ON NON-CONGRUENT NUMBERS WITH $8a\pm1$ TYPE ODD PRIME FACTORS AND TAME KERNELS

SHENXING ZHANG

ABSTRACT. Let n be a positive square-free integer, where every odd prime factor of n has form $8a \pm 1$. We determine when n is non-congruent with second minimal 2-primary Shafarevich-Tate group, in terms of the 4-ranks of class groups and a Jacobi symbol. In particular, when every odd prime factor of n has form 8a+1, this condition is equivalent to the vanishing of the 4-rank of the tame kernel of $\mathbb{Q}(\sqrt{n})$ for odd n, or $\mathbb{Q}(\sqrt{-n})$ for even n. This generalizes previous results.

Contents

1. Introduction	
1.1. Background	1
1.2. Main results	2
1.3. Notations	3
2. Preliminaries	3
2.1. Monsky matrix	3
2.2. Cassels pairing	4
2.3. Rédei matrix	5
2.4. Tame kernel	5
3. The odd case	6
4. The even case	6
References	11

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 over $\mathbb Q$ is positive, where

$$(1.1) E = E_n : y^2 = x^3 - n^2 x$$

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

$$(1.2) s_2(n) := \dim_{\mathbb{F}_2} \left(\frac{\operatorname{Sel}_2(E)}{E(\mathbb{Q})[2]} \right) = \dim_{\mathbb{F}_2} \operatorname{Sel}_2(E) - 2$$

Date: November 24, 2021.

²⁰²⁰ Mathematics Subject Classification. Primary 11G05; Secondary 11D25, 11R29, 11R70. Key words and phrases. non-congruent number; second 2-descent; elliptic curve; class group; tame kernel.

the pure 2-Selmer rank. Then

$$s_2(n) = \operatorname{rank}_{\mathbb{Z}} E(\mathbb{Q}) + \dim_{\mathbb{F}_2} \operatorname{III}(E/\mathbb{Q})[2]$$

by the exact sequence

$$0 \to E(\mathbb{Q})/2E(\mathbb{Q}) \to \mathrm{Sel}_2(E) \to \mathrm{III}(E/\mathbb{Q})[2] \to 0.$$

Certainly, $s_2(n) = 0$ implies that n is non-congruent. The examples of $s_2(n) = 0$ can be found in [Fen97], [Isk96] and [OZ15], which are corollaries of Monsky's formula for $s_2(n)$. This case is fully characterized in terms of class groups and the full Birch-Swinnerton-Dyer (BSD) conjecture holds, see [TYZ17, Theorem 1.1, Corollary 1.3] and [Smi16, Theorem 1.2]. The examples of non-congruent n with $\mathrm{III}(E/\mathbb{Q})[2^{\infty}] \cong (\mathbb{Z}/2\mathbb{Z})^2$ can be found in [LT00], [OZ14] and [OZ15]. When n is odd with prime factors 1 mod 4, it can be characterized as follows.

Denote by $(a,b)_v$ the Hilbert symbol. Denote by

(1.3)
$$r_{2^{a}}(A) = \dim_{\mathbb{F}_{2}} \left(\frac{2^{a-1}A}{2^{a}A} \right)$$

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 of $\mathbb{Q}(\sqrt{m})$.

Theorem 1.1 ([Wan16, Theorem 1.1]). Let $n = p_1 \cdots p_k \equiv 1 \mod 8$ be a squarefree positive integer with $p_i \equiv 1 \mod 4$. The following are equivalent:

- (i) $h_4(-n) = 1$ and $h_8(-n) \equiv \frac{d-1}{4} \pmod{2}$; (ii) $\operatorname{rank}_{\mathbb{Z}} E_n(\mathbb{Q}) = 0$ and $\operatorname{III}(E_n/\mathbb{Q})[2^{\infty}] \cong (\mathbb{Z}/2\mathbb{Z})^2$.

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

Wang also gave a sufficient condition on $\coprod (E/\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^{s_2(n)}$ for $s_2(n) \geq 4$. Recently, Qin in [Qin21, Theorem 1.5] proved that if $p \equiv 1 \mod 8$ 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 $\mathrm{III}(E_p/\mathbb{Q})[2^\infty] \cong (\mathbb{Z}/4\mathbb{Z})^2$.

1.2. Main results. In this paper, we will give a criterion of non-congruent n with $\coprod (E_n/\mathbb{Q})[2^{\infty}] \cong (\mathbb{Z}/2\mathbb{Z})^2$, where the odd prime factors of n are congruent to ± 1 modulo 8.

Theorem 1.2 (=Theorem 3.2). Let $n = p_1 \cdots p_k \equiv 1 \mod 8$ be a square-free positive integer with $p_i \equiv \pm 1 \mod 8$. The following are equivalent:

- (i) $h_4(-n) = 1, h_4(n) = 0 \text{ and } (\frac{-\mu}{d}) = -1;$ (ii) $\text{rank}_{\mathbb{Z}} E_n(\mathbb{Q}) = 0 \text{ and } \text{III}(E_n/\mathbb{Q})[2^{\infty}] \cong (\mathbb{Z}/2\mathbb{Z})^2.$

Here, $d \neq 1$ is the unique positive divisor of n such that $(d,n)_v = 1, \forall v$ and n = 1 $2\mu^2 - \tau^2$ where $\mu \equiv d \mod 4$.

Corollary 1.3 (= Corollary 3.4). Let $n = p_1 \cdots p_k \equiv 1 \mod 8$ be a square-free positive integer with $p_i \equiv 1 \mod 8$. The following are equivalent:

- (i) $r_4(K_2\mathcal{O}_{\mathbb{Q}(\sqrt{n})}) = 0;$
- (ii) $\operatorname{rank}_{\mathbb{Z}} E_n(\mathbb{Q}) = 0$ and $\operatorname{III}(E_n/\mathbb{Q})[2^{\infty}] \cong (\mathbb{Z}/2\mathbb{Z})^2$.

This generalizes [Qin21, Lemma 4.2].

Theorem 1.4 (= Theorem 4.1). Let $n = 2p_1 \cdots p_k \equiv 2 \mod 8$ be a square-free positive integer with $p_i \equiv \pm 1 \mod 8$. The following are equivalent:

(i)
$$h_4(-n/2) = 1$$
 and $\left(\frac{2-\sqrt{2}}{|d|}\right) = -1$;

(ii)
$$\operatorname{rank}_{\mathbb{Z}} E_n(\mathbb{Q}) = 0$$
 and $\operatorname{III}(E_n/\mathbb{Q})[2^{\infty}] \cong (\mathbb{Z}/2\mathbb{Z})^2$.

Here, $d \neq 1$ is the unique divisor of n such that $(d, n)_v = 1, \forall v \text{ and } d \equiv 1 \mod 8$.

Corollary 1.5 (= Corollary 4.2). Let $n = 2p_1 \cdots p_k \equiv 2 \mod 8$ be a square-free positive integer with $p_i \equiv 1 \mod 8$. The following are equivalent:

- (i) $r_4(K_2\mathcal{O}_{\mathbb{Q}(\sqrt{-n})}) = 0;$
- (ii) $\operatorname{rank}_{\mathbb{Z}} E_n(\mathbb{Q}) = 0$ and $\operatorname{III}(E_n/\mathbb{Q})[2^{\infty}] \cong (\mathbb{Z}/2\mathbb{Z})^2$.

1.3. Notations.

- $E = E_n$ the congruent elliptic curve associated a square-free positive integer n, see (1.1).
- $s_2(n)$ the pure 2-Selmer rank of E_n , see (1.2).
- (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 $\{\pm 1\} \stackrel{\sim}{\longrightarrow} \mathbb{F}_2$.
- $\left(\frac{a}{b}\right) = \prod_{p|b} (a,b)_p$ the Jacobi symbol, where (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 $\{\pm 1\} \xrightarrow{\sim} \mathbb{F}_2$.
- r_{2a} the 2^a -rank of a finite abelian group, see (1.3).
- $h_{2^a}(m)$ the 2^a -rank of the narrow class group of $\mathbb{Q}(\sqrt{m})$.
- $K_2\mathcal{O}_F$ the tame kernel of a number field F, see [Wei13, Theorem III.6.5].
- $m' = |m|/(2^{|m|}, m)$ the positive odd part of an integer m.
- $\mathbf{A} = \mathbf{A}_{n'}$ a matrix associated to n', see (2.2).
- \mathbf{D}_{ε} a matrix associated to n' and ε , see (2.3).
- $\mathbf{0} = (0, \dots, 0)^{\mathrm{T}}, \ \mathbf{1} = (1, \dots, 1)^{\mathrm{T}} \text{ and } \mathbf{b}_{\varepsilon} = \mathbf{D}_{\varepsilon} \mathbf{1}.$
- \mathbf{M}_n the Monsky matrix of E_n , see (2.4) and (2.4).
- \mathbf{R}_m the Rédei matrix of $\mathbb{Q}(\sqrt{m})$, see (2.9).
- V, V_1, V_2 sets associated to $\mathbb{Q}(\sqrt{m})$, see Theorems 2.4 and 2.5.
- v_p the normalized valuation on \mathbb{Q}_p .
- For a vector $\mathbf{d} = (\delta_1, \dots, \delta_k)^{\mathrm{T}} \in \mathbb{F}_2^k$, denote by $\psi(\mathbf{d}) = \prod_{j=1}^k p_j^{\delta_j}$. Then $\psi^{-1}(|d|) = (v_{p_1}(d), \dots, v_{p_k}(d))^{\mathrm{T}}$ for $d \mid p_1 \dots p_k$.

2. Preliminaries

2.1. Monsky matrix. Monsky in [HB94, Appendix] represented the pure 2-Selmer group as the kernel of a matrix over \mathbb{F}_2 . Let's recall it roughly. One can identify $\mathrm{Sel}_2(E_n)$ with

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

where D_{Λ} is a genus one curve defined by

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

Under this identification, O, (n, 0), (-n, 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) and (x - n, x + n, x) respectively.

Let $n' = p_1 \cdots p_k$ be an ordered prime decomposition of n' = n/(2, n). Denote by

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

and

(2.3)
$$\mathbf{D}_{\varepsilon} = \operatorname{diag} \left\{ \left[\frac{\varepsilon}{p_1} \right], \dots, \left[\frac{\varepsilon}{p_k} \right] \right\}.$$

Then $\mathbf{A1} = \mathbf{0}$ and $\operatorname{rank}(\mathbf{A}) \leq k - 1$.

When n is odd, each element in $\operatorname{Sel}_2(E_n)/E_n(\mathbb{Q})[2]$ can be presented as (d_1, d_2, d_3) , where both of d_1, d_2 are positive divisor of n. The system D_{Λ} is locally solvable everywhere if and only if certain conditions on Hilbert symbols hold. Then we can express the pure 2-Selmer group as the kernel of Monsky matrix

(2.4)
$$\mathbf{M}_n = \begin{pmatrix} \mathbf{A} + \mathbf{D}_2 & \mathbf{D}_2 \\ \mathbf{D}_2 & \mathbf{A} + \mathbf{D}_{-2} \end{pmatrix}$$

via the isomorphism

(2.5)
$$\operatorname{Sel}_{2}(E_{n})/E_{n}(\mathbb{Q})[2] \longrightarrow \operatorname{Ker} \mathbf{M}_{n} \\ (d_{1}, d_{2}, d_{3}) \longmapsto \begin{pmatrix} \psi^{-1}(d_{2}) \\ \psi^{-1}(d_{1}) \end{pmatrix}.$$

When n is even, each element in $\mathrm{Sel}_2(E_n)/E_n(\mathbb{Q})[2]$ can be presented as (d_1, d_2, d_3) , where both of d_2, d_3 are divisor of n' and $d_2 > 0, d_3 \equiv 1 \mod 4$. Then we can express the pure 2-Selmer group as the kernel of Monsky matrix

(2.6)
$$\mathbf{M}_n = \begin{pmatrix} \mathbf{A}^{\mathrm{T}} + \mathbf{D}_2 & \mathbf{D}_{-1} \\ \mathbf{D}_2 & \mathbf{A} + \mathbf{D}_2 \end{pmatrix}$$

via the isomorphism

(2.7)
$$\operatorname{Sel}_{2}(E_{n})/E_{n}(\mathbb{Q})[2] \longrightarrow \operatorname{Ker} \mathbf{M}_{n} \\ (d_{1}, d_{2}, d_{3}) \longmapsto \begin{pmatrix} \psi^{-1}(|d_{3}|) \\ \psi^{-1}(d_{2}) \end{pmatrix}.$$

In both cases, we have

$$(2.8) s_2(n) = 2k - \operatorname{rank}(\mathbf{M}_n).$$

2.2. Cassels pairing. Cassels in [Cas98] defined a skew-symmetric bilinear pairing $\langle -, - \rangle$ on the \mathbb{F}_2 -vector space $\mathrm{Sel}_2(E_n)/E_n(\mathbb{Q})[2]$. For any $\Lambda \in \mathrm{Sel}_2(E_n)$, choose any $P = (P_v) \in D_{\Lambda}(\mathbb{A}_{\mathbb{Q}})$. Note that H_i is locally solvable everywhere, hence it is solvable over \mathbb{Q} by Hasse-Minkowski principal. Choose $Q_i \in H_i(\mathbb{Q})$. 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 $\Lambda' = (d'_1, d'_2, d'_3) \in \mathrm{Sel}_2(E_n)$, define

$$\langle \Lambda, \Lambda' \rangle = \prod_{v} \langle \Lambda, \Lambda' \rangle_{v} \quad \text{where} \quad \langle \Lambda, \Lambda' \rangle_{v} = \prod_{i=1}^{3} (L_{i}(P_{v}), d'_{i})_{v}.$$

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

Lemma 2.1 ([Cas98, Lemma 7.2]). The local Cassels pairing $\langle -, - \rangle_p = +1$ 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.
- 2.3. **Rédei matrix.** Let $m \neq 0, 1$ be a square-free integer. Denote by $F = \mathbb{Q}(\sqrt{m})$ and $\mathbf{N}F = \mathbf{N}_{F/\mathbb{Q}}(F^{\times})$. Denote by C(F) the narrow class group of F. Let $D = p_1^* \cdots p_t^*$ be the decomposition of the discriminant of F into a product of *prime discriminants*

$$p^* = (-1)^{\frac{p-1}{2}}p, \qquad 2^* = -4, 8, -8.$$

By Gauss genus theory, we have $h_2(m) = t - 1$. To calculate $h_4(m)$, we need the Rédei matrix, which is defined as

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

Let V be the set of all square-free positive integers $d \mid D$. Then the following are equivalent:

- $d \in V \cap \mathbf{N}F$;
- $X^2 mY^2 = dZ^2$ is has nonzero solutions over \mathbb{Z} ;
- Hilbert symbols $(d, m)_p = 1, \forall p \mid D;$
- $\mathbf{R}_m \mathbf{d} = \mathbf{0}$, where $\mathbf{d} = (v_{p_1}(d), \dots, v_{p_t}(d))^{\mathrm{T}}$.

Rédei showed that

$$\theta: V \cap \mathbf{N}F \longrightarrow C(F)[2] \cap C(F)^2$$
$$d \longmapsto \operatorname{cl}[\mathfrak{d}]$$

is a two-to-one onto homomorphism, where $(d) = \mathfrak{d}^2$. Thus

(2.10)
$$h_4(m) = t - 1 - \text{rank}(\mathbf{R}_m).$$

See [R34] and [LY20, Example 2.6].

Example 2.2. Let $n = p_1 \cdots p_k$ be an odd positive square-free integer. When $n \equiv 1 \mod 4$, we have

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

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

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

$$\begin{split} \mathbf{R}_n &= \begin{pmatrix} \mathbf{A} + \mathbf{D}_{-1} & \mathbf{b}_2 \\ \mathbf{b}_{-1}^\mathrm{T} & \left[\frac{2}{n}\right] \end{pmatrix}, \qquad \qquad \mathbf{R}_{-n} = \mathbf{A}, \\ \mathbf{R}_{2n} &= \begin{pmatrix} \mathbf{A} + \mathbf{D}_{-2} & \mathbf{b}_2 \\ \mathbf{b}_{-2}^\mathrm{T} & \left[\frac{2}{n}\right] \end{pmatrix}, \qquad \qquad \mathbf{R}_{-2n} = \begin{pmatrix} \mathbf{A} + \mathbf{D}_2 & \mathbf{b}_2 \\ \mathbf{b}_2^\mathrm{T} & \left[\frac{2}{n}\right] \end{pmatrix}. \end{split}$$

2.4. **Tame kernel.** Denote by $K_2\mathcal{O}_F$ is the tame kernel of F. We list the results of $r_4(K_2\mathcal{O}_F)$ that we will use. Assume that |m| > 2.

Theorem 2.3 ([BS82]). The subgroup $K_2\mathcal{O}_F[2]$ 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. If m > 2, then

$$r_2(K_2\mathcal{O}_F) = k + \log_2 \# (\{\pm 1, \pm 2\} \cap \mathbf{N}F).$$

If m < -2, then

$$r_2(K_2\mathcal{O}_F) = k - 1 + \log_2 \#(\{1, 2\} \cap \mathbf{N}F).$$

Denote by m' = |m|/(2, m) the positive odd part of m. If $2 \notin \mathbf{N}F$, set $V_2 = \emptyset$.

Theorem 2.4 ([Qin95b, Theorem 3.4]). Suppose that m > 2. Denote by V_1 the set of positive $d \mid m'$ satisfying: there exists $\varepsilon = \pm 1$ or ± 2 such that $(d, -m)_p = \left(\frac{\varepsilon}{p}\right), \forall p \mid m'$. If $2 \in \mathbf{N}F$, then write $m = 2\mu^2 - \lambda^2, \mu, \lambda \in \mathbb{N}$ and denote by V_2 the set of positive $d \mid m'$ satisfying: there exists $\varepsilon = \pm 1$ such that $(d, -m)_p = \left(\frac{\varepsilon\mu}{p}\right), \forall p \mid m'$. We have

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

Theorem 2.5 ([Qin95a, Theorem 4.1]). Suppose that m < -2. Denote by V_1 the set of $d \mid m'$ satisfying: there exists $\varepsilon = 1$ or 2 such that $(d, -m)_p = \left(\frac{\varepsilon}{p}\right), \forall p \mid m'$. If $2 \in \mathbf{N}F$, then write $m = 2\mu^2 - \lambda^2, \mu, \lambda \in \mathbb{N}$ and denote by V_2 the set of $d \mid m'$ satisfying: $(d, -m)_p = \left(\frac{\mu}{p}\right), \forall p \mid m'$. We have

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

Denote by $\mathbf{B} = \mathbf{B}_m = \mathbf{A}_{m'} + \mathbf{D}_{m/m'}$, where $\mathbf{A}_{m'}$ is defined as (2.2). If m > 0, then

(2.11)
$$V_1 = \{ \psi(\mathbf{d}) : \mathbf{B}\mathbf{d} = \mathbf{b}_{\pm 1}, \mathbf{b}_{\pm 2} \}, \qquad V_2 = \{ \psi(\mathbf{d}) : \mathbf{B}\mathbf{d} = \mathbf{b}_{\pm \mu} \}.$$

If m < 0, then

(2.12)
$$V_1 = \{ \psi(\mathbf{d}) : \mathbf{B}\mathbf{d} = \mathbf{0}, \mathbf{b}_2 \} \cup \{ -\psi(\mathbf{d}) : \mathbf{B}\mathbf{d} = \mathbf{b}_{-1}, \mathbf{b}_{-2} \},$$
$$V_2 = \{ \psi(\mathbf{d}) : \mathbf{B}\mathbf{d} = \mathbf{b}_{\mu} \} \cup \{ -\psi(\mathbf{d}) : \mathbf{B}\mathbf{d} = \mathbf{b}_{-\mu} \}.$$

3. The odd case

Lemma 3.1. If $s_2(n) = 2$, then $\operatorname{rank}_{\mathbb{Z}} E_n(\mathbb{Q}) = 0$, $\operatorname{III}(E_n/\mathbb{Q})[2^{\infty}] \cong (\mathbb{Z}/2\mathbb{Z})^2$ holds if and only if the Cassels pairing on the pure 2-Selmer group $\operatorname{Sel}_2(E_n)/E_n(\mathbb{Q})[2]$ is non-degenerate.

Theorem 3.2. Let $n = p_1 \cdots p_k \equiv 1 \mod 8$ be a square-free positive integer with $p_i \equiv \pm 1 \mod 8$. The following are equivalent:

- (i) $h_4(-n) = 1, h_4(n) = 0$ and $\left(\frac{-\mu}{d}\right) = -1$;
- (ii) $\operatorname{rank}_{\mathbb{Z}} E_n(\mathbb{Q}) = 0$ and $\operatorname{III}(E_n/\mathbb{Q})[2^{\infty}] \cong (\mathbb{Z}/2\mathbb{Z})^2$.

Here, $d \neq 1$ is the unique positive divisor of n such that $(d, n)_v = 1, \forall v$ and $n = 2\mu^2 - \tau^2$ where $\mu \equiv d \mod 4$.

Proof. In this case, $\mathbf{D}_2 = \mathbf{O}$ and the Monsky matrix (2.4) is

$$\mathbf{M}_n = egin{pmatrix} \mathbf{A} & & & \ & \mathbf{A} + \mathbf{D}_{-1} \end{pmatrix}.$$

Since $\mathbf{A}\mathbf{1} = (\mathbf{A}^{\mathrm{T}} + \mathbf{D}_{-1})\mathbf{1} = \mathbf{0}$, we have $\operatorname{rank}(\mathbf{A}) \leq k-1$ and $\operatorname{rank}(\mathbf{A} + \mathbf{D}_{-1}) \leq k-1$. By (2.8), we have

$$s_2(n) = 2 \iff \operatorname{rank}(\mathbf{A}) = \operatorname{rank}(\mathbf{A} + \mathbf{D}_{-1}) = k - 1.$$

Since the Rédei matrices

$$\mathbf{R}_{-n} = \begin{pmatrix} \mathbf{A} & \mathbf{0} \\ \mathbf{b}_{-1}^{\mathrm{T}} & \mathbf{0} \end{pmatrix}, \quad \mathbf{R}_{n} = \mathbf{A} + \mathbf{D}_{-1}$$

and note that $\mathbf{1}^{\mathrm{T}}\mathbf{A} = \mathbf{b}_{-1}^{\mathrm{T}}$, we have $\mathrm{rank}(\mathbf{R}_{-n}) = \mathrm{rank}(\mathbf{A})$ and

$$s_2(n) = 2 \iff h_4(-n) = 1 \text{ and } h_4(n) = 0$$

by (2.9) and (2.10).

From the definition of d, we know that $\operatorname{Ker}(\mathbf{A} + \mathbf{D}_{-1}) = \{\mathbf{0}, \psi^{-1}(d)\}$. The pure 2-Selmer group of E_n is

$$\{(1,1,1),(1,n,n),(d,1,d),(d,n,nd)\}$$

by (2.5). Denote by $\Lambda = (1, n, n)$ and $\Lambda' = (d, 1, d)$. Then D_{Λ} is defined by

(3.1)
$$\begin{cases} H_1: & -t^2 + u_2^2 - u_3^2 = 0, \\ H_2: & -nt^2 + nu_3^2 - u_1^2 = 0, \\ H_3: & 2nt^2 + u_1^2 - nu_2^2 = 0. \end{cases}$$

Recall that $n=2\mu^2-\tau^2$. Then μ is odd and $n=u^2-2w^2$, where $u=2\mu-\tau$ and $w=-\mu+\tau$. Choose

$$Q_1 = (0, 1, 1) \in H_1(\mathbb{Q}),$$
 $L_1 = u_2 - u_3,$ $Q_3 = (w, n, u) \in H_3(\mathbb{Q}),$ $L_3 = 2wt + u_1 - uu_2.$

By Lemma 2.1,

$$\langle \Lambda, \Lambda' \rangle = \prod_{p|2n} (L_1 L_3(P_p), d)_p$$

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

When $p \mid n$, take $(t, u_1, u_2, u_3) = (1, 0, \sqrt{2}, 1)$ where $\sqrt{2} \equiv -u/w \mod p$. Then

$$L_1 L_3(P_p) = (\sqrt{2} - 1)(2w - \sqrt{2}u) \equiv 4(\sqrt{2} - 1)w \equiv -4\mu \mod p$$

and $(L_1L_3(P_p), d)_p = (-\mu, d)_p$. When p = 2, take $(t, u_1, u_2, u_3) = (0, \sqrt{n}, 1, -1)$. Then

$$(L_1L_3(P_2),d)_2 = (2(\sqrt{n}-u),d)_2 = (-\sqrt{n}-u,d)_2 = (-\mu,d)_2$$

by Lemma 3.3. Since $\mu \equiv d \mod 4$, we have $(-\mu, d)_2 = 1$ and

$$\langle \Lambda, \Lambda' \rangle = \prod_{p|d} (-\mu, d)_p = \left(\frac{-\mu}{d}\right).$$

Conclude the result by Lemma 3.1.

Lemma 3.3. We have $(-u \pm \sqrt{n}, -1)_2 = (-\mu, -1)_2$.

Proof. See [Qin95b, Lemma 3.1]. Clearly, $(\mu, -1)_2 = \pm 1$ if and only if $(-1, \pm \mu)_2 = 1$. Thus the equation $X^2 + Y^2 = \pm \mu$ is solvable in \mathbb{Q}_2 and so is $X^2 + nY^2 = \pm \mu$. Let $x, y \in \mathbb{Q}_2$ such that $x^2 + ny^2 = \pm \mu$. Denote by

$$h = y, \quad g = \frac{x - wy}{\mu}, \quad \alpha = g^2 + h^2,$$

 $\theta = g^2 - h^2 + 2gh, \quad \lambda = g^2 - h^2 - 2gh,$

$$\xi = \frac{g+h}{\alpha}, \quad \eta = \frac{g-h}{\alpha},$$

$$x = -\xi + \lambda \eta, \ y = \alpha \xi, \ a = -\eta - \lambda \xi, \ b = \alpha \eta.$$

Then

$$u\alpha + w\theta = \pm 1$$
, $\theta^2 + \lambda^2 = 2\alpha^2$, $\xi^2 + \eta^2 = \frac{2}{\alpha}$

and

$$\left(\frac{x+y\sqrt{n}}{2}\right)^2 + \left(\frac{a+b\sqrt{n}}{2}\right)^2$$

$$= \frac{1}{4}(\xi^2 + \eta^2)(1 + \lambda^2 w^2 + n\alpha^2 - 2\alpha\sqrt{n})$$

$$= \frac{1}{2\alpha}\left((u\alpha + \theta w)^2 + \lambda^2 w^2 + (u^2 - 2w^2)\alpha^2\right) - \sqrt{n}$$

$$= u(u\alpha + \theta w) - \sqrt{n} = \pm u - \sqrt{n}.$$

Hence we have $(\mu, -1)_2 = (u - \sqrt{n}, -1)_2 = (u + \sqrt{n}, -1)_2$.

When all prime factors of n are $\equiv 1 \mod 8$, we have the following corollary generalizing [Qin21, Lemma 4.2].

Corollary 3.4. Let $n = p_1 \cdots p_k \equiv 1 \mod 8$ be a square-free positive integer with $p_i \equiv 1 \mod 8$. The following are equivalent:

- (i) $r_4(K_2\mathcal{O}_{\mathbb{Q}(\sqrt{n})}) = 0;$
- (ii) $\operatorname{rank}_{\mathbb{Z}} E_n(\mathbb{Q}) = 0$ and $\operatorname{III}(E_n/\mathbb{Q})[2^{\infty}] \cong (\mathbb{Z}/2\mathbb{Z})^2$.

Proof. Since all $p_i \equiv 1 \mod 8$, we have $\mathbf{D}_{\varepsilon} = \mathbf{O}$ and $\mathbf{b}_{\varepsilon} = \mathbf{0}$ for any $\varepsilon = \pm 1, \pm 2$. Note that d = n in Theorem 3.2, the condition (ii) is equivalent to $\operatorname{rank}(\mathbf{A}) = k - 1$ and $\left(\frac{\mu}{n}\right) = \left(\frac{-\mu}{n}\right) = -1$.

Denote by $F = \mathbb{Q}(\sqrt{n})$. Combining with Theorem 2.4 and (2.11), we have

$$2^{r_4(K_2\mathcal{O}_F)+1} = \#\{\mathbf{d} : \mathbf{Ad} = \mathbf{0}\} + \#\{\mathbf{d} : \mathbf{Ad} = \mathbf{b}_{|\mu|} = \mathbf{b}_{\mu}\}\$$

and Ker $\mathbf{A} \supseteq \{\mathbf{0}, \mathbf{1}\}$. This implies that $r_4(K_2\mathcal{O}_F) = 0$ if and only if Ker $\mathbf{A} = \{\mathbf{0}, \mathbf{1}\}$ and $\mathbf{Ad} = \mathbf{b}_{\mu}$ is not solvable. Once we have Ker $\mathbf{A} = \{\mathbf{0}, \mathbf{1}\}$, we will get rank $(\mathbf{A}) = k - 1$. Since $\mathbf{1}^T \mathbf{A} = \mathbf{0}^T$, we will have Im $\mathbf{A} = \{\mathbf{d} : \mathbf{1}^T \mathbf{d} = 0\}$. Hence $\mathbf{Ad} = \mathbf{b}_{\mu}$ is solvable if and only if $\left(\frac{\mu}{n}\right) = 1$.

One can propose many equivalent conditions for (i), which generalizes [BC69] and [LT00, Lemma-Definition 1]. See also [Wan16, Theorem 4.2].

Proposition 3.5. Let n be a square-free positive integer with prime factors congruent to 1 modulo 8. If $h_4(-n) = 0$, then the following are equivalent:

- (i) $2 \mid b$, where $n = a^2 + 8b^2$;
- (ii) $\left(\frac{1+\sqrt{2}}{n}\right) = 1;$
- (iii) $\left(\frac{1+\sqrt{-1}}{n}\right) = 1;$
- $(iv) \left(\frac{\sqrt{2}}{n}\right) = (-1)^{\frac{n-1}{8}};$
- (v) $|u| \equiv 1 \mod 4$;
- (vi) $|\mu| \equiv 1 \mod 4$;
- (vii) $h_8(-n) = 0;$
- (viii) $\left(\frac{\mu}{n}\right) = 1$.

Proof. For any $p \mid n$, we have $\left(\frac{a}{p}\right) = \left(\frac{\sqrt{2}(1+\sqrt{-1})^2b}{p}\right) = \left(\frac{\sqrt{2}b}{p}\right)$. Thus $\left(\frac{a}{n}\right) = \left(\frac{\sqrt{2}b}{n}\right)$. Since

$$\left(\frac{a}{n}\right) = \left(\frac{n}{|a|}\right) = \left(\frac{a^2 + 8b^2}{|a|}\right) = \left(\frac{2}{|a|}\right) = (-1)^{\frac{a^2 - 1}{8}}$$

and

$$\left(\frac{b}{n}\right) = \left(\frac{n}{b'}\right) = \left(\frac{a^2 + 8b^2}{b'}\right) = 1, \quad b' = \text{odd part of } |b|,$$

we have $(-1)^{\frac{a^2-1}{8}} = \left(\frac{\sqrt{2}}{n}\right)$. By [LT00, Lemma-Definition 1], $2 \mid b$ if and only if

$$1 = (-1)^{\frac{n-a^2}{8}} = (-1)^{\frac{n-1}{8}} \left(\frac{\sqrt{2}}{n}\right)$$
$$= \prod_{p|n} (-1)^{\frac{p-1}{8}} \left(\frac{\sqrt{2}}{p}\right)$$
$$= \prod_{p|n} \left(\frac{1+\sqrt{2}}{p}\right) = \left(\frac{1+\sqrt{2}}{n}\right).$$

This is equivalent to (iii)-(vii) by [Wan16, Theorem 4.2]. Note that

$$\left(\frac{\mu}{n}\right) = \left(\frac{n}{|\mu|}\right) = \left(\frac{2\mu^2 - \tau^2}{|\mu|}\right) = \left(\frac{-1}{|\mu|}\right)$$

we have $(vi) \iff (viii)$.

4. The even case

Theorem 4.1. Let $n = 2p_1 \cdots p_k \equiv 2 \mod 8$ be a square-free positive integer with $p_i \equiv \pm 1 \mod 8$. The following are equivalent:

(i)
$$h_4(-n/2) = 1$$
 and $\left(\frac{2-\sqrt{2}}{|d|}\right) = -1$;

 $\begin{array}{l} (i) \ h_4(-n/2) = 1 \ and \left(\frac{2-\sqrt{2}}{|d|}\right) = -1; \\ (ii) \ \mathrm{rank}_{\mathbb{Z}} E_n(\mathbb{Q}) = 0 \ and \ \mathrm{III}(E_n/\mathbb{Q})[2^{\infty}] \cong (\mathbb{Z}/2\mathbb{Z})^2. \end{array}$

Here, $d \neq 1$ is the unique divisor of n such that $(d, n)_v = 1, \forall v \text{ and } d \equiv 1 \mod 8$.

Proof. In this case, $\mathbf{D}_2 = \mathbf{O}$ and the Monsky matrix (2.6) is

$$\mathbf{M}_n = \begin{pmatrix} \mathbf{A}^{\mathrm{T}} & \mathbf{D}_{-1} \\ & \mathbf{A} \end{pmatrix}.$$

Since $\mathbf{A}\mathbf{1} = \mathbf{0}$, we have rank $(\mathbf{A}) \leq k - 1$. The equation $\mathbf{M}_n \begin{pmatrix} \mathbf{x} \\ \mathbf{y} \end{pmatrix} = \mathbf{0}$ can be written

$$\mathbf{A}^{\mathrm{T}}\mathbf{x} = \mathbf{D}_{-1}\mathbf{y}, \quad \mathbf{A}\mathbf{y} = \mathbf{0}.$$

If y = 0, then $A^{T}x = 0$, which has at least two solutions. If y = 1, then $A^{T}(x + 1)$ 1) = 0, which has at least two solutions. Hence $s_2(n) = \dim_{\mathbb{F}_2} \operatorname{Ker} \mathbf{M}_n \geq 2$ and we have

$$s_2(n) = 2 \iff \operatorname{rank}(\mathbf{A}) = k - 1.$$

Denote by n' = n/2. Since the Rédei matrix

$$\mathbf{R}_{-n'} = \left(egin{smallmatrix} \mathbf{A} & \mathbf{0} \\ \mathbf{b}_{-1}^{\mathrm{T}} & 0 \end{smallmatrix}
ight)$$

and note that $\mathbf{1}^{\mathrm{T}}\mathbf{A} = \mathbf{b}_{-1}^{\mathrm{T}}$, we have

$$s_2(n) = 2 \iff h_4(-n/2) = 1$$

by (2.9) and (2.10).

From the definition of d, we know that $\operatorname{Ker} \mathbf{A}^{\mathrm{T}} = \{\mathbf{0}, \psi^{-1}(|d|)\}$. The pure 2-Selmer group of E is

$$\{(1,1,1),(d,1,d),(d,n',dn'),(1,n',n')\}$$

by (2.7). Denote by $\Lambda = (1, n', n')$ and $\Lambda' = (d, 1, d)$. Then D_{Λ} is defined by

(4.1)
$$\begin{cases} H_1: & -2t^2 + u_2^2 - u_3^2 = 0, \\ H_2: & -2n't^2 + n'u_3^2 - u_1^2 = 0, \\ H_3: & 4n't^2 + u_1^2 - n'u_2^2 = 0. \end{cases}$$

Choose

$$Q_1 = (0, 1, 1) \in H_1(\mathbb{Q}),$$
 $L_1 = u_2 - u_3,$ $Q_3 = (n' - 1, 4n', 2n' + 2) \in H_3(\mathbb{Q}),$ $L_3 = 2(n' - 1)t + 2u_1 - (n' + 1)u_2.$

By Lemma 2.1,

$$\langle \Lambda, \Lambda' \rangle = \prod_{p|2n} (L_1 L_3(P_p), d)_p$$

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

When $p \mid n$, take $(t, u_1, u_2, u_3) = (1, 0, 2, \sqrt{2})$. Then

$$(L_1L_3(P_p), d)_p = (-2(2-\sqrt{2}), d)_p = (\sqrt{2}-2, d)_p.$$

When p = 2, take $(t, u_1, u_2, u_3) = (0, \sqrt{n'}, 1, -1)$. Then

$$L_1L_3(P_2) = 2(2\sqrt{n'} - n' - 1) = -2(\sqrt{n'} - 1)^2$$

and $(L_1L_3(P_2), d)_2 = (-2, d)_2 = (-1, d)_2$. Hence

$$\langle \Lambda, \Lambda' \rangle = (-1, d)_2 \prod_{p|d} (\sqrt{2} - 2, d)_p = \left(\frac{2 - \sqrt{2}}{|d|}\right).$$

Conclude the result by Lemma 3.1.

Corollary 4.2. Let $n = 2p_1 \cdots p_k \equiv 2 \mod 8$ be a square-free positive integer with $p_i \equiv 1 \mod 8$. The following are equivalent:

- (i) $r_4(K_2\mathcal{O}_{\mathbb{Q}(\sqrt{-n})}) = 0;$
- (ii) $\operatorname{rank}_{\mathbb{Z}} E_n(\mathbb{Q}) = 0$ and $\operatorname{III}(E_n/\mathbb{Q})[2^{\infty}] \cong (\mathbb{Z}/2\mathbb{Z})^2$.

Proof. Since all $p_i \equiv 1 \mod 8$, we have $\mathbf{D}_{\varepsilon} = \mathbf{O}$ and $\mathbf{b}_{\varepsilon} = \mathbf{0}$ for any $\varepsilon = \pm 1, \pm 2$. Note that d = n' in Theorem 4.1, the condition (ii) is equivalent to rank $(\mathbf{A}) = k - 1$ and $\left(\frac{2-\sqrt{2}}{n'}\right) = -1$.

Denote by $F = \mathbb{Q}(\sqrt{-n})$ and write $-n = 2\mu^2 - \lambda^2, \mu, \lambda \in \mathbb{N}$. Combining with Theorem 2.5 and (2.12), we have

$$2^{r_4(K_2\mathcal{O}_F)+2} = 2\#\{\mathbf{d} : \mathbf{Ad} = \mathbf{0}\} + 2\#\{\mathbf{Ad} = \mathbf{b}_{|\mu|} = \mathbf{b}_{\mu}\}$$

and Ker $\mathbf{A} \supseteq \{\mathbf{0}, \mathbf{1}\}$. Therefore, $r_4(K_2\mathcal{O}_F) = 0$ if and only if Ker $\mathbf{A} = \{\mathbf{0}, \mathbf{1}\}$ and $\mathbf{Ad} = \mathbf{b}_{\mu}$ is not solvable. Once we have Ker $\mathbf{A} = \{\mathbf{0}, \mathbf{1}\}$, we will get rank $(\mathbf{A}) = k-1$. Since $\mathbf{1}^T \mathbf{A} = \mathbf{0}^T$, we will have Im $\mathbf{A} = \{\mathbf{d} : \mathbf{1}^T \mathbf{d} = 0\}$. Hence $\mathbf{Ad} = \mathbf{b}_{\mu}$ is solvable if and only if $(\frac{\mu}{n'}) = 1$.

Denote by $u = \lambda - \mu$ and $w = -\lambda/2 + \mu$. Then $n' = u^2 - 2w^2$ and

$$\left(\frac{\mu}{n'}\right) = \left(\frac{u+2w}{n'}\right) = \left(\frac{(2\pm\sqrt{2})w}{n'}\right).$$

The result then follows from

$$\left(\frac{w}{n'}\right) = \left(\frac{n'}{w'}\right) = \left(\frac{u^2 - 2w^2}{w'}\right) = \left(\frac{u^2}{w'}\right) = 1,$$

where w' is the positive odd part of w.

References

- [BC69] Pierre Barrucand and Harvey Cohn. Note on primes of type $x^2 + 32y^2$, class number, and residuacity. J. Reine Angew. Math., 238:67–70, 1969.
- [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. volume 494, pages 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.
- [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.
- [LT00] Delang Li and Ye Tian. On the Birch-Swinnerton-Dyer conjecture of elliptic curves $E_D: y^2 = x^3 D^2x$. Acta Math. Sin. (Engl. Ser.), 16(2):229–236, 2000.
- [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 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.
- [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.
- [Qin21] Hourong Qin. Congruent numbers, quadratic forms and K_2 . Math. Ann., 2021.
- [R34] 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.
- [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.
- [Wei13] Charles A. Weibel. *The K-book*, volume 145 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, 2013. An introduction to algebraic K-theory.

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