ON NON-CONGRUENT NUMBERS AS MULTIPLES OF NON-CONGRUENT NUMBERS

SHENXING ZHANG

ABSTRACT. Let $n = PQ$ be a square-free positive integer, where P is a product of primes congruent to 1 mod 8, and Q is a non-congruent number with a trivial 2-primary Shafarevich-Tate group. Under certain conditions on the Legendre symbols $\left(\frac{q}{p}\right)$ for primes $p \mid P, q \mid Q$, we establish a criteria characterizing when n is non-congruent with a minimal or a second minimal 2-primary Shafarevich-Tate group. We also provide a sufficient condition for n to be non-congruent with a larger 2-primary Shafarevich-Tate group. These results involve the class groups and tame kernels of quadratic fields.

1. INTRODUCTION

1.1. **Background.** A square-free positive integer n is called *congruent* if it is the area of a right triangle with rational lengths. This is equivalent to say, the Mordell-Weil rank of E_n over $\mathbb{Q}$ is positive, where

$$E_n : y^2 = x^3 - n^2 x$$

is the associated congruent elliptic curve. Denote by $\mathrm{Sel}_2(E_n)$ the 2-*Selmer group* of E_n over $\mathbb{Q}$ and

$$s_2(n) := \dim_{\mathbb{F}_2} \left(\frac{\mathrm{Sel}_2(E_n)}{E_n(\mathbb{Q})[2]} \right) = \dim_{\mathbb{F}_2} \mathrm{Sel}_2(E_n) - 2$$

the *pure* 2-*Selmer rank*. Then

$$s_2(n) = \mathrm{rank}_{\mathbb{Z}} E_n(\mathbb{Q}) + \dim_{\mathbb{F}_2} Ш(E_n)[2]$$

by the exact sequence

$$0 \to E_n(\mathbb{Q})/2E_n(\mathbb{Q}) \to \mathrm{Sel}_2(E_n) \to Ш(E_n)[2] \to 0,$$

where $Ш(E_n)$ is the Shafarevich-Tate group of $E_n/\mathbb{Q}$.

Certainly, $s_2(n) = 0$ implies that n is non-congruent with $Ш(E_n)[2^\infty] = 0$. The examples of $s_2(n) = 0$ can be found in [Fen97], [Isk96] and [OZ15], which are corollaries of Monsky's formula (2.8) for $s_2(n)$. This case is fully characterized in terms of the 2-primary class groups of imaginary quadratic fields, and the full Birch-Swinnerton-Dyer conjecture holds, see [TYZ17, Theorem 1.1, Corollary 1.3] and [Smi16, Theorem 1.2].

Date: July 14, 2025.

2020 *Mathematics Subject Classification.* Primary 14H52; Secondary 11G05, 11R11, 11R29, 11R70.

Key words and phrases. non-congruent number; descent method; elliptic curve; class group; tame kernel; Tate-Shafarevich group.

The examples of non-congruent n with $Ш(E_n)[2^\infty] \cong (\mathbb{Z}/2\mathbb{Z})^2$ can be found in [LT00], [OZ14], [OZ15] and [Zha23]. Denote by

$$r_{2^a}(A) = \dim_{\mathbb{F}_2}\Big(\frac{2^{a-1}A}{2^aA}\Big) \tag{1.1}$$

the 2^a-rank of a finite abelian group A. Denote by $h_{2^a}(m)$ the 2^a-rank of the narrow class group $\mathcal{A}_m$ of the quadratic field $\mathbb{Q}(\sqrt{m})$. Denote by $(a,b)_v$ the Hilbert symbol.

Theorem 1.1 ([Wan16, Theorem 1.1]). *Let $n = p_1 \cdots p_k \equiv 1 \bmod 8$ be a square-free positive integer with prime factors p_i such that $p_i \equiv 1 \bmod 4$ for all i. The following are equivalent:*

- *n is non-congruent with $Ш(E_n)[2^\infty] \cong (\mathbb{Z}/2\mathbb{Z})^2$;*
- *$h_4(-n) = 1$ and $h_8(-n) \equiv (d-1)/4 \bmod 2$,*

where d is a positive divisor of n such that either $(d,-n)_v = 1, \forall v, d \neq 1, n$, or $(2d,-n)_v = 1, \forall v$.

Theorem 1.2 ([WZ22, Theorem 1.1]). *Let $n = p_1 \cdots p_k \equiv 1 \bmod 8$ be a square-free positive integer with prime factors p_i such that $p_i \equiv \pm 1 \bmod 8$ for all i. The following are equivalent:*

- *n is non-congruent with $Ш(E_n)[2^\infty] \cong (\mathbb{Z}/2\mathbb{Z})^2$;*
- *$h_4(-n) = 1, h_8(-n) = 0$.*

Theorem 1.3 ([Zha23, Theorem 5.3]). *Let $n = p_1 \cdots p_k \equiv 1 \bmod 8$ be a square-free positive integer with prime factors p_i such that $p_i \equiv \pm 1 \bmod 8$ for all i. The following are equivalent:*

- *$2n$ is non-congruent with $Ш(E_{2n})[2^\infty] \cong (\mathbb{Z}/2\mathbb{Z})^2$;*
- *$h_4(-n) = 1$ and $d \equiv 9 \bmod 16$,*

where d is the unique divisor of n such that $(d,n)_v = 1, \forall v$ and $d \neq 1, d \equiv 1 \bmod 4$.

The condition that $d \equiv 9 \bmod 16$ is equivalent to $h_8(-n) + h_8(-2n) = 1$, see Proposition 2.9. This recovers [LQ23, Theorem 1.6].

Qin in [Qin22, Theorem 1.5] proved that if $p \equiv 1 \bmod 8$ is a prime with trivial 8-rank of the tame kernel $K_2\mathcal{O}_{\mathbb{Q}(\sqrt{p})}$, then p is non-congruent. Moreover, if the 4-rank of $K_2\mathcal{O}_{\mathbb{Q}(\sqrt{p})}$ is 1, then $Ш(E_p/\mathbb{Q})[2^\infty] \cong (\mathbb{Z}/4\mathbb{Z})^2$.

1.2. **Main results.** In this paper, we want to construct non-congruent numbers n with the form $n = PQ$, where

- P is a product of different primes $\equiv 1 \bmod 8$,
- Q is a non-congruent number prime to P, such that $Ш(E_Q)[2^\infty] = 0$.

Denote the prime decomposition of n by

$$n = \gcd(2,Q)p_1 \cdots p_k q_1 \cdots q_\ell,$$

where $P = p_1 \cdots p_k, Q = \gcd(2,Q)q_1 \cdots q_\ell$. Assume that there exists two vectors

$$\mathbf{u} = (u_1, \dots, u_k)^{\mathrm{T}} \in \mathbb{F}_2^k \quad \text{and} \quad \mathbf{v} = (v_1, \dots, v_\ell)^{\mathrm{T}} \in \mathbb{F}_2^\ell$$

such that the Legendre symbol $\big(\frac{p_i}{q_j}\big) = (-1)^{u_iv_j}$. Denote by

$$\mathbf{U}_P = \operatorname{diag}\{u_1, \dots, u_k\} \quad \text{and} \quad \mathbf{A}_P = (a_{ij})_{k\times k}$$

matrices defined over $\mathbb{F}_2$, such that the Hilbert symbol $(p_j, -P)_{p_i} = (-1)^{a_{ij}}$.

1.2.1. $s_2(n) = 0$.

Theorem 1.4. *Assume that* $\sum_{i=1}^k u_i = 0, \sum_{j=1}^\ell v_j = 1$, $p_1 \equiv \cdots \equiv p_k \equiv 1 \bmod 8$ *and* Q *is non-congruent with* $Ш(E_Q)[2^\infty] = 0$. *The following are equivalent:*

- n *is non-congruent with* $Ш(E_n) = 0$;
- $\mathbf{A}_P + \mathbf{U}_P$ *is invertible.*

1.2.2. $s_2(n) = 2$.

Theorem 1.5. *Assume that* $\sum_{i=1}^k u_i = 0, \sum_{j=1}^\ell v_j = 1$, $p_1 \equiv \cdots \equiv p_k \equiv 1 \bmod 8$ *and* Q *is non-congruent with* $Ш(E_Q)[2^\infty] = 0$. *The following are equivalent:*

- n *is non-congruent with* $Ш(E_n) \cong (\mathbb{Z}/2\mathbb{Z})^2$;
- $\mathrm{corank}(\mathbf{A}_P + \mathbf{U}_P) = 1$ *and* $\left(\frac{\gamma}{d}\right) = -\left(\frac{\sqrt{2}+1}{d}\right)$,

where $d \neq 1$ *is a positive divisor of* P *such that* $(d, -P)_{p_i} = (-1)^{u_i}, \forall p_i \mid d$; $(d, -P)_{p_i} = 1, \forall p_i \mid \frac{P}{d}$, *and* (α, β, γ) *is a primitive positive solution of* $d\alpha^2 + \frac{n}{d}\beta^2 = 4\gamma^2$.

Here, a *primitive positive solution* of $d\alpha^2 + \frac{n}{d}\beta^2 = 4\gamma^2$ is an integer solution such that $\alpha, \beta, \gamma > 0$ and $\gcd(\alpha, \beta, \gamma) = 1$.

When $\mathbf{u} = \mathbf{0}$, we obtain the following result:

Corollary 1.6. *Assume that* $\left(\frac{p_i}{q_j}\right) = 1, \forall i, j$, $p_1 \equiv \cdots \equiv p_k \equiv 1 \bmod 8$ *and* Q *is non-congruent with* $Ш(E_Q)[2^\infty] = 0$. *The following are equivalent:*

- n *is non-congruent with* $Ш(E_n) \cong (\mathbb{Z}/2\mathbb{Z})^2$;
- $h_4(-P) = 1$ *and* $\left(\frac{\gamma}{P}\right) = (-1)^{h_8(-P)}$;
- $h_4(-P) = 1$ *and* $\left(\frac{\gamma}{P}\right) = (-1)^{r_4(K_2\mathcal{O}_{\mathbb{Q}(\sqrt{P})})}$,

where (α, β, γ) *is a primitive positive solution of* $P\alpha^2 + Q\beta^2 = 4\gamma^2$.

When $\ell = 0$, we obtain the following results, which are special cases of Theorems 1.1,1.2 and 1.3.

Corollary 1.7. *Let* $n = p_1 \cdots p_k$ *be a square-free integer where* $p_1 \equiv \cdots \equiv p_k \equiv 1 \bmod 8$.

(1) The following are equivalent:
  - n *is non-congruent with* $Ш(E_n) \cong (\mathbb{Z}/2\mathbb{Z})^2$;
  - $h_4(-n) = 1$ *and* $h_8(-n) = 0$;
  - $r_4(K_2\mathcal{O}_{\mathbb{Q}(\sqrt{n})}) = 0$.

(2) The following are equivalent:
  - $2n$ *is non-congruent with* $Ш(E_{2n}) \cong (\mathbb{Z}/2\mathbb{Z})^2$;
  - $h_4(-n) = 1$ *and* $h_8(-n) + h_8(-2n) = 1$;
  - $r_4(K_2\mathcal{O}_{\mathbb{Q}(\sqrt{-2n})}) = 0$.

1.2.3. *General case.*

Theorem 1.8. *Assume that* $\left(\frac{p_i}{q_j}\right) = 1, \forall i, j$, $p_1 \equiv \cdots \equiv p_k \equiv 1 \bmod 8$ *and* Q *is non-congruent with* $Ш(E_Q)[2^\infty] = 0$. *If there is a decomposition* $P = f_1 \cdots f_r$ *such that*

- $h_4(-f_i) = 1, \forall i$;
- $\left(\frac{p}{p'}\right) = 1$ *for any* $i \neq j$ *and prime factors* $p \mid f_i, p' \mid f_j$;
- $\left(\frac{\gamma_i}{f_j}\right) = 1$ *if* $i \neq j$; $\left(\frac{\gamma_i}{f_i}\right) = (-1)^{h_8(-f_i)}$,

then n is non-congruent with $Ш(E_n) \cong (\mathbb{Z}/2\mathbb{Z})^{2r}$, where $(\alpha_i, \beta_i, \gamma_i)$ is a primitive positive solution of $f_i\alpha_i^2 + \frac{n}{f_i}\beta_i^2 = 4\gamma_i^2$.

When $\ell = 0$, we obtain the following results, where (1) is just [Wan16, Theorem 1.2].

Corollary 1.9. *Let $n = p_1 \cdots p_k$ be a square-free integer where $p_1 \equiv \cdots \equiv p_k \equiv 1 \bmod 8$.*

(1) If there is a decomposition $n = f_1 \cdots f_r$ such that
  - $h_4(-f_i) = 1, h_8(-f_i) = 0, \forall i$;
  - $h_8(-n) = r$, *or* $h_8(-n) = r - 1$ *and* $[(2, \sqrt{-n})] \notin \mathcal{A}_{-n}^4$;
  - $\left(\frac{p}{p'}\right) = 1$ *for any* $i \neq j$ *and prime factors* $p \mid f_i, p' \mid f_j$,

  then n is non-congruent with $Ш(E_n) \cong (\mathbb{Z}/2\mathbb{Z})^{2r}$.

(2) If there is a decomposition $n = f_1 \cdots f_r$ such that
  - $h_4(-f_i) = 1, h_8(-f_i) = 0, \forall i$;
  - $h_8(-2n) = r$;
  - $\left(\frac{p}{p'}\right) = 1$ *for any* $i \neq j$ *and prime factors* $p \mid f_i, p' \mid f_j$,

  then $2n$ is non-congruent with $Ш(E_{2n}) \cong (\mathbb{Z}/2\mathbb{Z})^{2r}$.

Let's sketch the proof of these results. Since the congruent elliptic curve E_n has full rational 2-torsion, the pure 2-Selmer group $\mathrm{Sel}_2'(E_n) := \mathrm{Sel}_2(E_n)/E_n(\mathbb{Q})[2]$ can be identified with a set of triples $(d_1, d_2, d_3) \in (\mathbb{Q}^\times/\mathbb{Q}^{\times 2})^3$, where d_1, d_2, d_3 may be taken as square-free integers. The local conditions for Selmer elements translate into certain quadratic residue conditions, which in turn correspond to the 4-ranks of class groups of associated quadratic fields. As established in [Wan16], $E_n(\mathbb{Q})$ is finite with $Ш(E_n)[2^\infty] \cong (\mathbb{Z}/2\mathbb{Z})^{s_2(n)}$ if and only if the Cassels pairing on $\mathrm{Sel}_2'(E_n)$ is non-degenerate. This condition can be expressed in terms of the 8-ranks of class groups and the 4-ranks of tame kernels of associated quadratic fields.

1.3. **Notations.** Denote by
- $\gcd(m, n)$ the greatest common divisor of integers m, n, where $m \neq 0$ or $n \neq 0$;
- $(a, b)_v$ the Hilbert symbol;
- $[a, b]_v$ the additive Hilbert symbol, i.e., the image of $(a, b)_v$ under the isomorphism $\{\pm 1\} \xrightarrow{\sim} \mathbb{F}_2$;
- $\left(\frac{a}{b}\right) = \prod_{p \mid b}(a, b)_p$ the Jacobi symbol, where $\gcd(a, b) = 1$ and $b > 0$;
- $\left[\frac{a}{b}\right]$ the additive Jacobi symbol, i.e., the image of $\left(\frac{a}{b}\right)$ under the isomorphism $\{\pm 1\} \xrightarrow{\sim} \mathbb{F}_2$;
- v_p the normalized valuation on $\mathbb{Q}_p$;
- $\mathbf{0} = (0, \ldots, 0)^{\mathrm{T}}$ and $\mathbf{1} = (1, \ldots, 1)^{\mathrm{T}}$;
- $r_{2^a}(A)$ the 2^a-rank of a finite abelian group A, see (1.1);

If n is a square-free positive integer, then we denote by
- $E_n : y^2 = x^3 - n^2 x$ the congruent elliptic curve associated to n;
- $\mathrm{Sel}_2(E_n)$ the 2-Selmer group of $E_n/\mathbb{Q}$;
- $Ш(E_n)$ the Shafarevich-Tate group of $E_n/\mathbb{Q}$;
- $\mathrm{Sel}_2'(E_n) := \mathrm{Sel}_2(E_n)/E_n(\mathbb{Q})[2]$ the pure 2-Selmer group of $E_n/\mathbb{Q}$;
- $s_2(n) = \dim_{\mathbb{F}_2} \mathrm{Sel}_2'(E_n)$ the pure 2-Selmer rank of E_n.

If n is odd with a fixed ordered prime decomposition $n = p_1 \cdots p_k$, then we denote by

- $\mathbf{A}_n = \big([p_j, -n]_{p_i}\big)_{k\times k}$ a matrix associated to n, see (2.2);
- $\mathbf{D}_{n,\varepsilon} = \operatorname{diag}\big\{\big[\frac{\varepsilon}{p_1}\big], \dots, \big[\frac{\varepsilon}{p_k}\big]\big\}$ a matrix associated to n and ε, see (2.3);
- $\mathbf{b}_{n,\varepsilon} = \mathbf{D}_{n,\varepsilon}\mathbf{1} = \big(\big[\frac{\varepsilon}{p_1}\big], \dots, \big[\frac{\varepsilon}{p_k}\big]\big)^{\mathrm{T}}$;
- $\mathbf{M}_n$ (resp. $\mathbf{M}_{2n}$) the Monsky matrix of E_n (resp. E_{2n}), see (2.4) and (2.6);
- $\psi_n(d) = \big(v_{p_1}(d), \dots, v_{p_k}(d)\big)^{\mathrm{T}}$ a vector over $\mathbb{F}_2$ associated to $0 < d \mid n$.

If $m \neq 0, 1$ is a square-free integer, then we denote by

- $F_m = \mathbb{Q}(\sqrt{m})$ a quadratic field;
- $\mathbf{R}_m$ the Rédei matrix of F_m, with a submatrix $\mathbf{R}'_m$, see (2.9) and (2.12);
- $\mathcal{A}_m$ the narrow class group of F_m;
- D_m the discriminant of F_m;
- $\omega_m = (D_m + \sqrt{D_m})/2$;
- $\mathcal{O}_m = \mathbb{Z} + \mathbb{Z}\omega_m$ the ring of integers of F_m;
- $\mathscr{D}_m$ the set of all square-free positive divisors of D_m;
- $\theta_m : \mathscr{D}_m \to \mathcal{A}_m[2]$ a two-to-one onto homomorphism, see Proposition 2.2;
- $h_{2^a}(m)$ the 2^a-rank of $\mathcal{A}_m$;
- $K_2\mathcal{O}_m$ the tame kernel of F_m;
- $\mathbf{B}_m = \mathbf{A}_n + \mathbf{D}_{n,m/n}$ a matrix associated to m, where n is the odd part of $|m|$.

2. Preliminaries

2.1. **The Monsky matrix.** By the 2-descent method, Monsky in [HB94, Appendix] represented the pure 2-Selmer group

$$\mathrm{Sel}'_2(E_n) := \frac{\mathrm{Sel}_2(E_n)}{E_n(\mathbb{Q})[2]}$$

as the kernel of a matrix $\mathbf{M}_n$ over $\mathbb{F}_2$. Let's recall it roughly. One can identify $\mathrm{Sel}_2(E_n)$ with

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

where D_Λ is a genus one curve defined by

$$\begin{cases} H_1: & -nt^2 + d_2u_2^2 - d_3u_3^2 = 0, \\ H_2: & -nt^2 + d_3u_3^2 - d_1u_1^2 = 0, \\ H_3: & 2nt^2 + d_1u_1^2 - d_2u_2^2 = 0. \end{cases} \tag{2.1}$$

Under this identification, $O, (n,0), (-n,0), (0,0)$ and other point $(x,y) \in E_n(\mathbb{Q})$ correspond to $(1,1,1), (2,2n,n), (-2n,2,-n), (-n,n,-1)$ and $(x-n, x+n, x)$ respectively.

Let n be an odd positive square-free integer with an ordered prime decomposition $n = p_1 \cdots p_k$. Denote by

$$\mathbf{A}_{2n} = \mathbf{A}_n := (a_{ij})_{k\times k} \quad \text{where} \quad a_{ij} = [p_j, -n]_{p_i} = \begin{cases} \big[\frac{p_j}{p_i}\big], & i \neq j; \\ \big[\frac{n/p_i}{p_i}\big], & i = j, \end{cases} \tag{2.2}$$

and

$$\mathbf{D}_{n,\varepsilon} := \operatorname{diag}\Big\{\Big[\frac{\varepsilon}{p_1}\Big], \dots, \Big[\frac{\varepsilon}{p_k}\Big]\Big\}. \tag{2.3}$$

Then $\mathbf{A}_n\mathbf{1} = \mathbf{0}$ and $\operatorname{corank} \mathbf{A}_n \geq 1$.

Monsky showed that each element in $\mathrm{Sel}_2'(E_n)$ can be represented as (d_1, d_2, d_3), where d_1, d_2, d_3 are all positive divisors of n. The system D_Λ is locally solvable everywhere if and only if certain conditions on the Hilbert symbols hold. Then we can express $\mathrm{Sel}_2'(E_n)$ as the kernel of the *Monsky matrix*

$$\mathbf{M}_n := \begin{pmatrix} \mathbf{A}_n + \mathbf{D}_{n,2} & \mathbf{D}_{n,2} \\ \mathbf{D}_{n,2} & \mathbf{A}_n + \mathbf{D}_{n,-2} \end{pmatrix} \tag{2.4}$$

via the isomorphism

$$\begin{aligned} \mathrm{Sel}_2'(E_n) &\to \operatorname{Ker} \mathbf{M}_n \\ (d_1, d_2, d_3) &\mapsto \begin{pmatrix} \psi_n(d_2) \\ \psi_n(d_1) \end{pmatrix}, \end{aligned} \tag{2.5}$$

where $\psi_n(d) := \big(v_{p_1}(d), \ldots, v_{p_k}(d)\big)^{\mathrm{T}} \in \mathbb{F}_2^k$ for any positive divisor d of n.

Similarly, each element in $\mathrm{Sel}_2'(E_{2n})$ can be represented as (d_1, d_2, d_3), where d_1, d_2, d_3 are all divisors of n and $d_2 > 0, d_3 \equiv 1 \bmod 4$. Then we can express $\mathrm{Sel}_2'(E_{2n})$ as the kernel of the *Monsky matrix*

$$\mathbf{M}_{2n} := \begin{pmatrix} \mathbf{A}_n^{\mathrm{T}} + \mathbf{D}_{n,2} & \mathbf{D}_{n,-1} \\ \mathbf{D}_{n,2} & \mathbf{A}_n + \mathbf{D}_{n,2} \end{pmatrix} \tag{2.6}$$

via the isomorphism

$$\begin{aligned} \mathrm{Sel}_2'(E_{2n}) &\to \operatorname{Ker} \mathbf{M}_{2n} \\ (d_1, d_2, d_3) &\mapsto \begin{pmatrix} \psi_n(|d_3|) \\ \psi_n(d_2) \end{pmatrix}. \end{aligned} \tag{2.7}$$

In both cases, we have

$$s_2(n) := \dim_{\mathbb{F}_2} \mathrm{Sel}_2'(E_n) = \operatorname{corank} \mathbf{M}_n. \tag{2.8}$$

2.2. **The Cassels pairing.** Cassels in [Cas98] defined a (skew-)symmetric bilinear pairing $\langle -, - \rangle$ on the $\mathbb{F}_2$-vector space $\mathrm{Sel}_2'(E_n)$. For any $\Lambda \in \mathrm{Sel}_2(E_n)$, the equation H_i in (2.1) is locally solvable everywhere. Thus H_i is solvable over $\mathbb{Q}$ by the Hasse-Minkowski principal. Choose $Q_i \in H_i(\mathbb{Q})$ and let L_i be a linear form such that $L_i = 0$ defines the tangent plane of H_i at Q_i. For any $\Lambda' = (d_1', d_2', d_3') \in \mathrm{Sel}_2(E_n)$, define the *Cassels pairing*

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

where $P_v \in D_\Lambda(\mathbb{Q}_v)$ for each place v of $\mathbb{Q}$. This pairing is independent of the choice of P_v, Q_i and the representative Λ. It is (skew-)symmetric and satisfies $\langle \Lambda, \Lambda \rangle = 0$.

Lemma 2.1 ([Cas98, Lemma 7.2])**.** *The local Cassels pairing $\langle -, - \rangle_v = 0$ if*

- *$v \nmid 2\infty$,*
- *the coefficients of H_i and L_i are all integral at v for $i = 1, 2, 3$, and*
- *modulo D_Λ and $L_i = 0$ by v, they define a curve of genus 1 over $\mathbb{F}_v$ together with tangents to it.*

2.3. **The narrow class group.** Let $F_m = \mathbb{Q}(\sqrt{m})$ be a quadratic field, where $m \neq 0, 1$ is a square-free integer. We will use the notations introduced in §1.3. Denote by $\mathbf{N} = \mathbf{N}_{F_m/\mathbb{Q}}$ the norm map. Fix an ordered decomposition of the odd part n of $|m|$: $n = p_1 \cdots p_k$. If $2 \mid D$, denote by $p_{k+1} = 2$. Let t be the number of prime factors of D_m. Then the Gauss genus theory tells:

Proposition 2.2 ([Hec81, Chapter 7]). *(1) The map $\theta_m : \mathscr{D}_m \to \mathcal{A}_m[2]$ defined as*

$$\theta_m(d) = [(d, \omega_m)]$$

is a two-to-one onto homomorphism. In particular,

$$h_2(m) = \dim_{\mathbb{F}_2} \mathcal{A}_m[2] = t - 1.$$

(2) Let $\mathfrak{a}$ be a non-zero fractional ideal of F_m. Then the ideal class $[\mathfrak{a}] \in \mathcal{A}_m^2$ if and only if $\mathbf{N}\mathfrak{a} \in \mathbf{N}F_m$.

When $m < 0$, the kernel of θ_m is $\{1, |m|\}$.

To calculate $h_4(m)$, we need the Rédei matrix, which is defined as

$$\mathbf{R}_m = ([p_j, m]_{p_i})_{t \times t}. \tag{2.9}$$

Example 2.3. Let $n = p_1 \cdots p_k$ be an odd positive square-free integer. Denote by

$$\mathbf{b}_{n,\varepsilon} := \left(\left[\frac{\varepsilon}{p_1}\right], \ldots, \left[\frac{\varepsilon}{p_k}\right]\right)^{\mathrm{T}} = \mathbf{D}_{n,\varepsilon}\mathbf{1}.$$

When $n \equiv 1 \bmod 4$, we have

$$\mathbf{R}_n = \mathbf{A}_n + \mathbf{D}_{n,-1}, \qquad \mathbf{R}_{-n} = \begin{pmatrix} \mathbf{A}_n & \mathbf{b}_{n,2} \\ \mathbf{b}_{n,-1}^{\mathrm{T}} & \left[\frac{2}{n}\right] \end{pmatrix},$$

$$\mathbf{R}_{2n} = \begin{pmatrix} \mathbf{A}_n + \mathbf{D}_{n,-2} & \mathbf{b}_{n,2} \\ \mathbf{b}_{n,2}^{\mathrm{T}} & \left[\frac{2}{n}\right] \end{pmatrix}, \qquad \mathbf{R}_{-2n} = \begin{pmatrix} \mathbf{A}_n + \mathbf{D}_{n,2} & \mathbf{b}_{n,2} \\ \mathbf{b}_{n,-2}^{\mathrm{T}} & \left[\frac{2}{n}\right] \end{pmatrix}.$$

When $n \equiv -1 \bmod 4$, we have

$$\mathbf{R}_n = \begin{pmatrix} \mathbf{A}_n + \mathbf{D}_{n,-1} & \mathbf{b}_{n,2} \\ \mathbf{b}_{n,-1}^{\mathrm{T}} & \left[\frac{2}{n}\right] \end{pmatrix}, \qquad \mathbf{R}_{-n} = \mathbf{A}_n,$$

$$\mathbf{R}_{2n} = \begin{pmatrix} \mathbf{A}_n + \mathbf{D}_{n,-2} & \mathbf{b}_{n,2} \\ \mathbf{b}_{n,-2}^{\mathrm{T}} & \left[\frac{2}{n}\right] \end{pmatrix}, \qquad \mathbf{R}_{-2n} = \begin{pmatrix} \mathbf{A}_n + \mathbf{D}_{n,2} & \mathbf{b}_{n,2} \\ \mathbf{b}_{n,2}^{\mathrm{T}} & \left[\frac{2}{n}\right] \end{pmatrix}.$$

One can see that the following are equivalent:

- $d \in \mathscr{D}_m \cap \mathbf{N}F_m$;
- $X^2 - mY^2 = dZ^2$ is solvable over $\mathbb{Q}$;
- the Hilbert symbols $(d, m)_v = 1, \forall v$;
- $\mathbf{R}_m \mathbf{d} = \mathbf{0}$, where $\mathbf{d} = \left(v_{p_1}(d), \ldots, v_{p_t}(d)\right)^{\mathrm{T}}$.

Rédei showed that θ_m induces a two-to-one onto homomorphism

$$\theta_m : \mathscr{D}_m \cap \mathbf{N}F_m \to \mathcal{A}_m[2] \cap \mathcal{A}_m^2, \tag{2.10}$$

which induces that

$$h_4(m) = \operatorname{corank} \mathbf{R}_m - 1. \tag{2.11}$$

Denote by

$$\mathbf{R}'_m = ([p_j, m]_{p_i})_{k \times t}. \tag{2.12}$$

If $2 \mid D_m$, then $\mathbf{R}'_m$ is the submatrix of $\mathbf{R}_m$ by removing the last row; otherwise $\mathbf{R}'_m = \mathbf{R}_m$. Since $\mathbf{1}^{\mathrm{T}}\mathbf{R}_m = \mathbf{0}^{\mathrm{T}}$, we have

$$\operatorname{rank}\mathbf{R}'_m = \operatorname{rank}\mathbf{R}_m. \tag{2.13}$$

See [Rè34] and [LY20, Example 2.6].

The 8-rank $h_8(m)$ can be obtained by the following proposition, which is similar to [Wan16, Proposition 3.6]. See also [JY11, Lu15].

Proposition 2.4. *For any $d \in \mathscr{D}_m \cap \mathbf{N}F_m$, let (α, β, γ) be a primitive positive solution of*

$$d\alpha^2 - \frac{m}{d}\beta^2 = 4\gamma^2.$$

Then

(1) *$\theta_m(d) \in \mathcal{A}_m^4$ if and only if $\big([\gamma, m]_{p_1}, \dots, [\gamma, m]_{p_t}\big)^{\mathrm{T}} \in \operatorname{Im}\mathbf{R}_m$;*
(2) *$\sum_{i=1}^t [\gamma, m]_{p_i} = 0$.*

In particular, $\theta_m(d) \in \mathcal{A}_m^4$ if and only if $\mathbf{b}_{n,\gamma} \in \operatorname{Im}\mathbf{R}'_m$, where n is the odd part of $|m|$.

Proof. Denote by σ the non-trivial automorphism of $\mathbb{Q}(\sqrt{m})$. If p is an odd prime factor of γ, then $p \nmid m$ and $\left(\frac{m}{p}\right) = 1$. Thus $(p) = \mathfrak{p}\mathfrak{p}^\sigma$ is split in F_m and $[\gamma, m]_p = 0$. We will show that $x = (d\alpha + \beta\sqrt{m})/2 \in \mathcal{O}_m$.

- If d is odd and m is even, then both of α and β are even and $x \in \mathcal{O}_m$.
- If d, m are odd, then α and β have same parities. If moreover both of α and β are odd, then $4 \mid (d - m/d)$, $m \equiv 1 \bmod 4$ and $x \in \mathcal{O}_m$.
- If d is even, then β is even and $x \in \mathcal{O}_m$.

Certainly, x is totally positive and $p \mid d\gamma^2 = \mathbf{N}(x)$. If both $\mathfrak{p}, \mathfrak{p}^\sigma$ divide $x\mathcal{O}_m$, then $p\mathcal{O}_m \mid x\mathcal{O}_m$ and $p \mid \alpha, \beta, \gamma$, which contradicts to $\gcd(\alpha, \beta, \gamma) = 1$. Hence only one of $\mathfrak{p}$ and $\mathfrak{p}^\sigma$ divides $x\mathcal{O}_m$. We may assume that $\mathfrak{p}^\sigma \mid x\mathcal{O}_m$ for each odd $p \mid \gamma$.

Assume that d is odd. If γ is odd, we have

$$x\mathcal{O}_m = \mathfrak{d}\prod_{p \mid \gamma}(\mathfrak{p}^\sigma)^{2v_p(\gamma)} = \gamma^2\mathfrak{d}\mathfrak{c}^{-2}, \quad \text{where } \mathfrak{c} := \prod_{p \mid \gamma}\mathfrak{p}^{v_p(\gamma)} \text{ with } \mathbf{N}\mathfrak{c} = \gamma \tag{2.14}$$

and $\mathfrak{d} = (d, \omega_m)$. If γ is even, one can show that m is odd. Then both of α and β are odd, $8 \mid (d - m/d)$ and $m \equiv 1 \bmod 8$. Thus $2\mathcal{O}_m = \mathfrak{q}\mathfrak{q}^\sigma$ is split in F. Similarly, only one of $\mathfrak{q}$ and $\mathfrak{q}^\sigma$ divides $x\mathcal{O}_m$. We may assume that $\mathfrak{q}^\sigma \mid x\mathcal{O}_m$. Hence we also have (2.14), where $\mathfrak{p}$ is $\mathfrak{q}$ for $p = 2$.

Assume that d is even. Then D_m is even, $m \not\equiv 1 \bmod 4$ and $2\mathcal{O}_m = \mathfrak{q}^2$ is ramified in F. Similarly, we have (2.14), where $\mathfrak{p} = \mathfrak{p}^\sigma = \mathfrak{q}$ for $p = 2$.

(1) By (2.14), we have $[\mathfrak{d}] = [\mathfrak{c}]^2$. Clearly, $[\mathfrak{d}] \in \mathcal{A}_m^4$ if and only if $[\mathfrak{c}] + [(a, \omega_m)] \in \mathcal{A}_m^2$ for some $a \in \mathscr{D}_m$. This is equivalent to $a\mathbf{N}\mathfrak{c} = a\gamma \in \mathbf{N}F_m$ by Proposition 2.2. Note that
   - $[a\gamma, m]_p = 1$ for any odd prime $p \mid \gamma$;
   - $[a\gamma, m]_\infty = 1$ because $a\gamma > 0$;
   - if $2 \nmid D_m$ and γ is odd, then a is odd and $m \equiv 1 \bmod 4$; if $2 \nmid D_m$ and γ is even, then $m \equiv 1 \bmod 8$.

   In other words, $[a\gamma, m]_v = 1$ for all $v \nmid D_m$. Thus $a\gamma \in \mathbf{N}F_m$ if and only if $[a, m]_{p_i} = [\gamma, m]_{p_i}$ for all $p_i \mid D_m$, if and only if

$$\mathbf{R}_m\big(v_{p_1}(a), \dots, v_{p_t}(a)\big)^{\mathrm{T}} = \big([\gamma, m]_{p_1}, \dots, [\gamma, m]_{p_t}\big)^{\mathrm{T}}.$$

(2) Denote by γ_0 the odd part of γ. If $m \not\equiv 1 \bmod 4$, then D_m is even and

$$\sum_{i=1}^{t}[\gamma, m]_{p_i} = \sum_{p|\gamma_0}[\gamma, m]_p = 0.$$

Here, $[\gamma, m]_\infty = 0$ because $\gamma > 0$. If $m \equiv 1 \bmod 4$ and γ is odd, then $[\gamma, m]_2 = 0$; if $m \equiv 1 \bmod 4$ and γ is even, then $m \equiv 1 \bmod 8$ and $[\gamma, m]_2 = 0$, as shown in the proof of (1). Therefore

$$\sum_{i=1}^{t}[\gamma, m]_{p_i} = \sum_{p|\gamma_0}[\gamma_0, m]_p + [\gamma, m]_2 = 0. \qquad \square$$

2.4. **The tame kernel.** Denote by $K_2\mathcal{O}_m$ the tame kernel of F_m. We list the results about 2-rank and 4-rank of $K_2\mathcal{O}_m$ that we will use. Assume that $|m| > 2$.

Theorem 2.5 ([BS82])**.** *The subgroup $K_2\mathcal{O}_m[2]$ is generated by the Steinberg symbols*

- $\{-1, d\}, d \mid m$;
- $\{-1, u + \sqrt{m}\}$, *where $m = u^2 - cw^2$ for some $c = -1, \pm 2$ and $u, w \in \mathbb{N}$.*

Denote by k the number of odd prime factors of m. Then

$$r_2(K_2\mathcal{O}_m) = \begin{cases} k + \log_2 \#\big(\{\pm 1, \pm 2\} \cap \mathbf{N}F_m\big); & \text{if } m > 2; \\ k - 1 + \log_2 \#\big(\{1, 2\} \cap \mathbf{N}F_m\big); & \text{if } m < -2. \end{cases}$$

Theorem 2.6 ([Qin95b, Theorem 3.4])**.** *Suppose that $m > 2$. Denote by V_1 the set of positive $d \mid n$ satisfying: there exists $\varepsilon \in \{\pm 1, \pm 2\}$ such that $(d, -m)_p = \left(\frac{\varepsilon}{p}\right), \forall p \mid n$. If $2 \in \mathbf{N}F_m$, then write $m = 2\mu^2 - \lambda^2, \mu, \lambda \in \mathbb{N}$ and denote by V_2 the set of positive $d \mid n$ satisfying: there exists $\varepsilon \in \{\pm 1\}$ such that $(d, -m)_p = \left(\frac{\varepsilon\mu}{p}\right), \forall p \mid n$. We have*

$$2^{r_4(K_2\mathcal{O}_m)+1} = \#V_1 + \#V_2.$$

Theorem 2.7 ([Qin95a, Theorem 4.1])**.** *Suppose that $m < -2$. Denote by V_1 the set of $d \mid n$ satisfying: there exists $\varepsilon \in \{1, 2\}$ such that $(d, -m)_p = \left(\frac{\varepsilon}{p}\right), \forall p \mid n$. If $2 \in \mathbf{N}F_m$, then write $m = 2\mu^2 - \lambda^2, \mu, \lambda \in \mathbb{N}$ and denote by V_2 the set of $d \mid n$ satisfying: $(d, -m)_p = \left(\frac{\mu}{p}\right), \forall p \mid n$. We have*

$$2^{r_4(K_2\mathcal{O}_m)+2} = \#V_1 + \#V_2.$$

Here, $V_2 = \emptyset$ if $2 \notin \mathbf{N}F_m$.

Let's translate these results into the language of matrices. Denote by n the odd part of $|m|$ and denote by $\mathbf{B}_m = \mathbf{A}_n + \mathbf{D}_{n,m/n}$, where $\mathbf{A}_n$ is defined as (2.2). If $m > 2$, then

$$\#\{\mathbf{x} : \mathbf{B}_m\mathbf{x} = \mathbf{b}_{n,\pm 1}, \mathbf{b}_{n,\pm 2}\} + \#\{\mathbf{x} : \mathbf{B}_m\mathbf{x} = \mathbf{b}_{n,\pm\mu}\} = 2^{r_4(K_2\mathcal{O}_m)+1}. \tag{2.15}$$

If $m < -2$, then

$$\#\{\mathbf{x} : \mathbf{B}_m\mathbf{x} = \mathbf{0}, \mathbf{b}_{n,2}\} + \#\{\mathbf{x} : \mathbf{B}_m\mathbf{x} = \mathbf{b}_{n,\mu}\} = \begin{cases} 2^{r_4(K_2\mathcal{O}_m)+2}, & \text{if } \mathbf{b}_{n,-1} \notin \operatorname{Im}\mathbf{B}_m; \\ 2^{r_4(K_2\mathcal{O}_m)+1}, & \text{if } \mathbf{b}_{n,-1} \in \operatorname{Im}\mathbf{B}_m. \end{cases} \tag{2.16}$$

Theorem 2.8. *Assume that $n = p_1 \cdots p_k$ is an odd positive square-free integer, where all prime factors p_i are congruent to ± 1 modulo 8 and $n \equiv 1 \bmod 8$. Write $n = \lambda^2 - 2\mu^2$ where $\lambda, \mu \in \mathbb{N}$.*

(1) We have $h_4(n)+1=h_4(2n)=h_4(-n)=h_4(-2n)=\operatorname{corank}\mathbf{A}_n$.
(2) If $h_4(-n)=1$, *then* $h_8(-n)=1-\left[\frac{\lambda+\mu}{d}\right]$. *If moreover all* $p_i\equiv 1 \bmod 8$, *then* $h_8(-n)=1-\left[\frac{\sqrt{2}+1}{n}\right]$.
(3) If $h_4(-2n)=1$, *then* $h_8(-2n)=1-\left[\frac{\lambda}{d}\right]$. *If moreover all* $p_i\equiv 1 \bmod 8$, *then* $h_8(-2n)=1-\left[\frac{\sqrt{2}}{n}\right]$.
(4) Assume that all $p_i\equiv 1 \bmod 8$. *We have* $r_4(K_2\mathcal{O}_{-2n})=0$ *if and only if* $h_4(-n)=1, h_8(-n)+h_8(-2n)=1$. *If* $h_4(-n)=1$, *then* $r_4(K_2\mathcal{O}_{-2n})\le 1$.
(5) Assume that all $p_i\equiv 1 \bmod 8$. *We have* $r_4(K_2\mathcal{O}_{n})=0$ *if and only if* $h_4(-n)=1, h_8(-n)=0$. *If* $h_4(-n)=1$, *then* $r_4(K_2\mathcal{O}_{n})\le 1$.

Here, $1<d\mid n$ *such that* $\mathbf{A}_n^{\mathrm{T}}\psi_n(d)=\mathbf{0}$.

Proof. (1) By the quadratic reciprocity law, we have

$$\mathbf{A}_n^{\mathrm{T}}=\mathbf{A}_n+\mathbf{D}_{n,-1}+\mathbf{b}_{n,-1}\mathbf{b}_{n,-1}^{\mathrm{T}}. \tag{2.17}$$

By $\mathbf{b}_{n,-1}^{\mathrm{T}}\mathbf{b}_{n,-1}=\mathbf{b}_{n,-1}^{\mathrm{T}}\mathbf{1}=\left[\frac{-1}{n}\right]=0$, one can show that

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

where $\mathbf{I}+\mathbf{1}\mathbf{b}_{n,-1}^{\mathrm{T}}$ is invertible since $(\mathbf{I}+\mathbf{1}\mathbf{b}_{n,-1}^{\mathrm{T}})^2=\mathbf{I}$. Thus

$$\operatorname{rank}\mathbf{R}_n=\operatorname{rank}\mathbf{R}'_{-n}=\operatorname{rank}\mathbf{R}'_{\pm 2n}=\operatorname{rank}\mathbf{A}_n,$$

which concludes the result by (2.11) and (2.13).

(2) Since $\theta_{-n}(n)=[(\sqrt{-n})]$ is the trivial class, we have

$$\mathcal{A}_{-n}[2]\cap\mathcal{A}_{-n}^2=\{[(1)],\theta_{-n}(2)\},$$

where $\theta_{-n}(2)=\theta_{-n}(2n)$. Note that $(\lambda+2\mu,2,\lambda+\mu)$ is a primitive positive solution of $2\alpha^2+\frac{n}{2}\beta^2=4\gamma^2$. Since $\operatorname{Im}\mathbf{R}'_{-n}=\{\mathbf{x}:\psi(d)^{\mathrm{T}}\mathbf{x}=0\}$, by Proposition 2.4, we have $h_8(-n)=1$ if and only if $\mathbf{b}_{n,\lambda+\mu}\in\operatorname{Im}\mathbf{R}'_{-n}$, if and only if $0=\psi(d)^{\mathrm{T}}\mathbf{b}_{n,\lambda+\mu}=\left[\frac{\lambda+\mu}{d}\right]$.

If all $p_i\equiv 1 \bmod 8$, then $d=n$ since $\mathbf{A}_n^{\mathrm{T}}\mathbf{1}=\mathbf{0}$. Let μ' be the odd part of μ. Then

$$\left[\frac{\mu}{n}\right]=\left[\frac{n}{\mu'}\right]=\left[\frac{\lambda^2-2\mu^2}{\mu'}\right]=0. \tag{2.18}$$

Since $\lambda\equiv\pm\sqrt{2}\mu \bmod p_i$, we have $\left[\frac{\lambda+\mu}{n}\right]=\left[\frac{\sqrt{2}+1}{n}\right]$.

(3) Note that $(2\mu,2,\lambda)$ is a primitive positive solution of $2\alpha^2+n\beta^2=4\gamma^2$. The result follows from arguments similar to (2).

(4) In this case, $\mathbf{B}_{-2n}=\mathbf{A}_n$ and $\mathbf{B}_{-2n}\mathbf{1}=\mathbf{b}_{n,-1}$. Note that

$$m=-2n=2(\lambda+2\mu)^2-(2\lambda+2\mu)^2.$$

By (2.16), $r_4(K_2\mathcal{O}_{-2n})=0$ if and only if $\operatorname{corank}\mathbf{A}_n=1$ and $\mathbf{b}_{n,\lambda+2\mu}\notin\operatorname{Im}\mathbf{A}_n$, if and only if $h_4(-n)=1$ and

$$1=\mathbf{1}^{\mathrm{T}}\mathbf{b}_{n,\lambda+2\mu}=\left[\frac{\lambda+2\mu}{n}\right]=\left[\frac{\sqrt{2}+2}{n}\right]=\left[\frac{\sqrt{2}+1}{n}\right]+\left[\frac{\sqrt{2}}{n}\right],$$

i.e., $h_8(-n)+h_8(-2n)=1$.

If $h_4(-n)=1$, then $\operatorname{corank}\mathbf{A}_n=1$. Thus $\mathbf{A}_n\mathbf{x}=\mathbf{0}$ has two solutions, $\mathbf{A}_n\mathbf{x}=\mathbf{b}_{n,\lambda+2\mu}$ has at most two solutions. Thus implies that $r_4(K_2\mathcal{O}_{-2n})\le 1$ by (2.16).

(5) The proof is similar to (4). $\square$

Proposition 2.9. *Let $n = p_1 \cdots p_k \equiv 1 \bmod 8$ be a square-free positive integer with odd prime factors p_i such that $p_i \equiv \pm 1 \bmod 8$ for all i. If $h_4(-n) = 1$, then*

$$h_8(-n) + h_8(-2n) \equiv \frac{d-1}{8} \bmod 2,$$

where d is the unique divisor of n such that $(d, n)_v = 1, \forall v$ and $d \neq 1, d \equiv 1 \bmod 4$.

Proof. Notice that $d = \left(\frac{-1}{|d|}\right)|d|$ and

$$\begin{aligned} 0 = [d, n]_{p_i} &= [d, -1]_{p_i} + [d, -n]_{p_i} \\ &= [d, -1]_{p_i} + [|d|, -n]_{p_i} + \left[\frac{-1}{|d|}\right][-1, -n]_{p_i} \\ &= [d, -1]_{p_i} + [|d|, -n]_{p_i} + \left[\frac{-1}{|d|}\right]\left[\frac{-1}{p_i}\right], \end{aligned}$$

we have

$$\begin{aligned} \mathbf{0} &= \mathbf{D}_{n,-1}\psi_n(|d|) + \mathbf{A}_n\psi_n(|d|) + \left[\frac{-1}{|d|}\right]\mathbf{b}_{n,-1} \\ &= (\mathbf{A}_n + \mathbf{D}_{n,-1})\psi_n(|d|) + \mathbf{b}_{n,-1}\mathbf{b}_{n,-1}^{\mathrm{T}}\psi_n(|d|) = \mathbf{A}_n^{\mathrm{T}}\psi_n(|d|) \end{aligned}$$

by (2.17). Write $n = \lambda^2 - 2\mu^2$ where $\lambda, \mu \in \mathbb{N}$. By Theorem 2.8 (2) and (3), $h_8(-n) + h_8(-2n) = 1$ if and only if

$$1 = \left[\frac{\lambda(\lambda+\mu)}{|d|}\right] = \left[\frac{1+\mu/\lambda}{|d|}\right] = \left[\frac{2+\sqrt{2}}{|d|}\right],$$

which is equivalent to $d \equiv 9 \bmod 16$ by [Zha23, Lemma 5.4]. □

3. The Selmer groups and the Cassles pairings

Let $n = PQ$ be a square-free positive integer with an ordered prime decomposition

$$n = \gcd(2, n)p_1 \cdots p_k q_1 \cdots q_\ell,$$

where $P = p_1 \cdots p_k, Q = \gcd(2, n)q_1 \cdots q_\ell$. Assume that $p_1 \equiv \cdots \equiv p_k \equiv 1 \bmod 8$ and there exists

$$\mathbf{u} = (u_1, \ldots, u_k)^{\mathrm{T}} \in \mathbb{F}_2^k, \qquad \mathbf{v} = (v_1, \ldots, v_\ell)^{\mathrm{T}} \in \mathbb{F}_2^\ell$$

such that the Legendre symbol $\left[\frac{p_i}{q_j}\right] = u_i v_j$. Clearly,

$$\mathbf{1}^{\mathrm{T}}\mathbf{u} = \sum_{i=1}^{k} u_i \quad \text{and} \quad \mathbf{1}^{\mathrm{T}}\mathbf{v} = \sum_{j=1}^{\ell} v_j.$$

Lemma 3.1. *Assume that $\mathbf{1}^{\mathrm{T}}\mathbf{u} = 0, \mathbf{1}^{\mathrm{T}}\mathbf{v} = 1$, $p_1 \equiv \cdots \equiv p_k \equiv 1 \bmod 8$ and Q is non-congruent with $Ш(E_Q)[2^\infty] = 0$. Then*

$$\operatorname{Ker}\mathbf{M}_n = \left\{ \begin{pmatrix} \mathbf{x} \\ \mathbf{0} \\ \mathbf{z} \\ \mathbf{0} \end{pmatrix} \,\middle|\, \mathbf{x}, \mathbf{z} \in \operatorname{Ker}(\mathbf{A}_P + \mathbf{U}_P) \right\}$$

In particular, $s_2(n) = 2\operatorname{corank}(\mathbf{A}_P + \mathbf{U}_P)$.

Proof. Note that $\mathbf{A}_n\mathbf{1}=\mathbf{0}$ and $\mathbf{A}_P^{\mathrm{T}}=\mathbf{A}_P$. By our assumptions,

$$\mathbf{A}_n=\begin{pmatrix}\mathbf{A}_P+\mathbf{U}_P & \mathbf{u}\mathbf{v}^{\mathrm{T}}\\ \mathbf{v}\mathbf{u}^{\mathrm{T}} & \mathbf{A}_Q\end{pmatrix}\quad\text{and}\quad \mathbf{A}_n^{\mathrm{T}}=\begin{pmatrix}\mathbf{A}_P+\mathbf{U}_P & \mathbf{u}\mathbf{v}^{\mathrm{T}}\\ \mathbf{v}\mathbf{u}^{\mathrm{T}} & \mathbf{A}_Q^{\mathrm{T}}\end{pmatrix}.$$

Note that $\mathbf{D}_{P,\pm 2}=\mathbf{O}_k$. If Q is odd, we have

$$\mathbf{M}_n=\begin{pmatrix}\mathbf{A}_P+\mathbf{U}_P & \mathbf{u}\mathbf{v}^{\mathrm{T}} & \mathbf{O}_k & \\ \mathbf{v}\mathbf{u}^{\mathrm{T}} & \mathbf{A}_Q+\mathbf{D}_{Q,2} & & \mathbf{D}_{Q,2}\\ \mathbf{O}_k & & \mathbf{A}_P+\mathbf{U}_P & \mathbf{u}\mathbf{v}^{\mathrm{T}}\\ & \mathbf{D}_{Q,2} & \mathbf{v}\mathbf{u}^{\mathrm{T}} & \mathbf{A}_Q+\mathbf{D}_{Q,-2}\end{pmatrix}.$$

If Q is even, we have

$$\mathbf{M}_n=\begin{pmatrix}\mathbf{A}_P+\mathbf{U}_P & \mathbf{u}\mathbf{v}^{\mathrm{T}} & \mathbf{O}_k & \\ \mathbf{v}\mathbf{u}^{\mathrm{T}} & \mathbf{A}_Q^{\mathrm{T}}+\mathbf{D}_{Q,2} & & \mathbf{D}_{Q,-1}\\ \mathbf{O}_k & & \mathbf{A}_P+\mathbf{U}_P & \mathbf{u}\mathbf{v}^{\mathrm{T}}\\ & \mathbf{D}_{Q,2} & \mathbf{v}\mathbf{u}^{\mathrm{T}} & \mathbf{A}_Q+\mathbf{D}_{Q,2}\end{pmatrix}.$$

If

$$\begin{pmatrix}\mathbf{x}\\ \mathbf{y}\\ \mathbf{z}\\ \mathbf{w}\end{pmatrix}\in\operatorname{Ker}\mathbf{M}_n,$$

then

$$(\mathbf{A}_P+\mathbf{U}_P)\mathbf{x}=\mathbf{u}\mathbf{v}^{\mathrm{T}}\mathbf{y},\qquad (\mathbf{A}_P+\mathbf{U}_P)\mathbf{z}=\mathbf{u}\mathbf{v}^{\mathrm{T}}\mathbf{w}$$

and

$$\mathbf{M}_Q\begin{pmatrix}\mathbf{y}\\ \mathbf{w}\end{pmatrix}=\begin{pmatrix}\mathbf{v}\mathbf{u}^{\mathrm{T}}\mathbf{x}\\ \mathbf{v}\mathbf{u}^{\mathrm{T}}\mathbf{z}\end{pmatrix}.$$

Since $\mathbf{A}_P=\mathbf{A}_P^{\mathrm{T}}$, we have $\mathbf{1}^{\mathrm{T}}\mathbf{A}_P=\mathbf{0}^{\mathrm{T}}$ and

$$0=\mathbf{1}^{\mathrm{T}}\mathbf{u}\mathbf{v}^{\mathrm{T}}\mathbf{y}=\mathbf{1}^{\mathrm{T}}(\mathbf{A}_P+\mathbf{U}_P)\mathbf{x}=\mathbf{1}^{\mathrm{T}}\mathbf{U}_P\mathbf{x}=\mathbf{u}^{\mathrm{T}}\mathbf{x}.\tag{3.1}$$

Similarly, $\mathbf{u}^{\mathrm{T}}\mathbf{z}=0$. Thus

$$\mathbf{M}_Q\begin{pmatrix}\mathbf{y}\\ \mathbf{w}\end{pmatrix}=\mathbf{0}.$$

Since $s_2(Q)=0$, $\mathbf{M}_Q$ is invertible and we have $\mathbf{y}=\mathbf{w}=\mathbf{0}$. Thus $\mathbf{x},\mathbf{z}\in\operatorname{Ker}(\mathbf{A}_P+\mathbf{U}_P)$,

$$\operatorname{Ker}\mathbf{M}_n=\left\{\begin{pmatrix}\mathbf{x}\\ \mathbf{0}\\ \mathbf{z}\\ \mathbf{0}\end{pmatrix}\,\middle|\,\mathbf{x},\mathbf{z}\in\operatorname{Ker}(\mathbf{A}_P+\mathbf{U}_P)\right\}$$

and $s_2(n)=2\operatorname{corank}(\mathbf{A}_P+\mathbf{U}_P)$. □

Proposition 3.2. *Let f_i,f_j be two positive divisors of P such that $\gcd(f_i,f_j)=1$ and $\psi_P(f_i),\psi_P(f_j)\in\operatorname{Ker}(\mathbf{A}_P+\mathbf{U}_P)$. Denote by*

$$\Lambda_t=(f_t,1,f_t)\quad\textit{and}\quad\Lambda_t'=(f_t,f_t,1)$$

for $t = i, j$. *Then*

$$\langle \Lambda_i', \Lambda_i \rangle = \left[\frac{\sqrt{2}+1}{f_i}\right] + \left[\frac{\gamma_i}{f_i}\right] = \left[\frac{\sqrt{2}+1}{f_i}\right] + \left[\frac{\gamma_i'}{f_i}\right],$$
$$\langle \Lambda_i', \Lambda_j \rangle = \left[\frac{\gamma_i}{f_j}\right] = \left[\frac{\gamma_j'}{f_i}\right],$$
$$\langle \Lambda_i', \Lambda_i' \rangle = \left[\frac{\gamma_i \gamma_i'}{f_i}\right], \qquad \langle \Lambda_i', \Lambda_j' \rangle = \left[\frac{\gamma_i \gamma_i'}{f_j}\right],$$

where $(\alpha_i, \beta_i, \gamma_i)$ $\big($*resp.* $(\alpha_i', \beta_i', \gamma_i')\big)$ *is a primitive positive solution of*

$$f_i \alpha_i^2 + \frac{n}{f_i}\beta_i^2 = 4\gamma_i^2 \qquad \left(\text{resp. } f_i \alpha_i'^2 - \frac{n}{f_i}\beta_i'^2 = 4\gamma_i'^2\right).$$

Proof. Let $(\alpha_i'', \beta_i'', \gamma_i'')$ be a primitive positive solution of $f_i\alpha_i''^2 - \frac{2n}{f_i}\beta_i''^2 = 4\gamma_i''^2$. It's easy to see that $\alpha_i, \beta_i, \gamma_i, \alpha_i', \beta_i', \gamma_i', \alpha_i'', \beta_i'', \gamma_i''$ are coprime to $n/\gcd(2,n)$.

(1) Recall that D_{Λ_i} is defined by

$$\begin{cases} H_1: & -nt^2 + u_2^2 - f_i u_3^2 = 0, \\ H_2: & -\frac{n}{f_i}t^2 + u_3^2 - u_1^2 = 0, \\ H_3: & 2nt^2 + f_i u_1^2 - u_2^2 = 0. \end{cases}$$

Choose

$$Q_1 = (\beta_i', f_i\alpha_i', 2\gamma_i') \in H_1(\mathbb{Q}), \qquad L_1 = \frac{n}{f_i}\beta_i' t - \alpha_i' u_2 + 2\gamma_i' u_3,$$
$$Q_2 = (0, 1, -1) \in H_2(\mathbb{Q}), \qquad L_2 = u_3 + u_1,$$
$$Q_3 = (\beta_i'', 2\gamma_i'', f_i\alpha_i'') \in H_3(\mathbb{Q}), \qquad L_3 = \frac{2n}{f_i}\beta_i'' t + 2\gamma_i'' u_1 - \alpha_i'' u_2.$$

By (3.1), we have $\mathbf{u}^{\mathrm{T}}\psi_P(f_t) = 0$, which implies that

$$\left[\frac{f_t}{q_s}\right] = \sum_{p_r | f_t} u_r v_s = v_s \mathbf{u}^{\mathrm{T}} \psi_P(f_t) = 0. \tag{3.2}$$

If $v = p_s \mid P$, then $\left[\frac{q_t}{p_s}\right] = \left[\frac{p_s}{q_t}\right] = u_s v_t$ and $p_s \equiv 1 \bmod 8$. Thus we have

$$\left[\frac{Q}{p_s}\right] = u_s \mathbf{v}^{\mathrm{T}}\mathbf{1} = u_s.$$

One can see that the s-th entry of the vector $(\mathbf{A}_P + \mathbf{U}_P)\psi_P(f_i)$ is

$$0 = u_s + \sum_{p|f_i}[p, -P]_{p_s} = \left[\frac{Q}{p_s}\right] + [f_i, -P]_{p_s} = \left[\frac{Q}{p_s}\right] + \left[\frac{P/f_i}{p_s}\right] = \left[\frac{n/f_i}{p_s}\right]$$

if $p_s \mid f_i$;

$$0 = \sum_{p|f_i}[p, -P]_{p_s} = [f_i, -P]_{p_s} = \left[\frac{f_i}{p_s}\right]. \tag{3.3}$$

if $p_s \mid \frac{P}{f_i}$.

(i) The case $v = p_s \mid f_i$. Take

$$P_v = (t, u_1, u_2, u_3) = \big(1, \sqrt{-2n/f_i}, 0, \sqrt{-n/f_i}\big).$$

Note that

$$\big(\beta_i'\sqrt{-n/f_i}+2\gamma_i'\big)\big(-\beta_i'\sqrt{-n/f_i}+2\gamma_i'\big)=f_i\alpha_i'^2$$

and one of $\pm\beta_i'\sqrt{-n/f_i}+2\gamma_i'$ is congruent to $4\gamma_i'$ modulo v. Since $[f_i,f_t]_v=0$ for $t=i,j$ by (3.3), we have

$$\big[\pm\beta_i'\sqrt{-n/f_i}+2\gamma_i',f_t\big]_v=[4\gamma_i',f_t]_v.$$

Then

$$\big[L_1(P_v),f_t\big]_v=\big[4\gamma_i'\sqrt{-n/f_i},f_t\big]_v=\big[\gamma_i'\sqrt{-n/f_i},f_t\big]_v.$$

Similarly,

$$\begin{aligned}\big[L_2(P_v),f_t\big]_v&=\big[(\sqrt{2}+1)\sqrt{-n/f_i},f_t\big]_v,\\ \big[L_3(P_v),f_t\big]_v&=\big[4\sqrt{2}\gamma_i''\sqrt{-n/f_i},f_t\big]_v=\big[\sqrt{2}\gamma_i''\sqrt{-n/f_i},f_t\big]_v.\end{aligned}$$

Thus

$$\begin{aligned}\big[L_1L_2(P_v),f_t\big]_v&=\big[(\sqrt{2}+1)\gamma_i',f_t\big]_v,\\ \big[L_1L_3(P_v),f_t\big]_v&=\big[\sqrt{2}\gamma_i'\gamma_i'',f_t\big]_v.\end{aligned}$$

(ii) The case $v=p_s\mid\frac{P}{f_i}$. Take

$$P_v=(t,u_1,u_2,u_3)=\big(0,1,\sqrt{f_i},1\big).$$

Similarly to (i), we have

$$\begin{aligned}\big[L_1(P_v),f_t\big]_v&=[4\gamma_i',f_t]_v=[\gamma_i',f_t]_v,\\ \big[L_2(P_v),f_t\big]_v&=[2,f_t]_v=0,\\ \big[L_3(P_v),f_t\big]_v&=[4\gamma_i'',f_t]_v=[\gamma_i'',f_t]_v,\end{aligned}$$

and then

$$\begin{aligned}\big[L_1L_2(P_v),f_t\big]_v&=[\gamma_i',f_t]_v,\\ \big[L_1L_3(P_v),f_t\big]_v&=[\gamma_i'\gamma_i'',f_t]_v.\end{aligned}$$

By Lemma 2.1 and (3.2), we have

$$\begin{aligned}\langle\Lambda_i,\Lambda_i\rangle&=\sum_{v\mid f_i}\big[\sqrt{2}\gamma_i'\gamma_i'',f_i\big]_v+\sum_{v\mid\frac{P}{f_i}}[\gamma_i'\gamma_i'',f_i]_v=\Big[\frac{\sqrt{2}\gamma_i'\gamma_i''}{f_i}\Big],\\ \langle\Lambda_i,\Lambda_j\rangle&=\sum_{v\mid f_i}\big[\sqrt{2}\gamma_i'\gamma_i'',f_j\big]_v+\sum_{v\mid\frac{P}{f_i}}[\gamma_i'\gamma_i'',f_j]_v=\Big[\frac{\gamma_i'\gamma_i''}{f_j}\Big],\\ \langle\Lambda_i,\Lambda_i'\rangle&=\sum_{v\mid f_i}\big[(\sqrt{2}+1)\gamma_i',f_i\big]_v+\sum_{v\mid\frac{P}{f_i}}[\gamma_i',f_i]_v=\Big[\frac{(\sqrt{2}+1)\gamma_i'}{f_i}\Big],\\ \langle\Lambda_i,\Lambda_j'\rangle&=\sum_{v\mid f_i}\big[(\sqrt{2}+1)\gamma_i',f_j\big]_v+\sum_{v\mid\frac{P}{f_i}}[\gamma_i',f_j]_v=\Big[\frac{\gamma_i'}{f_j}\Big],\end{aligned}\tag{3.4}$$

(2) Recall that $D_{\Lambda_i'}$ is defined by

$$\begin{cases} H_1: & -nt^2 + f_i u_2^2 - u_3^2 = 0, \\ H_2: & -nt^2 + u_3^2 - f_i u_1^2 = 0, \\ H_3: & \frac{2n}{f_i} t^2 + u_1^2 - u_2^2 = 0. \end{cases}$$

Choose

$$\begin{aligned} Q_1 &= (\beta_i, 2\gamma_i, f_i\alpha_i) \in H_1(\mathbb{Q}), & L_1 &= \frac{n}{f_i}\beta_i t - 2\gamma_i u_2 + \alpha_i u_3, \\ Q_2 &= (\beta_i', f_i\alpha_i', 2\gamma_i') \in H_2(\mathbb{Q}), & L_2 &= \frac{n}{f_i}\beta_i' t - \alpha_i' u_3 + 2\gamma_i' u_1, \\ Q_3 &= (0, 1, -1) \in H_3(\mathbb{Q}), & L_3 &= u_1 + u_2. \end{aligned}$$

(i) The case $v \mid f_i$. Take

$$P_v = (t, u_1, u_2, u_3) = \big(1, \sqrt{-n/f_i}, \sqrt{n/f_i}, 0\big).$$

Similarly, we have

$$\begin{aligned} \big[L_1(P_v), f_t\big]_v &= \big[4\gamma_i\sqrt{n/f_i}, f_t\big]_v = \big[\gamma_i\sqrt{n/f_i}, f_t\big]_v, \\ \big[L_2(P_v), f_t\big]_v &= \big[4\gamma_i'\sqrt{-n/f_i}, f_t\big]_v = \big[\gamma_i'\sqrt{-n/f_i}, f_t\big]_v, \\ \big[L_3(P_v), f_t\big]_v &= \big[(\sqrt{-1}+1)\sqrt{n/f_i}, f_t\big]_v, \end{aligned}$$

and then

$$\begin{aligned} \big[L_1L_2(P_v), f_t\big]_v &= \big[\sqrt{-1}\gamma_i\gamma_i', f_t\big]_v = \big[\gamma_i\gamma_i', f_t\big]_v, \\ \big[L_1L_3(P_v), f_t\big]_v &= \big[(\sqrt{-1}+1)\gamma_i, f_t\big]_v = \big[(\sqrt{2}+1)\gamma_i, f_t\big]_v. \end{aligned}$$

Here, we use the fact that

$$\begin{aligned} 4\sqrt{-1} &= (\sqrt{2}+\sqrt{-2})^2, \\ (\sqrt{2}+1)(\sqrt{-1}+1) &= \frac{1}{2}(\sqrt{2}+\sqrt{-1}+1)^2 \end{aligned}$$

are squares in $\mathbb{Q}_v$.

(ii) The case $v \mid \frac{P}{f_i}$. Take

$$P_v = (t, u_1, u_2, u_3) = \big(0, 1, 1, \sqrt{f_i}\big).$$

Similarly, we have

$$\begin{aligned} \big[L_1(P_v), f_t\big]_v &= [-4\gamma_i, f_t]_v = [\gamma_i, f_t]_v, \\ \big[L_2(P_v), f_t\big]_v &= [4\gamma_i', f_t]_v = [\gamma_i', f_t]_v, \\ \big[L_3(P_v), f_t\big]_v &= [2, f_t]_v = 0, \end{aligned}$$

and then

$$\begin{aligned} \big[L_1L_2(P_v), f_t\big]_v &= [\gamma_i\gamma_i', f_t]_v, \\ \big[L_1L_3(P_v), f_t\big]_v &= [\gamma_i, f_t]_v. \end{aligned}$$

By Lemma 2.1 and (3.2), we have

$$\begin{aligned}
\langle \Lambda_i', \Lambda_i' \rangle &= \sum_{v \mid f_i} [\gamma_i\gamma_i', f_i]_v + \sum_{v \mid \frac{P}{f_i}} [\gamma_i\gamma_i', f_i]_v = \left[\frac{\gamma_i\gamma_i'}{f_i}\right], \\
\langle \Lambda_i', \Lambda_j' \rangle &= \sum_{v \mid f_i} [\gamma_i\gamma_i', f_j]_v + \sum_{v \mid \frac{P}{f_i}} [\gamma_i\gamma_i', f_j]_v = \left[\frac{\gamma_i\gamma_i'}{f_j}\right], \\
\langle \Lambda_i', \Lambda_i \rangle &= \sum_{v \mid f_i} \left[(\sqrt{2}+1)\gamma_i, f_i\right]_v + \sum_{v \mid \frac{P}{f_i}} [\gamma_i, f_i]_v = \left[\frac{(\sqrt{2}+1)\gamma_i}{f_i}\right], \\
\langle \Lambda_i', \Lambda_j \rangle &= \sum_{v \mid f_i} \left[(\sqrt{2}+1)\gamma_i, f_j\right]_v + \sum_{v \mid \frac{P}{f_i}} [\gamma_i, f_j]_v = \left[\frac{\gamma_i}{f_j}\right],
\end{aligned} \tag{3.5}$$

Finally, we conclude the results by (3.4) and (3.5). ☐

4. Proof of main theorems

Lemma 4.1. *The following are equivalent:*

- *n is non-congruent with $\text{Ш}(E_n)[2^\infty] \cong (\mathbb{Z}/2\mathbb{Z})^{s_2(n)}$;*
- *the Cassels pairing on $\mathrm{Sel}_2'(E_n)$ is non-degenerate.*

Proof. The proof is due to [Wan16, pp 2146, 2157]. Since

$$0 \to E_n[2] \to E_n[4] \xrightarrow{\times 2} E_n[2] \to 0$$

is exact, we have the long exact sequence

$$0 \to \frac{E_n(\mathbb{Q})[2]}{2E_n(\mathbb{Q})[4]} \to \mathrm{Sel}_2(E_n) \to \mathrm{Sel}_4(E_n) \to \mathrm{Im}\,\mathrm{Sel}_4(E_n) \to 0,$$

where $\mathrm{Im}\,\mathrm{Sel}_4(E_n)$ is the image of $\mathrm{Sel}_4(E_n) \xrightarrow{\times 2} \mathrm{Sel}_2(E_n)$. It's known that the kernel of the Cassels pairing on $\mathrm{Sel}_2(E_n)$ is $\mathrm{Im}\,\mathrm{Sel}_4(E_n)$. Thus

$$\mathrm{rank}_{\mathbb{Z}}\, E_n(\mathbb{Q}) = 0, \quad \text{Ш}(E_n)[2^\infty] \cong (\mathbb{Z}/2\mathbb{Z})^{s_2(n)}$$

if and only if $\#\mathrm{Sel}_2(E_n) = \#\mathrm{Sel}_4(E_n)$, if and only if $\mathrm{Im}\,\mathrm{Sel}_4(E_n) = E_n[2]$ in $\mathrm{Sel}_2(E_n)$, if and only if the Cassels pairing on $\mathrm{Sel}_2'(E_n)$ is non-degenerate. ☐

Proof of Theorem 1.4. It follows from Lemma 3.1 that $s_2(n) = 0$ if and only if $\mathbf{A}_P + \mathbf{U}_P$ is invertible. This concludes the result. ☐

Proof of Theorem 1.5. By Lemma 3.1, $s_2(n) = 2$ if and only if $\mathrm{corank}(\mathbf{A}_P + \mathbf{U}_P) = 1$. Assume that $\mathrm{corank}(\mathbf{A}_P + \mathbf{U}_P) = 1$ from now on. By our assumptions, $\psi_P(d)$ is a non-zero vector lying in $\mathrm{Ker}(\mathbf{A}_P + \mathbf{U}_P)$. Then

$$\mathrm{Ker}\,\mathbf{M}_n = \left\{ \begin{pmatrix}\mathbf{0}\\\mathbf{0}\\\mathbf{0}\\\mathbf{0}\end{pmatrix}, \begin{pmatrix}\mathbf{0}\\\mathbf{0}\\\psi_P(d)\\\mathbf{0}\end{pmatrix}, \begin{pmatrix}\psi_P(d)\\\mathbf{0}\\\mathbf{0}\\\mathbf{0}\end{pmatrix}, \begin{pmatrix}\psi_P(d)\\\mathbf{0}\\\psi_P(d)\\\mathbf{0}\end{pmatrix} \right\}.$$

Thus

$$\mathrm{Sel}_2'(E_n) = \{(1,1,1), (d,1,d), (1,d,d), (d,d,1)\}$$

by (2.5) and (2.7).

Denote by $\Lambda = (d,1,d)$ and $\Lambda' = (d,d,1)$. Then

$$\langle \Lambda, \Lambda' \rangle = \left[\frac{\sqrt{2}+1}{d}\right] + \left[\frac{\gamma}{d}\right]$$

by Proposition 3.2. Hence the Cassels pairing on $\mathrm{Sel}_2'(E_n)$ is non-degenerate if and only if $\left(\frac{\sqrt{2}+1}{d}\right)\left(\frac{\gamma}{d}\right) = -1$. Conclude the results by Lemma 4.1. $\square$

Proof of Corollary 1.6. Take $\mathbf{u} = \mathbf{0}$ and $\mathbf{v} = (1,0,\dots,0)^{\mathrm{T}}$ in Theorem 1.5, we obtain that $\mathbf{U}_P = \mathbf{O}$. Thus $\operatorname{corank}(\mathbf{A}_P + \mathbf{U}_P) = 1$ if and only if $\operatorname{corank} \mathbf{A}_P = 1$, if and only if $h_4(-P) = 1$ by (2.11).

Since $\mathbf{A}_P \mathbf{1} = \mathbf{0}$, the non-zero vector in $\operatorname{Ker} \mathbf{A}_P$ is $\psi_P(d) = \mathbf{1}$. Thus $d = P$ and we conclude the result by Theorem 2.8 (2) and (5). $\square$

Example 4.2. We give two examples to show that our results produce new non-congruent numbers.

(1) Clearly, $\mathbf{M}_3 = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$. Thus $q = 3$ is a non-congruent number with $\text{Ш}(E_3)[2^\infty] = 0$. If $p = 193$, then $\left(\frac{p}{q}\right) = 1$, $\mathbf{A}_p = 0$ and $h_4(-p) = 1$. Since $52^2 \equiv 2 \bmod p$, we have

$$h_8(-p) = 1 - \left[\frac{\sqrt{2}+1}{p}\right] = 1 - \left[\frac{53}{193}\right] = 0.$$

Since $193 \times 1^2 + 3 \times 1^2 = 4 \times 7^2$ and $\left(\frac{7}{p}\right) = 1$, we obtain that $n = pq = 3 \times 193$ is non-congruent with $\text{Ш}(E_n)[2^\infty] \cong (\mathbb{Z}/2\mathbb{Z})^2$ by Corollary 1.6.

(2) Clearly, $\mathbf{M}_{10} = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$. Thus $Q = 2q = 10$ is a non-congruent number with $\text{Ш}(E_{10})[2^\infty] = 0$. If $p = 241 = 23^2 - 2 \times 12^2$, then $\left(\frac{p}{q}\right) = 1$, $\mathbf{A}_p = 0$ and $h_4(-p) = 1$. Since $22^2 \equiv 2 \bmod p$, we have

$$h_8(-p) = 1 - \left[\frac{\sqrt{2}+1}{p}\right] = 1 - \left[\frac{23}{241}\right] = 0.$$

Since $241 \times 2^2 + 10 \times 24^2 = 4 \times 41^2$ and $\left(\frac{41}{p}\right) = 1$, we obtain that $n = 2pq = 10 \times 241$ is non-congruent with $\text{Ш}(E_n)[2^\infty] \cong (\mathbb{Z}/2\mathbb{Z})^2$ by Corollary 1.6.

Proof of Corollary 1.7. (1) Note that $(\alpha, \beta, \gamma) = (4, 2n-2, n+1)$ is a positive primitive solution of $n\alpha^2 + \beta^2 = 4\gamma^2$. Thus $\left[\frac{\gamma}{n}\right] = \left[\frac{n+1}{n}\right] = 0$. This concludes the result by Corollary 1.6 and Theorem 2.8 (5).

(2) Write $n = \lambda^2 - 2\mu^2$ where $\lambda, \mu \in \mathbb{N}$. Then $(2, 2\mu, \lambda)$ is a primitive positive solution of $n\alpha^2 + 2\beta^2 = 4\gamma^2$. By Theorem 2.8 (3), $\left[\frac{\lambda}{n}\right] = 1 - h_8(-2n)$. This conclude the result by Theorem 2.8 (4) and Corollary 1.6. $\square$

Proof of Theorem 1.8. By our assumptions (we rearrange the order of prime factors of P),

$$\mathbf{A}_P + \mathbf{U}_P = \mathbf{A}_P = \operatorname{diag}\{\mathbf{A}_{f_1}, \cdots \mathbf{A}_{f_r}\}.$$

Since $h_4(-f_i) = 1$, we have $\operatorname{corank} \mathbf{A}_{f_i} = 1$ by Theorem 2.8 (1). Since $\mathbf{A}_{f_i}\mathbf{1} = \mathbf{0}$, we have $s_2(n) = 2r$ and the kernel of $\mathbf{M}_n$ is consists of vectors

$$\begin{pmatrix} \mathbf{c}_1 \\ \vdots \\ \mathbf{c}_r \\ \mathbf{0} \\ \mathbf{d}_1 \\ \vdots \\ \mathbf{d}_r \\ \mathbf{0} \end{pmatrix},$$

where $\mathbf{c}_i, \mathbf{d}_i = \mathbf{0}$ or $\mathbf{1}$ are vectors in $\operatorname{Ker} \mathbf{A}_{f_i}$. Thus $\operatorname{Sel}_2'(E_n)$ is generated by $\Lambda_1, \ldots, \Lambda_r, \Lambda_1', \ldots, \Lambda_r'$, where

$$\Lambda_i = (f_i, 1, f_i), \quad \Lambda_i' = (f_i, f_i, 1)$$

by (2.5) and (2.7). By Proposition 3.2, we have $\left[\frac{\gamma_i'}{f_j}\right] = \left[\frac{\gamma_j}{f_i}\right]$ and the Cassles pairing with respect to this basis is

$$\mathbf{X} = \begin{pmatrix} * & \mathbf{B}^{\mathrm{T}} + \mathbf{C} \\ \mathbf{B} + \mathbf{C} & \mathbf{B} + \mathbf{B}^{\mathrm{T}} \end{pmatrix},$$

where

$$\mathbf{B} = \left(\left[\frac{\gamma_i}{f_j}\right]\right)_{r\times r} \quad \text{and} \quad \mathbf{C} = \operatorname{diag}\left\{\left[\frac{\sqrt{2}+1}{f_1}\right], \cdots, \left[\frac{\sqrt{2}+1}{f_r}\right]\right\}.$$

Since $h_4(-f_i) = 1$, we have

$$\mathbf{C} = \operatorname{diag}\{1 - h_8(-f_1), \cdots, 1 - h_8(-f_r)\}$$

by Theorem 2.8 (2). By our assumptions,

$$\mathbf{B} = \operatorname{diag}\Big\{h_8(-f_1), \cdots, h_8(-f_r)\Big\}.$$

Therefore, $\mathbf{X} = \begin{pmatrix} * & \mathbf{I} \\ \mathbf{I} & \mathbf{O} \end{pmatrix}$ is invertible, i.e., the Cassles pairing on $\operatorname{Sel}_2'(E_n)$ is non-degenerate. Conclude the results by Lemma 4.1. $\square$

Proof of Corollary 1.9. (1) Since

$$\mathbf{R}_{-n} = \operatorname{diag}\{\mathbf{A}_n, 0\} = \operatorname{diag}\{\mathbf{A}_{f_1}, \cdots \mathbf{A}_{f_r}, 0\},$$

we have $h_4(-n) = r$ and $\mathcal{A}_{-n}[2] \cap \mathcal{A}_{-n}^2$ is generated by $\theta_{-n}(f_1), \ldots, \theta_{-n}(f_{r-1})$ and $\theta_{-n}(2)$ by (2.10) and (2.11). Here, one notice that

$$\theta_{-n}(f_1) \cdots \theta_{-n}(f_r) = \theta_{-n}(n) = [(\sqrt{-n})]$$

is the trivial class. If $h_8(-n) = r$, or $h_8(-n) = r - 1$ and $[(2, \sqrt{-n})] \notin \mathcal{A}_{-n}^4$, then all $\theta_{-n}(f_i) \in \mathcal{A}_{-n}[2] \cap \mathcal{A}_{-n}^4$. By Proposition 2.4, this implies that $\mathbf{b}_{n,\gamma_i} \in \operatorname{Im} \mathbf{A}_n$, where $(\alpha_i, \beta_i, \gamma_i)$ is a primitive positive solution of $f_i\alpha_i^2 - \frac{n}{f_i}\beta_i^2 = 4\gamma_i^2$. Thus $\mathbf{b}_{f_j,\gamma_i} \in \operatorname{Im} \mathbf{A}_{f_j}$ for all j. Since $\mathbf{1}^{\mathrm{T}}\mathbf{A}_{f_j} = \mathbf{0}^{\mathrm{T}}$, we have

$$0 = \mathbf{1}^{\mathrm{T}}\mathbf{b}_{f_j,\gamma_i} = \left[\frac{\gamma_i}{f_j}\right].$$

Conclude the results by Theorem 1.8.

(2) Similar to (1), $h_4(-2n) = r$ and $\mathcal{A}_{-2n}[2] \cap \mathcal{A}_{-2n}^2$ is generated by $\theta_{-2n}(f_1)$, $\dots$, $\theta_{-2n}(f_r)$ by (2.10) and (2.11). Here, one notice that

$$\theta_{-2n}(2) = \theta_{-2n}(f_1) \cdots \theta_{-2n}(f_r)$$

since $\theta_{-2n}(2n) = [(\sqrt{-2n})]$ is the trivial class. If $h_8(-2n) = r$, then all $\theta_{-2n}(f_i) \in \mathcal{A}_{-2n}[2] \cap \mathcal{A}_{-2n}^4$. One can conclude the results similar to (1). $\square$

This paper reveals a new phenomenon: for a general non-congruent number n with the second minimal 2-primary Shafarevich group, the criterion cannot be expressed solely in terms of the 4-ranks and 8-ranks of class groups of quadratic fields, even though this is possible when the prime factors of n lie in certain residue classes. A key remaining problem is how to find simple arithmetic conditions that characterize non-congruent numbers with specific 2-primary Shafarevich groups.

Acknowledgements. The author is partially supported by the National Natural Science Foundation of China (Grant No. 12271335) and the Fundamental Research Funds for the Central Universities (No. JZ2023HGTB0217).

References

[BS82] J. Browkin and A. Schinzel. On Sylow 2-subgroups of K_2O_F for quadratic number fields *F. J. Reine Angew. Math.*, 331:104–113, 1982.

[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.

[Fen97] Keqin Feng. Non-congruent number, odd graph and the BSD conjecture on $y^2 = x^3 - n^2x$. In *Singularities and complex geometry (Beijing, 1994)*, volume 5 of *AMS/IP Stud. Adv. Math.*, pages 54–66. Amer. Math. Soc., Providence, RI, 1997.

[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.

[Isk96] Boris Iskra. Non-congruent numbers with arbitrarily many prime factors congruent to 3 modulo 8. *Proc. Japan Acad. Ser. A Math. Sci.*, 72(7):168–169, 1996.

[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.

[LQ23] Guilin Li and Hourong Qin. Diophantine equations, class groups and non-congruent numbers. *Ramanujan J.*, 62(4):1081–1105, 2023.

[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.

[Lu15] Qing Lu. 8-rank of the class group and isotropy index. *Sci. China Math.*, 58(7):1433–1444, 2015.

[LY20] Jianing Li and Chia-Fu Yu. The Chevalley-Gras formula over global fields. *J. Théor. Nombres Bordeaux*, 32(2):525–543, 2020.

[OZ14] Yi Ouyang and Shen Xing 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.

[Qin95a] Hou Rong Qin. The 2-Sylow subgroups of the tame kernel of imaginary quadratic fields. *Acta Arith.*, 69(2):153–169, 1995.

[Qin95b] Hou Rong Qin. The 4-rank of K_2O_F for real quadratic fields F. *Acta Arith.*, 72(4):323–333, 1995.

[Qin22] Hourong Qin. Congruent numbers, quadratic forms and K_2. *Math. Ann.*, 383:1647–1686, 2022.

[Rè34] L. Rèdei. 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.

[Smi16] Alexander Smith. The congruent numbers have positive natural density. *arXiv: Number Theory*, page 32, 2016.
[TYZ17] Ye Tian, Xinyi Yuan, and Shou-Wu Zhang. Genus periods, genus points and congruent number problem. *Asian J. Math.*, 21(4):721–773, 2017.
[Wan16] Zhang Jie Wang. Congruent elliptic curves with non-trivial Shafarevich-Tate groups. *Sci. China Math.*, 59(11):2145–2166, 2016.
[WZ22] Zhangjie Wang and Shenxing Zhang. On the quadratic twist of elliptic curves with full 2-torsion. *preprint*, 2022.
[Zha23] Shenxing Zhang. On a comparison of Cassels pairings of different elliptic curves. *Acta Arith.*, 211(1):1–23, 2023.

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