

Denote by $\pi(x)$ the number of prime ideals in $\mathbb{Z}[I]$ with norm less than or equal x. Then the prime ideal theorem over $\mathbb{Z}[I]$ tells $\pi(x) \sim \mathrm{Li}(x)$. Certainly, $h(\eta) \leqslant \pi(x/\mathbf{N}\eta)$. Then we have

$$\begin{aligned}\sum_{\mathbf{N}\eta\leqslant 20}^{*} h(\eta) &\ll \mathrm{Li}(x),\\ \sum_{20<\mathbf{N}\eta\leqslant M_1}^{*} h(\eta) &= o\Big(\frac{x(\log\log x)^{k-1}}{\log x}\Big),\\ \sum_{M_2<\mathbf{N}\eta\leqslant x^{\frac{k-1}{k}}}^{*} h(\eta) &= o\Big(\frac{x(\log\log x)^{k-1}}{\log x}\Big)\end{aligned} \tag{5.9}$$

by Lemma 5.11. If $\mathbf{N}\eta > x^{\frac{k-1}{k}}$, then $\mathbf{N}\lambda_{k-1} > x^{\frac{1}{k}}$ and $x/\mathbf{N}\eta < x^{\frac{1}{k}} < \mathbf{N}\lambda_{k-1}$. Therefore, $h(\eta) = 0$ and

$$\sum_{x^{\frac{k-1}{k}}<\mathbf{N}\eta\leqslant x}^{*} h(\eta) = 0. \tag{5.10}$$

Denote by $\pi'(y, \mathscr{B}, \mathfrak{a})$ the number of primes $\theta \in \mathbb{Z}[I]$ such that $\mathbf{N}\theta \leqslant y$ and $\theta \bmod \mathfrak{a} \in \mathscr{B} \subseteq \big(\mathbb{Z}[I]/\mathfrak{a}\big)^{\times}$. Since $\theta \in \mathcal{P}$ has positive imaginary part, we have

$$h(\eta) = \frac{1}{2}\Big(\pi'(x/\mathbf{N}\eta, \mathscr{A}_\eta, \mathfrak{c}_\eta) - \pi'(\mathbf{N}\lambda_{k-1}, \mathscr{A}_\eta, \mathfrak{c}_\eta)\Big) + O(\sqrt{x}).$$

Here the error term originates from $-p$ with $p \equiv 3 \bmod 4$ rational prime, and the implicit constant is absolute. By (5.8), (5.9), (5.10) and the facts that

$$\sum_{M_1<\mathbf{N}\eta\leqslant M_2}^{*} \pi'(\mathbf{N}\lambda_{k-1}, \mathscr{A}_\eta, \mathfrak{c}_\eta) \ll M_2\mathrm{Li}(M_2) = o\Big(\frac{x(\log\log x)^{k-1}}{\log x}\Big)$$

and M_2 is of much small order than $x^{\frac{1}{4}}$, we obtain

$$\#C'_k(x,\alpha,B) \sim \frac{1}{2} \sideset{}{^*}\sum_{M_1<\mathbf{N}\eta\leqslant M_2} \pi'(x/\mathbf{N}\eta, \mathscr{A}_\eta, \mathfrak{c}_\eta) \tag{5.11}$$

with error term $o\big(\#C_k(x)\big)$.

By [Lan94, Theorem 6.1], we have an exact sequence

$$1 \longrightarrow \mathbb{Z}[I]^\times \longrightarrow (\mathbb{Z}[I]/\mathfrak{c}_\eta)^\times \xrightarrow{\Phi} I(\mathfrak{c}_\eta)/P_{\mathfrak{c}_\eta} \longrightarrow 1 \tag{5.12}$$

where $\Phi(\gamma) = (\gamma) \bmod P_{\mathfrak{c}_\eta}$. Denote by $\pi(y,\mathscr{B},\mathfrak{c})$ the number of prime ideals $\mathfrak{p}$ such that $\mathbf{N}\mathfrak{p} \leqslant y$ and $\mathfrak{p} \bmod P_\mathfrak{c} \in \mathscr{B} \subseteq I(\mathfrak{c})/P_\mathfrak{c}$. Denote by $\mathscr{T}_\eta = \Phi(\mathscr{A}_\eta)$. Then

$$\pi'(y,\mathscr{A}_\eta,\mathfrak{c}_\eta) = \pi(y,\mathscr{T}_\eta,\mathfrak{c}_\eta) \qquad \text{and} \qquad \#\mathscr{A}_\eta = \#\mathscr{T}_\eta \tag{5.13}$$

by noting that every prime ideal in a class of $\mathscr{T}$ corresponds to exactly one primary prime element.

Define

$$\psi(y,\mathscr{B},\mathfrak{c}) = \sum_{\substack{\mathbf{N}\mathfrak{a}\leqslant y\\ \mathfrak{a} \bmod P_\mathfrak{c} \in \mathscr{B}}} \Lambda(\mathfrak{c}).$$

Then we have the standard asymptotic relation $\psi(y,\mathscr{B},\mathfrak{c}) \sim \log y \cdot \pi(y,\mathscr{B},\mathfrak{c})$.

Therefore,

$$2\log x \cdot \#C'_k(x,\alpha,B) \sim \sideset{}{^*}\sum_{M_1<\mathbf{N}\eta\leqslant M_2} \psi(x/\mathbf{N}\eta, \mathscr{T}_\eta, \mathfrak{c}_\eta) \tag{5.14}$$

by (5.11) and (5.13). By the orthogonality of characters and the exact sequence (5.12), we get

$$\psi(y,\mathscr{T}_\eta,\mathfrak{c}_\eta) = \frac{4}{\varphi(\eta)} \sum_\chi \psi(y,\chi) \sum_{\mathfrak{a} \bmod P_{\mathfrak{c}_\eta} \in \mathscr{T}_\eta} \overline{\chi(\mathfrak{a})},$$

where χ runs over all characters of $I(\mathfrak{c}_\eta)/P_{\mathfrak{c}_\eta}$ and

$$\psi(y,\chi) = \sum_{\mathbf{N}\mathfrak{a}\leqslant y} \Lambda(\mathfrak{a})\chi(\mathfrak{a}).$$

Therefore,

$$2\log x \cdot \#C'_k(x,\alpha,B) \sim S_1 + S_2, \tag{5.15}$$

where

$$S_1 = \sideset{}{^*}\sum_{M_1<\mathbf{N}\eta\leqslant M_2} \frac{4\#\mathscr{T}_\eta}{\varphi(\eta)} \psi(x/\mathbf{N}\eta, \chi_0),$$
$$S_2 = \sideset{}{^*}\sum_{M_1<\mathbf{N}\eta\leqslant M_2} \frac{4}{\varphi(\eta)} \sum_{\chi\neq\chi_0} \psi(x/\mathbf{N}\eta,\chi) \sum_{\mathfrak{a} \bmod P_{\mathfrak{c}_\eta} \in \mathscr{T}_\eta} \overline{\chi(\mathfrak{a})}.$$

The main term is

$$\begin{aligned}
S_1 &= 2^{-k-\ell-2} \sideset{}{^*}\sum_{M_1<\mathbf{N}\eta\leqslant M_2} \psi(x/\mathbf{N}\eta,\chi_0) \qquad \text{by Lemma 5.10 and (5.13)}\\
&\sim 2^{-k-\ell-2} \sideset{}{^*}\sum_{M_1<\mathbf{N}\eta\leqslant M_2} \log(x/\mathbf{N}\eta)\mathrm{Li}(x/\mathbf{N}\eta)\\
&\sim 2^{-k-\ell-2}\log x \sideset{}{^*}\sum_{M_1<\mathbf{N}\eta\leqslant M_2} \mathrm{Li}(x/\mathbf{N}\eta)\\
&\sim \frac{\log x\cdot\log\log x}{(k-1)\cdot 2^{k+\ell+2}}\cdot \#T_k'(x) \qquad \text{by Lemma 5.11}\\
&\sim \frac{\log x\cdot\log\log x}{(k-1)\cdot 2^{k\ell+3k+\binom{k}{2}}}\cdot \#C_{k-1}(x) \qquad \text{by Lemma 5.6 and (5.7)}\\
&\sim 2^{-k\ell-3k-\binom{k}{2}}\log x\cdot \#C_k(x) \qquad \text{by (1.1)}.
\end{aligned}$$

By (5.14) and Lemma 5.5, this theorem is reduced to showing that S_2 is an error term.

Denote by $\mathfrak{f}$ the conductor of the exceptional primitive conductor with $Z = 256M_2$ in Page Theorem 5.4. Then $S_2 = S_3 + S_4$, where

$$S_3 = \sideset{}{^*}\sum_{\substack{M_1<\mathbf{N}\eta\leqslant M_2\\ \mathfrak{f}\mid\mathfrak{c}_\eta}} \frac{4}{\varphi(\eta)} \sum_{\chi\neq\chi_0} \psi(x/\mathbf{N}\eta,\chi) \sum_{\mathfrak{a} \bmod P_{\mathfrak{c}_\eta}\in\mathscr{T}_\eta} \overline{\chi(\mathfrak{a})},$$

$$S_4 = \sideset{}{^*}\sum_{\substack{M_1<\mathbf{N}\eta\leqslant M_2\\ \mathfrak{f}\nmid\mathfrak{c}_\eta}} \frac{4}{\varphi(\eta)} \sum_{\chi\neq\chi_0} \psi(x/\mathbf{N}\eta,\chi) \sum_{\mathfrak{a} \bmod P_{\mathfrak{c}_\eta}\in\mathscr{T}_\eta} \overline{\chi(\mathfrak{a})}.$$

We have

$$\begin{aligned}
S_3 &\ll \sideset{}{^*}\sum_{\substack{M_1<\mathbf{N}\eta\leqslant M_2\\ \mathfrak{f}\mid\mathfrak{c}_\eta}} \psi(x/\mathbf{N}\eta,\chi_0) \ll x \sideset{}{^*}\sum_{\substack{M_1<\mathbf{N}\eta\leqslant M_2\\ \mathfrak{f}\mid\mathfrak{c}_\eta}} (\mathbf{N}\eta)^{-1}\\
&= \frac{x}{\mathbf{N}\mathfrak{f}} \sum_{M_1<t\mathbf{N}\mathfrak{f}\leqslant M_2} t^{-1} \sideset{}{^*}\sum_{\substack{\mathfrak{f}\mid\mathfrak{c}_\eta\\ \mathbf{N}\eta=t\mathbf{N}\mathfrak{f}}} 1 \ll \frac{x\log M_2}{\mathbf{N}\mathfrak{f}}.
\end{aligned}$$

By the Page Theorem 5.4 for $Z = 256M_2$, there is a positive constant c_6 such that the Siegel zero β of the primitive character with modulus $\mathfrak{f}$ has the property

$$\beta > 1 - \frac{c_6}{\log 256M_2}.$$

By the Siegel Theorem 5.3 for $F = \mathbb{Q}(I)$, there is a constant $c_4 = c_4(2, 1/200) > 0$ such that

$$\beta \leqslant 1 - c_4(4\mathbf{N}\mathfrak{f})^{-1/200}.$$

Therefore, $\mathbf{N}\mathfrak{f} \gg (\log M_2)^{100}$ and $S_3 \ll x(\log M_2)^{-99}$ is an error term.

Since there is no Siegel zero in S_4, we can apply the explicit formula (5.6) with $T = (\mathbf{N}\eta)^4$ to all the $\psi(x/\mathbf{N}\eta, \chi)$ in S_4. Then we obtain

$$\begin{aligned}\psi(x/\mathbf{N}\eta,\chi) \ll & x(\mathbf{N}\eta)^{-1}(\log x)^2 \exp\Big(-\frac{c_7\log(x/\mathbf{N}\eta)}{\log \mathbf{N}\eta}\Big) \\ & + x(\mathbf{N}\eta)^{-5}(\log x)^2 + x^{1/4}(\mathbf{N}\eta)^{-1/4}\log(x/\mathbf{N}\eta)\end{aligned}$$

and $S_4 \ll S_5 + S_6 + S_7$, where

$$\begin{aligned} S_5 = & \sideset{}{^*}\sum_{\substack{M_1<\mathbf{N}\eta\leqslant M_2\\ \mathfrak{f}\dagger\mathfrak{c}_\eta}} x(\mathbf{N}\eta)^{-1}(\log x)^2 \exp\Big(-\frac{c_7\log(x/\mathbf{N}\eta)}{\log\mathbf{N}\eta}\Big), \\ & \ll x(\log x)^2\exp\big(-c_8(\log\log x)^{100}\big)\cdot \sideset{}{^*}\sum_{\substack{M_1<\mathbf{N}\eta\leqslant M_2\\ \mathfrak{f}\dagger\mathfrak{c}_\eta}} (\mathbf{N}\eta)^{-1} \\ & \ll x(\log x)^3\exp\big(-c_8(\log\log x)^{100}\big), \\ S_6 = & \sideset{}{^*}\sum_{\substack{M_1<\mathbf{N}\eta\leqslant M_2\\ \mathfrak{f}\dagger\mathfrak{c}_\eta}} x(\mathbf{N}\eta)^{-5}(\log x)^2 \ll x(\log x)^2 M_1^{-3} \ll x(\log x)^{-200}, \\ S_7 = & \sideset{}{^*}\sum_{\substack{M_1<\mathbf{N}\eta\leqslant M_2\\ \mathfrak{f}\dagger\mathfrak{c}_\eta}} x^{1/4}(\mathbf{N}\eta)^{-1/4}\log(x/\mathbf{N}\eta) \ll x^{1/4}\log x\cdot M_2^{3/4} \ll x^{1/2}.\end{aligned}$$

Hence S_4 is also an error term. This finishes the proof. □

6. Distribution result

Assume that $\mathrm{Sel}_2(E/\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^2$. Let $n = p_1\cdots p_k$ be an element in $\mathscr{Q}_k(x)$ with $p_1 < \cdots < p_k$. Then $n \in \mathscr{P}_k(x)$ if and only if $h_4(n) = 1$ and $h_8(n) \equiv \frac{d-1}{4} \bmod 2$, where d is a certain divisor of n. As shown in the proof of Theorem 1.1(B), the rank of $\mathbf{A} = \mathbf{A}_n$ is $k-1$ or $k-2$.

Assume that $\operatorname{rank}\mathbf{A} = k-2$. As shown in the proof of Theorem 1.1(B), $h_4(n) = 1$ if and only if $\mathbf{b}_2 \notin \operatorname{Im}\mathbf{A}$. In this case, $d = p_1^{s_1}\cdots p_k^{s_k} \equiv 5 \bmod 8$, where $\operatorname{Ker}\mathbf{A} = \{\mathbf{0},\mathbf{1},\mathbf{d},\mathbf{d}+\mathbf{1}\}$ and $\mathbf{d} = (s_1,\dots,s_k)^{\mathrm{T}}$. We may assume that $s_k = 0$. By [JY11, Theorem 3.3(ii)], $h_8(n) = 1$ if and only if

$$\Big(\frac{d}{d'}\Big)_4\Big(\frac{d'}{d}\Big)_4 = -1, \tag{6.1}$$

where $d' = n/d$.

Assume that $\operatorname{rank}\mathbf{A} = k-1$. Then $h_4(n) = 1$, $\mathbf{b}_2 \in \operatorname{Im}\mathbf{A}$ and $d = p_1^{s_1}\cdots p_k^{s_k}$, where $\mathbf{A}\mathbf{d} = \mathbf{b}_2$ and $\mathbf{d} = (s_1,\cdots,s_k)^{\mathrm{T}}$. By [JY11, Theorem 3.3(iii), (iv)], $h_8(n) = 1$ if and only if

$$\Big(\frac{2d}{d'}\Big)_4\Big(\frac{2d'}{d}\Big)_4 = (-1)^{\frac{n-1}{8}}$$

where $d' = n/d$.

Proof of Theorem 1.3. For $k \geqslant 2$, let $\mathscr{B}$ be the set of all symmetric $\mathbf{B} \in M_k(\mathbb{F}_2)$ with rank $k-2$ and $\mathbf{B}\mathbf{1} = \mathbf{0}$. Let $\mathscr{I}$ be the set of all vectors $\alpha = (\alpha_1,\dots,\alpha_k)$ with $\alpha_i \in \{1,5,9,13\}$ and $\alpha_1\cdots\alpha_k \equiv 1 \bmod 8$. Denote by $\mathscr{I}_\mathbf{B}$ the set of all $\alpha \in \mathscr{I}$ such that $\mathbf{b}(\alpha) \notin \operatorname{Im}\mathbf{B}$, where $\mathbf{b}(\alpha) = \Big(\Big[\frac{2}{\alpha_1}\Big],\dots,\Big[\frac{2}{\alpha_k}\Big]\Big)^{\mathrm{T}}$. Since $\alpha_1\cdots\alpha_k \equiv 1 \bmod 8$, we have $\mathbf{b}(\alpha)^{\mathrm{T}}\mathbf{1} = 0$. For any $\mathbf{B} \in \mathscr{B}$ and $\alpha \in \mathscr{I}_{\mathbf{B}}$, $C_k(x, \alpha, \mathbf{B})$ is the set of all $n = p_1 \cdots p_k \in \mathscr{P}_k(x)$ satisfying

- $p_1 < \cdots < p_k$ and $\mathbf{A}_n = \mathbf{B}$;
- $p_i \equiv \alpha_i \bmod 16$ for all $1 \leqslant i \leqslant k$;
- $\left(\dfrac{p_i}{q_j}\right) = 1$ for all $1 \leqslant i \leqslant k$ and $1 \leqslant j \leqslant \ell$

by (6.1). Moreover, if $\mathbf{B} \in \mathscr{B}$ and $\alpha \notin \mathscr{I}_{\mathbf{B}}$, then $C_k(x, \alpha, \mathbf{B}) \cap \mathscr{P}_k(x) = \emptyset$. Therefore, the number $N_1(x)$ of those $n \in \mathscr{P}_k(x)$ with $\operatorname{rank} \mathbf{A}_n = k - 2$ is

$$N_1(x) = \sum_{\mathbf{B} \in \mathscr{B}} \sum_{\alpha \in \mathscr{I}_{\mathbf{B}}} \#C_k(x, \alpha, \mathbf{B}) \sim 2^{-k\ell - 3k - 1 - \binom{k}{2}} \cdot \#C_k(x) \cdot \sum_{\mathbf{B} \in \mathscr{B}} \#\mathscr{I}_{\mathbf{B}} \tag{6.2}$$

by Theorem 5.7.

Now we count the number of $\mathscr{I}_{\mathbf{B}}$ with given $\mathbf{B}$. Given $\mathbf{b} = (b_1, \cdots, b_k)^{\mathrm{T}} \notin \operatorname{Im} \mathbf{B}$ with $\mathbf{b}^{\mathrm{T}}\mathbf{1} = 0$, the number of α with $\mathbf{b}(\alpha) = \mathbf{b}$ is 2^k. This is because $\alpha_i = 1, 9$ if $b_i = 0$ and $\alpha_i = 5, 13$ if $b_i = 1$. Since $\mathbf{B}$ is symmetric and $\mathbf{B1} = \mathbf{0}$, the size of $\operatorname{Im} \mathbf{B} \subset \mathscr{H}_n := \left\{\mathbf{u} : \mathbf{1}^{\mathrm{T}}\mathbf{u} = 0\right\}$ is 2^{k-2}. If $\mathbf{b}^{\mathrm{T}}\mathbf{1} = 0$ and $\operatorname{rank}(\mathbf{B}, \mathbf{b}) = k - 1$, then $\mathbf{b} \in \mathscr{H}_n - \operatorname{Im} \mathbf{B}$ has 2^{k-2} choices. Consequently, $\#\mathscr{I}_{\mathbf{B}} = 2^{2k-2}$ and then

$$N_1(x) \sim 2^{-k\ell - k - 3 - \binom{k}{2}} \cdot \#C_k(x) \cdot \#\mathscr{B}.$$

Proposition 6.1 ([BCJ+06]). *Denote by $\mathscr{B}_{k,r}$ the set of $k \times k$ symmetric matrices over $\mathbb{F}_2$ with rank r. Then*

$$\#\mathscr{B}_{k,r} = u_{r+1} 2^{\binom{r+1}{2}} \cdot \prod_{i=0}^{k-r-1} \frac{2^k - 2^i}{2^{k-r} - 2^i},$$

where u_i is defined in Theorem 1.3.

The left-top minor of $\mathbf{B}$ of order $k - 1$ induces a bijection $\mathscr{B} \to \mathscr{B}_{k-1,k-2}$. So $\#\mathscr{B} = \#\mathscr{B}_{k-1,k-2}$ and we get

$$N_1(x) \sim 2^{-k\ell - k - 3}(1 - 2^{1-k}) u_{k-1} \cdot \#C_k(x).$$

The number $N_2(x)$ of $n \in \mathscr{P}_k(x)$ with $\operatorname{rank} \mathbf{A}_n = k - 1$ can be obtained similarly:

$$N_2(x) \sim 2^{-k - k\ell - 2} u_k \cdot \#C_k(x).$$

We refer to our previous paper [Wan17] for more details. This finishes the proof of this theorem. □

Acknowledgement. The first author is supported by the National Natural Science Foundation of China (Grant No. 11801344) and Natural Science Foundation of Shaanxi Province (Grant No. 2020JQ-401). The second author is supported by the National Natural Science Foundation of China (Grant No. 12001510). The authors are greatly indebted to Professor Ye Tian for many instructions and suggestions.

References

[BCJ+06] Morgan V. Brown, Neil J. Calkin, Kevin James, Adam J. King, Shannon Lockard, and Robert C. Rhoades. Trivial Selmer groups and even partitions of a graph. *Integers*, 6:A33, 17, 2006.

[Cas98] J. W. S. Cassels. Second descents for elliptic curves. *J. Reine Angew. Math.*, 494:101–127, 1998. Dedicated to Martin Kneser on the occasion of his 70th birthday.

[CO89] J. E. Cremona and R. W. K. Odoni. Some density results for negative Pell equations; an application of graph theory. *J. London Math. Soc. (2)*, 39(1):16–28, 1989.

[Dav80] Harold Davenport. *Multiplicative number theory*, volume 74 of *Graduate Texts in Mathematics*. Springer-Verlag, New York-Berlin, second edition, 1980. Revised by Hugh L. Montgomery.

[Fen96] Keqin Feng. Non-congruent numbers, odd graphs and the Birch-Swinnerton-Dyer conjecture. *Acta Arith.*, 75(1):71–83, 1996.

[Fog61] E. Fogels. On the zeros of Hecke's L-functions. I. *Acta Arith.*, 7(2):87–106, 1961.

[Fog63] E. Fogels. Über die Ausnahmenullstelle der Heckeschen L-Funktionen. *Acta Arith.*, 8:307–309, 1963.

[Fuj98] Masahiko Fujiwara. θ-congruent numbers. In *Number theory (Eger, 1996)*, pages 235–241. de Gruyter, Berlin, 1998.

[HB94] D. R. Heath-Brown. The size of Selmer groups for the congruent number problem. II. *Invent. Math.*, 118(2):331–370, 1994. With an appendix by P. Monsky.

[Hec81] Erich Hecke. *Lectures on the theory of algebraic numbers*, volume 77 of *Graduate Texts in Mathematics*. Springer-Verlag, New York-Berlin, 1981. Translated from the German by George U. Brauer, Jay R. Goldman and R. Kotzen.

[HR95] Jeffrey Hoffstein and Dinakar Ramakrishnan. Siegel zeros and cusp forms. *Internat. Math. Res. Notices*, 6:279–308, 1995.

[IK04] Henryk Iwaniec and Emmanuel Kowalski. *Analytic number theory*, volume 53 of *American Mathematical Society Colloquium Publications*. American Mathematical Society, Providence, RI, 2004.

[IR90] Kenneth Ireland and Michael Rosen. *A classical introduction to modern number theory*, volume 84 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1990.

[JY11] Hwanyup Jung and Qin Yue. 8-ranks of class groups of imaginary quadratic number fields and their densities. *J. Korean Math. Soc.*, 48(6):1249–1268, 2011.

[Lan09] Edmund Landau. Handbuch der Lehre von der Verteilung der Primzahlen. Teubner, 1909.

[Lan18] Edmund Landau. Über Ideale und Primideale in Idealklassen. *Math. Z.*, 2(1-2):52–154, 1918.

[Lan94] Serge Lang. *Algebraic number theory*, volume 110 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1994.

[LT00] Delang Li and Ye Tian. On the Birch-Swinnerton-Dyer conjecture of elliptic curves $E_D\colon y^2 = x^3 - D^2x$. *Acta Math. Sin. (Engl. Ser.)*, 16(2):229–236, 2000.

[Maz77] B. Mazur. Modular curves and the Eisenstein ideal. *Inst. Hautes Études Sci. Publ. Math.*, 47:33–186 (1978), 1977. With an appendix by Mazur and M. Rapoport.

[Maz78] B. Mazur. Rational isogenies of prime degree (with an appendix by D. Goldfeld). *Invent. Math.*, 44(2):129–162, 1978.

[Ono96] Ken Ono. Euler's concordant forms. *Acta Arith.*, 78(2):101–123, 1996.

[OZ14] Yi Ouyang and ShenXing Zhang. On non-congruent numbers with 1 modulo 4 prime factors. *Sci. China Math.*, 57(3):649–658, 2014.

[OZ15] Yi Ouyang and Shenxing Zhang. On second 2-descent and non-congruent numbers. *Acta Arith.*, 170(4):343–360, 2015.

[Rei34] L. Rédei. Arithmetischer Beweis des Satzes über die Anzahl der durch vier teilbaren Invarianten der absoluten Klassengruppe im quadratischen Zahlkörper. *J. Reine Angew. Math.*, 171:55–60, 1934.

[Rho09] Robert C. Rhoades. 2-Selmer groups and the Birch-Swinnerton-Dyer conjecture for the congruent number curves. *J. Number Theory*, 129(6):1379–1391, 2009.

[Sil09] Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer, Dordrecht, second edition, 2009.

[Wan16] Zhang Jie Wang. Congruent elliptic curves with non-trivial Shafarevich-Tate groups. *Sci. China Math.*, 59(11):2145–2166, 2016.

[Wan17] Zhang Jie Wang. Congruent elliptic curves with non-trivial Shafarevich-Tate groups: distribution part. *Sci. China Math.*, 60(4):593–612, 2017.

School of Mathematics and statistics, Shaanxi Normal University, Xi'an 710119, China
Email address: zhangjiewang@snnu.edu.cn

School of Mathematics, Hefei University of Technology, Hefei, Anhui 230000, China
Email address: zhangshenxing@hfut.edu.cn