Abstract

We study a subclass of congruent elliptic curves $E^{(n)} : y^2 = x^3 - n^2x$, where $n$ is a positive integer congruent to 1 (mod 8) with all prime factors congruent to 1 (mod 4). We characterize such $E^{(n)}$ with Mordell-Weil rank zero and 2-primary part of Shafarevich-Tate group isomorphic to $(\mathbb{Z}/2\mathbb{Z})^2$. We also discuss such $E^{(n)}$ with 2-primary part of Shafarevich-Tate group isomorphic to $(\mathbb{Z}/2\mathbb{Z})^{2k}$ with $k \geq 2$.

1 Introduction

A positive integer $n$ is called a congruent number if it is the area of a right triangle with rational lengths, which is equivalent the congruent elliptic curve $E^{(n)} : y^2 = x^3 - n^2x$ has positive Mordell-Weil rank. Heegner [1] proved that any prime number $p \equiv 5 \pmod{8}$ is a congruent number. Recently, Tian [2] introduced the induction method involving $L$-value and as a corollary he proved that: for any $k \geq 1$, there are infinitely many square-free congruent number $n \equiv 1 \pmod{8}$ with exactly $k$ prime divisors.

In this paper, we mainly study rank zero congruent elliptic curves with 2-primary part of Shafarevich-Tate group non-trivial. Li-Tian [3] considered those $n$ with all prime factors congruent to 1 (mod 8). They found a sufficient condition for $n$ to be a non-congruent number with $\mathbb{X}(E^{(n)}/\mathbb{Q})[2\infty] \simeq (\mathbb{Z}/2\mathbb{Z})^2$. Rhoades [4] suspected that their condition is also necessary, which is proved in Theorem 3 of this paper. Under our case, Ouyang-Zhang [5] also found a sufficient condition for $n \equiv 1 \pmod{8}$ non-congruent with $\mathbb{X}(E^{(n)}/\mathbb{Q})[2\infty] \simeq (\mathbb{Z}/2\mathbb{Z})^2$.

To state our characterization, we introduce some notations. For a positive square-free integer $n$, let $\mathcal{A}_n$ denote the ideal class group of $K = \mathbb{Q}(\sqrt{-n})$ and $D$ be the fundamental discriminant of $K$. We denote $D$ to be the set of all positive square-free divisors of $D$. Then $D$ has a group structure. Gauss genus theory (see Proposition 2) implies that there is a 2 to 1 correspondence $\theta$ between $D \cap N(K^\times)$ and $\mathcal{A}_n[2] \cap 2A_n$. Here $N(K^\times)$ denotes the image of the norm map from $K^\times$ to $\mathbb{Q}^\times$, $\mathcal{A}_n[2]$ denotes the 2-elementary subgroup of $\mathcal{A}_n$, and $2A_n$ denotes the subgroup of the square elements in $\mathcal{A}_n$. We define the 2-rank $h_2(n)$ of $\mathbb{Q}(\sqrt{-n})$ by rank$_{2^i}2^{i-1}\mathcal{A}_n/2^iA_n$ for $i \geq 1$. Then we have $h_4(n) = \text{rank}_{2^2}\mathcal{A}_n[2] \cap 2A_n$. If $h_4(n) = 1$, then there exist $d_1, d_2 \in D$ corresponding to the non-trivial element in $\mathcal{A}_n[2] \cap 2A_n$. Moreover if $n \equiv 1 \pmod{8}$ with all prime factors congruent to 1 (mod 4),

---

1 Congruent Elliptic Curves with Non-trivial Shafarevich-Tate Groups. SCIENCE CHINA Mathematics, Doi: 10.1007/s11425-015-0741-3
then the product of odd part $d'_i$ of $d_i$ equals $n$. This is because the kernel of $\theta$ is \{1, $n$\} in this case. Then we denote $d = d(n)$ be the maximal integer of $d'_1, d'_2$.

Now we can state our first main result.

**Theorem 1.** Let $n$ be a positive square-free integer congruent to 1 (mod 8) with all prime factors congruent to 1 (mod 4) distinct and $h_4(n) = 1$, then the following are equivalent:

(i) $h_8(n) \equiv \frac{d(n) - 1}{4} \pmod{2}$;

(ii) $\text{rank}_2 E^{(n)}(\mathbb{Q}) = 0$ and $\text{III}(E^{(n)}/\mathbb{Q})[2^\infty] \simeq (\mathbb{Z}/2\mathbb{Z})^2$.

The strategy of the proof of Theorem 1 is the following.

- Note that a necessary condition of (ii) holds is $s_2(n) = 2$, where $s_2(n)$ is the pure 2-Selmer rank given by $\text{rank}_2 \text{Sel}_2(E^{(n)})/E^{(n)}[2](\mathbb{Q})$. By Monsky matrix ($\S 2.1$) and Redei matrix ($\S 3.1$), we deduce that $s_2(n) = 2$ is equivalent to $h_4(n) = 1$.

- From the short exact sequence $0 \to E^{(n)}[2] \to E^{(n)}[4] \xrightarrow{\times 2} E^{(n)}[2] \to 0$, we derive the following long exact sequence

$$0 \to E^{(n)}[2](\mathbb{Q})/2E^{(n)}[4](\mathbb{Q}) \to \text{Sel}_2(E^{(n)}) \to \text{Sel}_4(E^{(n)}) \to \text{ImSel}_4(E^{(n)}) \to 0 \quad (1.1)$$

Moreover Cassels [6] introduced a pairing on $\text{Sel}_2(E^{(n)})/E^{(n)}[2](\mathbb{Q})$ with kernel given by $\text{ImSel}_4(E^{(n)})/E^{(n)}[2](\mathbb{Q})$ ($\S 2.2$). Note that (ii) is equivalent to $\#\text{Sel}_2(E^{(n)}) = \#\text{Sel}_4(E^{(n)})$, which is equivalent to $\#E^{(n)}[2](\mathbb{Q})/2E^{(n)}[4](\mathbb{Q}) = \#\text{ImSel}_4(E^{(n)})$ by the long exact sequence. From the Cassels pairing, we know (ii) is equivalent to the Cassels pairing is non-degenerate.

- Gauss pairing is computable($\S 4.1$), its non-degeneration in this case is equivalent to a quartic residue symbol.

- Gauss genus theory ($\S 3.2$) reduces this residue symbol to 8-rank $h_8(n)$ of $\mathbb{Q}(\sqrt{-n})$.

For the case $k \geq 2$, we have the following second main result.

**Theorem 2.** Let $n$ be a positive square-free integer with all prime factors congruent to 1 (mod 8) and $k$ be a positive integer. Assume that either $h_8(n) = k - 1$ with the ideal class $[(2, \sqrt{-n})] \not\equiv 4A_n$ or $h_8(n) = k$. If $n$ has a decomposition $d_1 \cdots d_k$ with $d_i > 1$ satisfying the following ideal class group conditions:

1. $h_4(d_i) = 1, 1 \leq i \leq k$;

2. $\left(\frac{p_{i_1}}{p_{i_2}}\right) = 1$ for any prime divisor $p_{i_j}$ of $d_{i_j}$ with $i_1 \neq i_2$, where $(;)$ is the Legendre symbol;

3. $h_8(d_i) = 0, 1 \leq i \leq k$.

Then

$$\text{rank}_2 E^{(n)}(\mathbb{Q}) = 0, \quad \text{III}(E^{(n)}/\mathbb{Q})[2^\infty] \simeq (\mathbb{Z}/2\mathbb{Z})^{2k} \quad (1.2)$$

We remark that for $k = 2$, the condition is not empty by Remark 4. And in $\S 4.2$ we can get congruent elliptic curves such that (1.2) holds under a more general condition (see Theorem 4). As to the distribution result of elliptic curves in Theorems 1 and 2 we will study this in a coming paper [7] but with Theorem 2 limited to $k = 2$. 

2
2 Congruent Elliptic Curves

Let $E^{(n)}$ be the congruent elliptic curve $y^2 = x^3 - n^2x$ defined over $\mathbb{Q}$, where $n$ is a positive square-free integer. Then from classical result, we can identify the 2-Selmer group of $E^{(n)}$ with:

$$\text{Sel}_2(E^{(n)}) = \left\{ \Lambda = (d_1, d_2, d_3) \in (\mathbb{Q}^\times/\mathbb{Q}^\times 2)^3 \mid D_\Lambda(\Lambda) \neq \emptyset, \ d_1d_2d_3 \in \mathbb{Q}^\times 2 \right\}$$

where $\Lambda$ is the adele ring over $\mathbb{Q}$ and for $\Lambda = (d_1, d_2, d_3), D_\Lambda$ is a genus one curve in $\mathbb{P}^3$ 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, $E^{(n)}(\mathbb{Q})/2E^{(n)}(\mathbb{Q})$ is given by: $(x - n, x + n, x)$ if $(x, y) \in E^{(n)}(\mathbb{Q}) - E^{(n)}(\mathbb{Q})[2]$ and $E^{(n)}(\mathbb{Q})[2]$ corresponds to

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

Then these 4 elements correspond to $(n, 0), (-n, 0), (0, 0), O$ respectively under the Kummer map.

2.1 Monsky Matrix

Monsky (see the appendix of Heath-Brown [8]) represented $\text{Sel}_2(E^{(n)}/E^{(n)}(\mathbb{Q})[2]$ with the kernel of a $2k \times 2k$ matrix $M$ over $\mathbb{F}_2$, which is closely related to 4-rank of $\mathbb{Q}(\sqrt{-n})$.

Before introducing the Monsky matrix, we define the additive Legendre symbol $\left[ \frac{a}{p} \right]$, where $p$ is a prime and $a$ an integer coprime to $p$, it is 0 if the Legendre symbol $\left( \frac{a}{p} \right) = 1$ and 1 otherwise.

For a positive square-free odd integer $n = p_1 \cdots p_k$, the corresponding Monsky matrix $M_n$ is defined by:

$$M_n = \left( \begin{array}{cc}
A + D_{-2} & D_2 \\
D_2 & A + D_2
\end{array} \right)$$

where $D_a = \text{diag}\left\{ \left[ \frac{n}{p_1} \right], \ldots, \left[ \frac{n}{p_k} \right] \right\}$ and $A = (a_{ij})_{k \times k}$ with $a_{ij} = \left[ \frac{p_i}{p_j} \right]$ if $i \neq j$, and $a_{ii} = \sum_{j \neq i} a_{ij}$.

To connect $\text{Sel}_2(E^{(n)})/E^{(n)}(\mathbb{Q})[2]$ with the kernel of corresponding Monsky matrix, we first choose representatives of $\text{Sel}_2(E^{(n)})/E^{(n)}(\mathbb{Q})[2]$ with nice properties, see the following lemma:

Lemma 1. For a positive square-free odd integer $n$, the following holds:

(1) Any $\Lambda \in \text{Sel}_2(E^{(n)})$ can be represented by $(d_1, d_2, d_3)$ with $d_i$ square-free integers, $d_2 > 0, d_1|2n, d_2|2n$ and $d_1, d_2$ have the same parity;

(2) Assume that all elements in $\text{Sel}_2(E^{(n)})$ have representatives as in (1), then for any $\Lambda \in \text{Sel}_2(E^{(n)})$, there is a unique $\Lambda_0 \in E^{(n)}(\mathbb{Q})[2]$ such that $\Lambda \Lambda_0 = (d_1, d_2, d_3)$ with $d_1 > 0, d_2 > 0, d_1|n, d_2|n;$
Proof. (1): Since \(d_i \in \mathbb{Q}^\times / \mathbb{Q}^{\times 2}\), we may chose \(d_i\) square-free integers. For \(\Lambda \in \text{Sel}_2(E^{(n)})\) we have \(D_\Lambda(\mathbb{R}) \neq \emptyset\), this implies that \(d_2 > 0\).

If \(d_1 \nmid 2n\), then there is a prime divisor \(p|d_1\) with \(p \nmid 2n\). Since \(d_1d_2d_3 \in \mathbb{Q}^{\times 2}\), hence \(p|d_2d_3\), we assume \(p|d_2\), which implies \(p \nmid d_3\). Consider \(D_\Lambda(\mathbb{Q}_p)\): from \(H_3\) we know that \(p|t\), then use \(H_1\) and \(p|d_2, p \nmid d_3\) we get \(p|u_3\). Comparing \(p\)-divisibility of two sides of \(H_2\), we get \(p|u_1\). Again consider \(H_3\), then \(p|u_2\) by counting \(p\)-divisibility of two sides. We arrive at \(p|(t, u_1, u_2, u_3)\), then we can easily get they are infinitely \(p\)-divisible, which is impossible, hence \(d_1|2n\). Similarly \(d_2|2n\).

\(d_1, d_2\) has same parity: as else \(2\) divide exact one of \(d_1, d_2\), for example \(2|d_1\), then \(2 \nmid d_2\), this implies \(2|d_3\), so from \(H_3\) we know \(2|u_2\) and from \(H_2\) we know \(2|t\), then by \(2\)-divisibility of \(H_3\), we get \(2|u_1\), again by \(2\)-divisibility of \(H_2\), we get \(2|u_3\), hence \(2|(t, u_1, u_2, u_3)\), same argument as above implies this is impossible, hence \(d_1, d_2\) has same parity.

(2): If \(d_1\) is even, then by (1) so is \(d_2\), then \(\Lambda_0 = (2, 2n, n)\) is the unique element in \(E^{(n)}(\mathbb{Q})[2]\) with the required property if \(d_1 > 0\), else \((-2n, 2, -n)\) is the unique one. If \(d_1\) is odd, then so is \(d_2\), if \(d_1 < 0\) then \((-n, n, 1)\) is the unique element satisfying the required property, else \((1, 1, 1)\) is.

For the representatives of \(\text{Sel}_2(E^{(n)})/E^{(n)}(\mathbb{Q})[2]\) as in (2) of Lemma \(\text{I}\) we have a bijection

\[
\text{Sel}_2(E^{(n)})/E^{(n)}(\mathbb{Q})[2] \rightarrow \left\{ x \in \mathbb{F}_2^{2k} \mid M_nx = 0 \right\}
\]

(2.2) given by \((d_1, d_2, d_3) \mapsto (v_{p_1}(d_1), \cdots, v_{p_k}(d_1), v_{p_1}(d_2), \cdots, v_{p_k}(d_2))^T\), where \(v_p(d)\) denotes the \(p\)-adic valuation of \(d\).

Now we explain why (2.2) is a bijection: For \(\Lambda\) chosen as in (2) of Lemma \(\text{I}\) we have \(D_\Lambda(\mathbb{Q}_p) \neq \emptyset\) for \(p \nmid n\), while for \(p|n\) the local solvability of \(D_\Lambda\) is:

1. \(p \nmid d_1, p \nmid d_2\) : \(\left( \frac{d_1}{p} \right) = \left( \frac{d_2}{p} \right) = 1\);
2. \(p \nmid d_1, p|d_2\) : \(\left( \frac{2d_1}{p} \right) = \left( \frac{2n/d_2}{p} \right) = 1\);
3. \(p|d_1, p \nmid d_2\) : \(\left( \frac{-2n/d_1}{p} \right) = \left( \frac{2d_2}{p} \right) = 1\);
4. \(p|d_1, p|d_2\) : \(\left( \frac{-n/d_1}{p} \right) = \left( \frac{n/d_2}{p} \right) = 1\).

Assume \(d_1 = \prod_{i=1}^k p_i^{x_i}, d_2 = \prod_{i=1}^k p_i^{y_i}\), then the above says that: for \(p_i\)

\[
x_1 \sum_{i \neq j} \left[ \frac{p_i}{p_j} \right] x_j + \sum_{i \neq j} x_j \left[ \frac{d_1}{p_j} \right] = x_1 \left[ \frac{n/d_1}{p_i} \right] + (1 - x_1) \left[ \frac{d_1}{p_i} \right] = \left[ \frac{-2}{p_i} \right] x_i + \left[ \frac{2}{p_i} \right] y_i
\]

\[
y_1 \sum_{i \neq j} \left[ \frac{p_i}{p_j} \right] y_j + \sum_{i \neq j} y_j \left[ \frac{d_2}{p_j} \right] = y_1 \left[ \frac{n/d_2}{p_i} \right] + (1 - y_1) \left[ \frac{d_2}{p_i} \right] = \left[ \frac{2}{p_i} \right] x_i + \left[ \frac{2}{p_i} \right] y_i
\]

Hence the map (2.2) is a bijection.

Moreover, Monsky proved that \(M\) has even rank if \(n \equiv 1, 3 \pmod{8}\).

### 2.2 Cassels Pairsing

Cassels \(\text{II}\) introduced a skew-symmetric bilinear pairing on the \(\mathbb{F}_2\)-vector space \(\text{Sel}_2(E^{(n)})/E^{(n)}(\mathbb{Q})[2]\):

\[
\langle , \rangle : \text{Sel}_2(E^{(n)})/E^{(n)}(\mathbb{Q})[2] \times \text{Sel}_2(E^{(n)})/E^{(n)}(\mathbb{Q})[2] \rightarrow \{ \pm 1 \}
\]

(2.3)
It is defined as follows: for any \( \Lambda = (d_1, d_2, d_3), \Lambda' = (d'_1, d'_2, d'_3) \in \text{Sel}_2(E^{(n)}), \) let \( D_{\Lambda} \) be the genus one curve corresponding to \( \Lambda \) and \( Q_i \in H_i(\mathbb{Q}) \) be a global point on \( H_i \), the existence of \( Q_i \) follows from Hasse-Minkovski principle, since \( H_i \) is locally solvable everywhere as \( D_{\Lambda} \) is so. Let \( L_i \) be the tangent line of \( H_i \) at \( Q_i \) and view it as a hyperplane in \( \mathbb{P}^3 \). Let \( P = (P_p) \in D_{\Lambda}(\mathbb{A}) \) be any adelic point on \( D_{\Lambda} \), then

\[
\langle \Lambda, \Lambda' \rangle_p = \prod_p \langle \Lambda, \Lambda' \rangle_p, \quad \langle \Lambda, \Lambda' \rangle_p = \prod_{i=1}^3 \left( L_i(P_p), d'_i \right)_p
\]

where \( p \) runs over all places of \( \mathbb{Q} \) and \( (\cdot, \cdot)_p \) is the Hilbert symbol at \( \mathbb{Q}_p \).

Note that skew-symmetry over \( \mathbb{F}_2 \) is also symmetry, so the left kernel and right kernel of the Cassels pairing \( (\cdot, \cdot) \) are the same. An important property of Cassels pairing says that the kernel of the Cassels pairing is

\[
\text{ImSel}_4(E^{(n)})/E^{(n)}(\mathbb{Q})[2]
\]

where \( \text{ImSel}_4(E^{(n)}) \) is associated to the long exact sequence derived from

\[
0 \to E[2] \to E[4] \xrightarrow{\times 2} E[2] \to 0.
\]

In fact almost all local Cassels pairing are 1.

**Lemma 2** (Cassels\cite{6} Lemma 7.2). The local Cassels pairing \( (\cdot, \cdot)_p = +1 \) if \( p \) satisfying

1. \( p \neq 2, \infty; \)
2. The coefficients of \( H_i \) and \( L_i \) are all integral at \( p \) for \( i = 1, 2, 3; \)
3. Modulo \( D_{\Lambda} \) and \( L_i \) by \( p \), they define a curve of genus 1 over \( \mathbb{F}_p \), together with tangents to it.

### 3 Gauss Genus Theory

In this section, we will introduce Gauss genus theory: classical theory, 4-rank and Redei matrix, 8-rank and higher Redei matrix.

Let \( K \) be an imaginary quadratic number field with fundamental discriminant \( D \) and ideal class group \( \mathcal{A} \) (written additively). The classical Gauss genus theory characterize \( \mathcal{A}[2] \) and \( 2\mathcal{A} \), where \( \mathcal{A}[2] \) consists of all those ideal classes killed by 2 and \( 2\mathcal{A} \) denotes all those ideal classes which are squares.

To state Gauss genus theorem, we give some notations: let \( p_1, \ldots, p_t \) be the different prime divisors of \( D \), \( \mathcal{O}_K \) the ring of algebraic integers of \( K \). \( N = N_{K/\mathbb{Q}} \) is the norm from \( K \) to \( \mathbb{Q} \) and \( \alpha_0 \) is the integer \( \frac{D + \sqrt{D}}{2} \), whence we have \( \mathcal{O}_K = \mathbb{Z} + \mathbb{Z} \alpha_0 \). In this section we use \( (a, b) \) to denote the greatest common divisor of \( a, b \) if \( a, b \in \mathbb{Z} \) else the ideal generated by \( a, b \) if \( a, b \in K \). We also use \( (c_1, \cdots, c_k) \) to denote a vector in \( \mathbb{F}_2^k \). We hope this will not cause confusion since we can tell apart them easily from the context.

**Proposition 1.**

1. \( \mathcal{A}[2] \) is an elementary abelian 2-group generated by the ideal classes \( [(p_i, \alpha_0)] \) and \( \text{rank}_{\mathbb{F}_2} \mathcal{A}[2] = t - 1; \)
2. For an ideal \( \mathfrak{a} \), then \( [\mathfrak{a}] \in 2\mathcal{A} \) if and only if there is a non-zero integer \( z \) and \( \mathfrak{a} \in \mathfrak{a} \) such that: \( z^2 \cdot N\mathfrak{a} = N \mathfrak{a} \).

For the proof of Proposition\cite{1} we refer to Chapter 7 of Hecke\cite{9}, there is also an elementary proof see Nemenzo-Wada\cite{10}.  

5
3.1 4-rank and Redei matrix

To deal with 4-rank and 8-rank, we will prove some well-known results, these can be seen in some papers( for example Jung-Yue [11] ) but with no proof. As we mentioned in the introduction, we will relate $\mathcal{A}[2] \cap 2\mathcal{A}$ with norm elements of $K^\times$, solving quadratic homogeneous Diophantine equation and also Redei matrix. Note that we have $h_4(\mathcal{A}) = \text{rank}_{\mathbb{Z}_2}\mathcal{A}[2] \cap 2\mathcal{A}$, so the 4-rank is reduced to study $\mathcal{A}[2] \cap 2\mathcal{A}$. Now we first set up the $2-1$ correspondence on $\mathcal{A}[2] \cap 2\mathcal{A}$.

**Proposition 2.** The following map is an epimorphism

$$\theta : \mathcal{D}(K) \cap N_{K/\mathbb{Q}}(K^\times) \to \mathcal{A}[2] \cap 2\mathcal{A}, \quad d \mapsto [(d, \alpha_0)]$$

with $\text{Ker}(\theta) = \{1, -D'\}$, where $D'$ denotes the square-free part of $D$ and $\mathcal{D}(K)$ denotes all those positive square-free divisors of $D$ with group multiplication

$$d_1 \odot d_2 := \frac{d_1 d_2}{(d_1, d_2)^2}$$

**Proof.** First $\theta$ is well-defined: For any $d \in \mathcal{D}(K) \cap N_{K/\mathbb{Q}}(K^\times)$, then $\theta(d) = [(d, \alpha_0)] \in \mathcal{A}[2]$ since $d|D$ as $d \in \mathcal{D}(K)$. From $d \in N_{K/\mathbb{Q}}(K^\times)$, we know there is some $\alpha \in K^\times$ such that $d = N\alpha$, then by multiply a suitable positive integer $z$, we can write $z\alpha = xd + y\alpha_0 \in (d, \alpha_0)$. Hence from Proposition $[\ref{prop:kernel}]$ we get $\theta(d) = [(d, \alpha_0)] \in 2\mathcal{A}$ since $(d, \alpha_0)$ has norm $d$.

Second $\theta$ is a homomorphism: For any $d_1 \in \mathcal{D}(K) \cap N_{K/\mathbb{Q}}(K^\times)$, if $(d_1, d_2) = 1$ then we have the following ideal equalities( note multiplication of ideals is written additively )

$$(d_1, \alpha_0) + (d_2, \alpha_0) = (d_1 d_2, \alpha_0, d_1 \cdot \alpha_0, d_2 \cdot \alpha_0) = (d_1 d_2, \alpha_0) \quad (3.1)$$

Then for general $d_1, d_2$ we have $d_i = \frac{d_i}{(d_1, d_2)} \cdot (d_1, d_2)$, whence from equation $[\ref{eq:ideal}]$ we have

$$(d_i, \alpha_0) = \left(\frac{d_i}{(d_1, d_2)}, \alpha_0\right) + \left((d_1, d_2), \alpha_0\right)$$

Consequently

$$(d_1, \alpha_0) + (d_2, \alpha_0) = 2\left((d_1, d_2), \alpha_0\right) + \sum_{i=1}^{2} \left(\frac{d_i}{(d_1, d_2)}, \alpha_0\right) = 2\left((d_1, d_2), \alpha_0\right) + (d_1 \odot d_2, \alpha_0)$$

Thus we have

$$\theta(d_1) + \theta(d_2) = \theta(d_1 \odot d_2)$$

Hence $\theta$ is a group homomorphism.

Now we show that $\theta$ is surjective: It is clear from genus theory ( see Proposition $[\ref{prop:genus}]$ ), every element of $\mathcal{A}[2]$ is of the form $[(d, \alpha_0)]$ with $d$ a positive square-free divisor $D$. So for any $[a] \in \mathcal{A}[2] \cap 2\mathcal{A}$, there is a $d \in \mathcal{D}(K)$, such that $[a] = [(d, \alpha_0)]$. Since $[(d, \alpha_0)] \in 2\mathcal{A}$, then by Proposition $[\ref{prop:existence}]$ there is a non-zero integer $z$ and an $\alpha \in (d, \alpha_0)$ such that

$$z^2d = z^2 \cdot N_{K/\mathbb{Q}}\{(d, \alpha_0)\} = N\alpha$$

Therefore $d \in N_{K/\mathbb{Q}}(K^\times)$.

We begin to determine the kernel of $\theta$: For any $d \in \text{Ker}(\theta)$, then $d|D$ is a positive square-free integer such that $d = N(\beta)$ and $(d, \alpha_0) = (\alpha)$ is a principal ideal. Thus there are integers $x, y \in \mathcal{O}_K$ such that

$$\alpha = xd + y\alpha_0$$
Let \( x = m + na_0, y = m' + n'a_0 \in \mathcal{O}_K \) with \( m, n, m', n' \in \mathbb{Z} \), then
\[
\alpha = ud + v\sqrt{D}
\]
where
\[
u = m + \frac{D}{2d} \cdot (nd + m') + n' \cdot \frac{D(D+1)}{4d}, \quad v = \frac{nd + n'D + m'}{2}
\]
Hence \( N\alpha = d \left( du^2 + \frac{-D}{d}v^2 \right) = N \{(d, \alpha_0)\} = d \), then
\[
du^2 + \frac{-D}{d}v^2 = 1 \tag{3.2}
\]
(i): If \( D \equiv 1 \pmod{4} \), then \( d, \frac{D}{d} \) are odd and \( 2u, 2v \in \mathbb{Z} \), then from equation (3.2) we get
\[
d(2u)^2 + \frac{-D}{d}(2v)^2 = 4
\]
Note that the Diophantine equation \( ar^2 + bs^2 = 4 \) with \( a, b \) positive odd integer and \( ab \equiv 3 \pmod{4} \) has integer solution only if \( a = 1 \) or \( b = 1 \), hence \( d = 1 \) or \( \frac{-D}{d} = 1 \), thus we have two solutions \( d = 1 \) or \(-D\).

(ii): If \( 4 \mid D \), we assume that \( D \neq -4 \), else it is trivial. Now we divided into two cases according to \( d \)'s parity:

If \( d \) is odd, then \( u, 2v \in \mathbb{Z} \) and \( 4d \mid D \), thus from equation (3.2) we get
\[
du^2 + \frac{-D}{4d}(2v)^2 = 1
\]
Then from the solvability of the Diophantine equation \( ar^2 + bs^2 = 1 \) with \( a, b \) positive odd, we get \( d = 1 \) or \( \frac{-D}{d} = 1 \), the latter solution requires that \( 4 \mid |D| \) since \( d \) is odd.

If \( d \) is even, then \( 2u, 2v \in \mathbb{Z} \), and \( 2 \mid d \), \( 4 \nmid d \), \( \frac{-D}{d} \), thus from equation (3.2) we get:
\[
d(2u)^2 + \frac{-D}{d}(2v)^2 = 4
\]
Note the Diophantine equation \( at^2 + bs^2 = 4 \) with \( a, b \) positive even integer and \( 4 \nmid a \) can have integral solution only if \( a = b = 2 \) or \( b = 4 \): the first case requires that \( D = -4 \) which has been excluded; the latter case implies that \( d = \frac{-D}{4} \) and requires \( 8 \mid D \) since \( d \) is even.

In summary, we always have \( \text{Ker}(\theta) = \{1, -D'\} \). This completes the proof. \( \square \)

Now we are ready to introduce the Redei matrix \( R \) (called reduced Redei matrix in Jung-Yue [11] ) of \( K \): first we assume that if \( 2 \mid D \), then \( p_t = 2 \). Then the Redei matrix \( R = (r_{ij}) \) is a \((t-1) \times t\) matrix over \( \mathbb{F}_2 \) defined by:
\[
r_{ii} = \begin{bmatrix} \frac{D}{p_t} \\ p_t \end{bmatrix}, \quad r_{ij} = \begin{bmatrix} p_i \\ p_j \end{bmatrix} \quad \text{if } i \neq j, \quad \text{where } p_i^* = (-1)^{\frac{p_i-1}{2}} p_i
\]
Note \( R \) is very similar to the matrix \( A \) occurring in the definition of Monsky matrix. Now we can relates \( R \) to \( h_4(n) \) via the following isomorphism which is parallel to the Monsky matrix.

**Proposition 3.** The following is an isomorphism:
\[
\mathcal{D}(K) \cap N(K^\times) \to \left\{ X \in \mathbb{F}_2^t | RX = 0 \right\}, \quad d \mapsto X_d := \left( v_{p_1}(d), \ldots, v_{p_t}(d) \right)^T
\]
with inverse map given by \( (x_1, \ldots, x_t)^T \mapsto \prod_{i=1}^t p_i^{x_i} \).
This Proposition is a special case of Proposition 4 with \( c = 1 \). Hence from Proposition 2 and 3 we know that \( h_4(A) = t - 1 - \text{rank}_2 R \).

To deal with 4-rank of \( K \), these propositions are sufficient. But for 8-rank, we have to generalize Proposition 3 to general \( c \), see the following:

**Proposition 4.** Let \( c \) be a positive odd integer coprime with \( D \) such that for any prime divisor \( p \) of \( c \), we have \((\frac{D}{p}) = 1 \). Then the following is an isomorphism:

\[
\left\{ d \in D(K) \left| dc \in N_{K/Q}(K^\times) \right. \right\} \rightarrow \left\{ X \in \mathbb{F}_2^t \left| RX = C \right. \right\} \quad \text{where } C = \left( \frac{c}{p_1}, \cdots, \frac{c}{p_t-1} \right)^T
\]

and the inverse map is given by \((x_1, \cdots, x_t)^T \mapsto \prod_{i=1}^t p_i^{x_i} \).

**Proof.** For \( d \in D(K) \), note that \( dc \in N_{K/Q}(K^\times) \) if and only if the following equation:

\[
de cz^2 = x^2 - Dy^2 \quad (\text{3.3})
\]

is solvable over \( \mathbb{Z} \). Hence modulo equation (3.3) by odd prime divisors of \( D \), we see the solvability of equation (3.3) implies that:

1. \((\frac{-cd/d}{p}) = 1 \) for \( p \mid d \) odd prime divisor;
2. \((\frac{cd}{p}) = 1 \) for \( p \mid -D/d \) odd prime divisor.

But the inverse direction is also true, since we have

**Lemma 3.** The local conditions (1),(2) also implies the solvability of the Diophantine equation (3.3) under the hypothesis of Proposition 4.

**Proof.** of the Lemma:

By Hasse-Minkovski principle, it suffices to show that (3.3) is locally solvable everywhere. For \( p \nmid 2cD \), this is obvious. For \( p \mid c \), this local solvability follows from the hypothesis of Proposition 4. For odd \( p \mid D \), this is just the local conditions (1),(2). So we just need to show that (3.3) is solvable at \( Q_2 \). Whence it suffices to show that the Hilbert symbol \((cd, D)_2 = 1 \).

Let \( d_0 \) and \( \bar{d} \) be the odd part of \( d \), \( -D/d \) respectively and \( 2^s = d/d_0 \). If we use \( s \) to denote the 2-adic valuation of \( D \), then

\[
(c, D)_2 = (c, d_0 \bar{d})_2 \cdot (-2^s c) \cdot (d_0 \bar{d} c) \cdot (c d_0 \bar{d}) = (D/c) \cdot (c d_0 \bar{d}) = (c d_0 \bar{d})
\]

where we have used \((\frac{D}{c}) = 1 \) which follows from the hypothesis of Proposition 4.

Whence we are reduced to show \((d, D)_2 = (c d_0 \bar{d}) \). Note the conditions (1) and (2) imply that: \((\frac{2^{s-r} c d}{d_0}) = 1 \), \((\frac{2^r c d}{d_0}) = 1 \). From either \( d_0 \) or \(-d_0 \) is congruent to 1 (mod 4), we
have \((d_0, -d_0) = 1\). Therefore
\[
(d, D) = \left(2^n d_0, -2^n d_0 \tilde{d}\right) = (2^n, -2^n d_0 \tilde{d})_2 = (d_0, -d_0)_2 \cdot (d_0, \tilde{d})_2
\]
\[
= \left(\frac{2^n}{d_0}, \frac{d_0}{\tilde{d}}\right) \cdot \left(\frac{2^n d_0}{\tilde{d}}\right) = \left(\frac{2^n d_0 d}{\tilde{d}}\right)
\]
This completes the proof of the Lemma.

Thus the expected isomorphism is reduced to show that the local conditions (1) and (2) are equivalent to \(RX_d = C\). Let \(X = (x_1, \cdots, x_t) \in \mathbb{F}_p^t\) such that \(RX = C\), then for any \(1 \leq i \leq t - 1\) we have
\[
\sum_{j \neq i} x_j \left[ \frac{p_j}{p_i} \right] + x_i \left[ \frac{D/p_i^s}{p_i} \right] = \left[ \frac{c}{p_i} \right] \tag{3.4}
\]
If \(x_i = 0\), then \(p_i \mid d := \prod_{i=1}^{t-1} p_i^{r_i}\), and equation (3.4) is equivalent to \(\left( \frac{a_{i-1}}{p_i} \right) = 1\). If \(x_i = 1\), then \(p_i \mid d\), the equation (3.4) is equivalent to \(\left( \frac{-iD/d}{p_i} \right) = 1\).

For \(i = t\): we may assume that \(p_t \neq 2\), whence \(D = -p_1 \cdots p_t \equiv 1 \pmod{4}\). Then add all equations in (3.4) we get
\[
\sum_{i=1}^{t-1} \sum_{j \neq i} x_j \left[ \frac{p_j}{p_i} \right] + \sum_{i=1}^{t-1} x_i \left[ \frac{D/p_i^s}{p_i} \right] = \sum_{i=1}^{t-1} \left[ \frac{c}{p_i} \right] \tag{3.5}
\]
Then for this equation we have its left hand side is
\[
\sum_{i=1}^{t-1} \sum_{j \neq i} x_j \left[ \frac{p_j}{p_i} \right] + \sum_{i=1}^{t-1} x_i \sum_{j \neq i} \left[ \frac{p_j}{p_i} \right] + \sum_{i=1}^{t-1} x_i \left[ \frac{p_t}{p_i} \right]
\]
\[
= x_i \sum_{i=1}^{t-1} \left[ \frac{p_t}{p_i} \right] + \sum_{i=1}^{t-1} x_i \left[ \frac{p_i}{p_t} \right] + \sum_{i=1}^{t-1} x_i \left[ \frac{p_j}{p_i} \right]
\]
\[
= x_i \sum_{i=1}^{t-1} \left[ \frac{p_t}{p_i} \right] + \sum_{i=1}^{t-1} \left[ \frac{p_i}{p_t} \right] + \sum_{i=1}^{t-1} \left[ \frac{p_j}{p_j} \right]
\]
If we use \(p_1 \cdots p_{t-1}\) to denote the product \(p_1 \cdots p_t\) with \(p_i\) omitted, then the left hand side of equation (3.5) equals
\[
x_i \left[ \frac{p_t}{p_1 \cdots p_{t-1}} \right] + \sum_{i=1}^{t-1} x_i \left[ \frac{p_t}{p_1 \cdots p_{t-1}} \right] + \sum_{i=1}^{t-1} x_i \left[ \frac{p_1 \cdots p_{t-1}}{p_i} \right] = x_i \left[ \frac{D/p_i^s}{p_i} \right] + \sum_{i=1}^{t-1} x_i \left[ \frac{p_t}{p_i} \right]
\]
where for the last equation we used the quadratic reciprocity law and \(p_1 \cdots p_t \equiv 3 \pmod{4}\), as then one of \(p_i\) and \(p_1 \cdots p_{t-1} \cdots p_t\) must be congruent to 1 (mod 4). Since \(\left( \frac{D}{p_i} \right) = 1\), then
\[
1 = \left( \frac{-p_1 \cdots p_t}{c} \right) = \left( \frac{-1}{c} \right) \cdot \left( \frac{p_1 \cdots p_t}{c} \right) = \left( \frac{c}{p_1 \cdots p_t} \right)
\]
Hence the right hand side of the equation (3.5) equals \( \frac{c}{p_i} \), thus as what we do for equation (3.4) we get the local solvability is also true for \( p_i \).

Hence, the local conditions on \( d \) is satisfied if and only if \( RX_d = C \). This finishes the proof. \( \square \)

### 3.2 8-rank

In this subsection, we will use classical Gauss genus theory and 4-rank to derive 8-rank \( h_8(K) = \text{rank}_\mathbb{Z} \mathcal{A}[2] \cap 4\mathcal{A} \) of \( K = \mathbb{Q}(\sqrt{-n}) \); this is equivalent to determine those elements in \( \mathcal{A}[2] \cap 2\mathcal{A} \) also lie in 4A.

In this subsection, for the quadratic field, we always assume that \( n = p_1 \cdots p_k \) is a positive square-free integer with all prime factors \( p_i \equiv 1 \pmod{4} \), hence we get a contradiction, which implies that \( c \) is odd.

For any \( 2^r d \in \mathcal{D}(K) \cap N_{K/\mathbb{Q}}(K^\times) \) with \( d|n \) and \( r = 0 \) or 1 such that \( \theta(2^r d) \) is non-trivial, then from Proposition 2 we know that the following Diophantine equation

\[
2^r z^2 = dx^2 + \frac{n}{d} y^2
\]

is solvable over \( \mathbb{Z} \), and let \( (a,b,c) = (x,y,z) \) be a positive primitive integer solution, then \( c \) is odd, as else \( c \) is even, then \( a,b \) must be odd, since \( (a,b,c) \) is a primitive solution, then modulo equation (3.6) by 4 we get: \( 0 \equiv d + \frac{n}{d} \equiv 2 \pmod{4} \), since every divisor of \( n \) is congruent to 1 \pmod{4}, hence we get a contradiction, which implies that \( c \) is odd.

Then \( \mathcal{d} = |c|^2 \) where \( \mathcal{d} = (2^r d, c_0) \) and \( c \) is a certain integral ideal over \( c \). From \( (c, D) = 1 \) we know that any prime \( p|c \) is unramified in \( K \), moreover \( p \) splits in \( K \), as else \( (p) \) is a prime ideal in \( K \), by prime ideal decomposition we know either \( (p) | (a) \) or \( (p) | (\overline{a}) \) since we have \( 2^r dc^2 = Na \) with \( a = da + b\sqrt{\mathcal{D}} \in \mathcal{O}_K \), but either \( (p) | (a) \) or \( (p) | (\overline{a}) \) implies that \( p|a,b,c \) which is impossible since \( (a,b,c) \) is a primitive solution. Whence we get any prime divisor of \( c \) splits in \( K \). Then \( (p) = \mathfrak{pp} | N(a) \), similarly exactly one of \( p, \overline{p} \) divide \( (a) \), then \( (a) = \mathcal{d} \prod_{p|c} p^{2v_p(c)} \). Therefore \( |\mathcal{d}| = |c|^2 \) with \( c \) an integral ideal over \( c \).

Now we study when \( |\mathcal{d}| = |c|^2 \in 4A \) if and only if there is a \( [m] \in \mathcal{A}[2] \) with norm \( m \in \mathcal{D}(K) \) such that \( \mathcal{d} + [m] \in 2\mathcal{A} \), which is equivalent to

\[
mcZ^2 = X^2 - D Y^2
\]

is solvable over \( \mathbb{Z} \) by Proposition 2. Modulo the equation (3.6) by any prime divisor \( p \) of \( c \), we get \( (\frac{c}{p}) = 1 \). And \( c \) is odd, then by Proposition 4 we know that \( |\mathcal{d}| \in 4A \) if and only if \( C \in \text{ImR} \) where \( C = \left( \frac{c}{p_1}, \ldots, \frac{c}{p_k} \right)^T \).

**Remark 1.** We remark that for a given \( d \) as above and another primitive solution \( (a',b',c') \) of the equation \( (3.6) \), there is another \( C' \), but we may have \( C \neq C' \). For example \( K = \mathbb{Q}(\sqrt{-13 \cdot 17}) \), then \( R = \left( \begin{array}{ccc} 0 & 0 & 1 \\ 0 & 0 & 0 \end{array} \right) \), whence \( h_4(n) = 1 \) and 13 represents the only non-trivial element in \( \mathcal{A}[2] \cap 2\mathcal{A} \), then for the equation \( z^2 = 13x^2 + 17y^2 \) we have two universal solution \( (x,y,z) = (1,2,9) \) and \( (4,1,15) \), and correspondingly \( C = (0,0)^T \), \( C' = (1,0)^T \), they are not equal but both lies in \( \text{ImR} \), hence \( h_4(n) = 1 \). In fact, by Sage software we have the ideal class group of \( K \) is isomorphic to \( \mathbb{Z}/8\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \).

Now if \( d_1, d_2 \in \mathcal{D}(K) \cap N_{K/\mathbb{Q}}(K^\times) \) and \( C_1, C_2 \) are given as above, we know \( d := d_1 \odot d_2 \in \mathcal{D}(K) \cap N_{K/\mathbb{Q}}(K^\times) \). Then we have a natural question: does \( [(d,c_0)] \in 4A \) have any relation with \( C_1, C_2 \)? This is given by:
Proposition 5. Let $K = \mathbb{Q}(\sqrt{-n})$ be an imaginary quadratic number field with $n = p_1 \cdots p_k$ a square-free positive integer such that all $p_i \equiv 1 \pmod{4}$, and $2^{r_1}d_1, 2^{r_2}d_2 \in \mathcal{D}(K) \cap N_{K/\mathbb{Q}}(K^\times)$ with $d_i|n$ and $r_i \in \{0,1\}$. Let $2^s d = 2^{r_1}d_1 \circ 2^{r_2}d_2$ with $d|n$. Assume that $(a_i, b_i, c_i) = (x, y, z)$ be positive primitive integer solution of

$$2^r x^2 = d_i x^2 + \frac{n}{d_i} y^2$$  \hspace{1cm} (3.7)$$

and $C_i := \left(\left[\frac{a_i}{p_i}\right], \cdots, \left[\frac{a_i}{p_k}\right]\right)^T, i = 1, 2$. If we denote $\mathfrak{d} = (2^s d, \alpha_0)$ and $R$ the Redei matrix of $K$, then $[\mathfrak{d}] \in 4A \iff$ if and only if $C_1 + C_2 \in \text{Im} R$.

Proof. Let $\alpha_i = d_i a_i + b_i \sqrt{-n} \in \mathcal{O}_K$, then $2^{r_i} d_i c_i^2 = \alpha_i \overline{\alpha}_i$, thus we have

$$2^{r_1 + r_2} d_1 d_2 (c_1 c_2)^2 = N_{K/\mathbb{Q}}(\alpha_1 \alpha_2) = a^2 + nb^2$$  \hspace{1cm} (3.8)$$

with $a = d_1 d_2 a_1 a_2 - b_1 b_2 n$, $b = d_1 d_2 a_2 + b_2 d_1 a_1$. Then we want to derive a primitive solution of $2^2 x^2 = dx^2 + \frac{n}{d} y^2$ with $z = \frac{c_1 c_2}{c_i}$ from equation (3.7), then this will finish our proof by Proposition 4. Before proceeding further, we introduce a notation: for a prime $p$ and an integer $m$, the notation $p^n||m$ means that $p^n|m$ but $p^{n+1}|m$. We claim that:

If a prime $p|(c_1 c_2, a, b)$ then $p^{2v_p(c_1)}||(c_1 c_2, a, b)$, where $s_p := \min \{ v_p(c_1), v_p(c_2) \}$.

Since $p|c_1 c_2$ then $p$ is odd and we may assume that $p|c_1$, hence

$$p^2 | 2^{r_1} d_1 c_i^2 = \alpha_1 \overline{\alpha}_1$$  \hspace{1cm} (3.9)$$

but $p \nmid \alpha_1$ by the solution $(a_1, b_1, c_1)$ is primitive and $c_1$ is coprime with $2n$. Similar argument as the paragraph in equation (3.6) we get $p$ splits in $K$ with $(p) = \mathfrak{p} \mathfrak{p}$ and $p \neq \mathfrak{p}$, and exactly one of $\mathfrak{p}, \mathfrak{p}$ divide the principal ideal $(\alpha_1)$, we may assume that $p|(\alpha_1)$, so $\mathfrak{p} \nmid (\alpha_1)$. Then from ideal version of equation (3.9) we know that $p^{2v_p(c_1)}||(\alpha_1)$. But $p$ also divides $a, b$, hence $p|\alpha_1 \alpha_2$, whence we have

$$p \mathfrak{p} | (\alpha_1)(\alpha_2)$$

since $\mathfrak{p} \nmid (\alpha_1)$, from this we have $\mathfrak{p} | (\alpha_2)$, similarly we have $p^{2v_p(c_2)}||(\alpha_2)$ but $p \nmid (\alpha_2)$. Hence by the prime ideal decomposition of $(\alpha_1 \alpha_2)$, we know their $p, \mathfrak{p}$ components are $p^{2v_p(c_1)}$ and $p^{2v_p(c_2)}$ respectively. From this we get $p^{2v_p||c_1 c_2, a, b)}$.

From this claim we know there is a positive integer $c_0$ such that $(c_1 c_2, a, b) = c_0^2$. By the definition of $a, b$ we can easily get $(d_1, d_2)|a, (d_1, d_2)|b$. Now we deal with 2-part of $a, b$.

If $r_1 = r_2 = 0$, then from equation (3.7) we know exact one of $a_i, b_i$ is even for $i = 1, 2$. Since

$$a \equiv a_1 a_2 - b_1 b_2 (\text{mod} 2), \quad b \equiv a_1 b_2 + a_2 b_1 (\text{mod} 2)$$  \hspace{1cm} (3.10)$$

then exactly one of $a, b$ is even.

If exact one of $r_1, r_2$ is 0, then exact one of $a_1, a_2, b_1, b_2$ is even, then $a, b$ are odd by equation (3.10).

If $r_1 = r_2 = 1$, then $r = 0$, and all of $a_1, a_2, b_1, b_2$ are odd, hence from equation (3.10) we get $a, b$ are even. If $4|(a, b)$, then modulo $a, b$ by 4 respectively we have

$$a_1 a_2 \equiv b_1 b_2 (\text{mod} 4), \quad a_1 b_2 \equiv -a_2 b_1 (\text{mod} 4)$$

Then we get

$$a_2 b_2 \equiv a_1^2 a_1 b_2 \equiv -b_1^2 a_2 b_2 \equiv -a_2 b_2 (\text{mod} 4)$$

11
Then $2|a_2b_2$ which is impossible.

Thus in any case we have $2^{r_1r_2}||(a, b)$. So if we denote

$$a' = \frac{a}{c_0^22^{r_1r_2} \cdot d(d_1, d_2)}, \quad b' = \frac{b}{c_0^22^{r_1r_2} \cdot d(d_1, d_2)}, \quad c' = \frac{c_1c_2}{c_0^2}$$

then from equation (3.8) we get $(x, y, z) = (a', b', c')$ is a primitive positive integer solution of

$$2^r z^2 = dx^2 + \frac{n}{d}y^2$$

Whence the proof is finished by Proposition 4.

3.3 Higher Redei matrix

In this subsection, we will define a higher Redei matrix $R^*$, which is analogous to Redei matrix, for example we also have a 2 to 1 epimorphism from $\ker(R^*)$ to $A[2] \cap 4A$.

In this subsection, we let $K = \mathbb{Q}(\sqrt{-n})$ be an imaginary quadratic number field, where $n = d_1 \cdots d_k$ is a square-free positive integer with all prime factors congruent to 1 (mod 8) such that

1. $h_4(d_i) = 1, 1 \leq i \leq k$;
2. $\left(\frac{p_i}{p_{i+2}}\right) = 1$ for any prime divisor $p_{i_j}$ of $d_{i_j}$ with $i_1 \neq i_2$.

Since all prime divisors of $n$ are congruent to 1 (mod 8), then the Redei matrix $R$ is

$$R = \begin{pmatrix} A & 0 \\ \end{pmatrix}, \quad A = \text{diag}(A_{d_1}, \ldots, A_{d_k})$$

as $n$ satisfying (2), where $A_{d_i}$ denotes the corresponding $A$-matrix in defining the corresponding Monsky matrix of $d_i$. From $h_4(d_i) = 1$ and all prime divisor of $d_i$ are congruent to 1 (mod 8) we get $\text{rank}(A_{d_i}) = \omega(d_i) - 1$ by Proposition 2 and 3, where $\omega(d_i)$ denotes the number of prime divisors of $d_i$.

If we define $d_{k+1} := 2$, then under $\theta$, the image of $d_1, \ldots, d_{k-1}, d_{k+1}$ form a base of $A_{n}[2] \cap 2A_n$ by Proposition 2 and 3. Let $d_i = (d_i, a_0)$ for $1 \leq i \leq k+1$. Then the problem of determining whether $[\theta]$ is in $\text{im}(R)$ is reduced to determine whether $C_i \in \text{Im}(R)$ according to the argument before Remark 1 of §3.2. Here $C_i$ is defined to be $\left(\begin{array}{c} a_1 \\ \vdots \\ a_{\omega(n)} \end{array}\right)$, where $(a_i, b_i, c_i) = (x, y, z)$ is a fixed primitive positive integer solution of

$$z^2 = dx^2 + \frac{n}{d}y^2$$

for $1 \leq i \leq k-1$, and $(a_k, b_k, c_k)$ is the primitive solution derived similarly as in Proposition 5 from those $(a_i, b_i, c_i)$ chosen above since $\theta(d_k) = \prod_{i=1}^{k-1} \theta(d_i)$, while $(a_{k+1}, b_{k+1}, c_{k+1}) = (x, y, z)$ is a fixed primitive positive integer solution of

$$2z^2 = x^2 + ny^2$$

Since a vector $y \in \mathbb{F}_2^{\omega(n)}$ lies in $\text{Im}(R)$ if and only if

$$(0, \ldots, 0, 1, \ldots, 1, 0 \cdots, 0)_{\omega(d_i)} y = 0$$

Then from this and Proposition 4 we know $[\theta] = [(d_i, \sqrt{-n})] \in 4A$ if and only if $\left[\frac{c_j}{d_j}\right] = 1$ for any $1 \leq j \leq k$. Hence by Proposition 5 we get that any $d = \prod_{i=1}^{k+1} d_i^{c_i}$ contributes to
$h_8(n)$ if and only if $\sum_{i=1}^{k+1} x_i \left[ \frac{c_i}{d_i} \right] = 0$ for $1 \leq j \leq k$. This motivates us to define a higher Redei matrix $R^*$: it is a $k \times (k+1)$ matrix over $\mathbb{F}_2$ given by

$$R^* = \begin{pmatrix} A^* & B^* \end{pmatrix}$$

with $A^* = (a_i^*)_{k \times k}$, $a_i^j = \left[ \frac{c_i}{d_i} \right]$ and $B^* = \left( \left[ \frac{c_{a+1}}{d_i} \right], \ldots, \left[ \frac{c_{a+k+1}}{d_i} \right] \right)^T$.

Similar to the Redei matrix, the sum of every row elements of $A^*$ is zero by the choice of $c_k$ and Proposition [3]. And we also get a 2 to 1 epimorphism as in Redei matrix:

$$\left\{ x \in \mathbb{F}_2^{k+1} \mid R^* x = 0 \right\} \rightarrow A[2] \cap 4A, \quad x \mapsto \theta \left( \prod_{i=1}^{k+1} d_i^{x_i} \right)$$

(3.11)

follows from above argument. Thus similar as 4-rank and Redei matrix we get

$$h_8(K) = k - \text{rank}R^*$$

**Remark 2.** It seems as if $A^*$ depends on the choice of $(a_i, b_i, c_i)$, but from Cassels pairing we will see that $A^*$ doesn’t depend on the choice, so $A^*$ is intrinsic.

## 4 Proof of Main Theorems

In this section, we will prove our main theorems according to the strategy explained in the introduction.

### 4.1 First Main Theorem

For a positive square-free integer $n = p_1 \cdots p_k \equiv 1 \pmod{8}$ with all prime factors congruent to $1 \pmod{4}$, the corresponding Monsky matrix of $\text{Sel}_2(E(n))$ and Redei matrix of $\mathbb{Q}(\sqrt{-n})$ are of the form

$$M = \begin{pmatrix} A + D_2 & D_2 \\ D_2 & A + D_2 \end{pmatrix}, \quad R = \begin{pmatrix} A & B \end{pmatrix}$$

where $B = (b_1, \ldots, b_k)^T$ with $b_i = \left[ \frac{2}{p_i} \right]$ and $A$ is a $k \times k$ symmetric matrix over $\mathbb{F}_2$ with all row sum 0, hence all $A$’s column sum are also 0. And we have $h_4(n) = k - \text{rank}R$.

According to the strategy in the introduction, we begin with the first step: relate $s_2(n)$ with $h_4(n)$ via Monsky matrix and Redei matrix.

**Lemma 4.** For a positive square-free integer $n = p_1 \cdots p_k \equiv 1 \pmod{8}$ with all $p_i \equiv 1 \pmod{4}$, then $s_2(n) = 2$ if and only if $h_4(n) = 1$. And if this is satisfied, then the corresponding pure-2 Selmer group $\text{Sel}_2(E(n)/\mathbb{Q})/E(n)(\mathbb{Q})[2]$ is generated by

$$(n, n, 1), \quad (d, d^*, dd^*)$$

where $d^* = d$ if $\text{rank}A = k - 2$ and else $d^* = n/d$ with $d = \prod p_i^{x_i}$, here $x = (x_1, \ldots, x_k)^T \in \mathbb{F}_2^k$ is a non-trivial solution of $Ax = 0$ with $x \neq x_0$ if $\text{rank}A = k - 2$ and else $x$ is a solution of $Ax = B$, here $x_0 = (1, \ldots, 1)^T$.

**Proof.** By properties of Monsky matrix and Redei matrix, this is equivalent to show that the rank of $M$ is $2k - 2$ if and only if that of $R$ is $k - 1$. 

13
If we denote $R_i$ to be the $(k-1) \times (k+1)$ matrix obtained from $R$ by deleting the $i$-th row vector, then by elementary linear transforms, the following matrices have same rank over $\mathbb{F}_2$:

$$M, \quad M' := \left( \begin{array}{cc} A & D_2 \\ D_2 & A \end{array} \right), \quad M'' := \left( \begin{array}{c} R_k \\ * \\ R_1^T \end{array} \right)$$

where $M''$ derives from $M'$ by: adding the first $k-1$ row to the $k$-th row, then adding the last $k-1$ column to the $(k+1)$-th column, and then moving the $k$-th row as the last row.

If $\text{rank} R = k - 1$: from $A$ is symmetric and $\sum_{i=1}^k b_i = \left[ \frac{2}{n} \right]$ with $n \equiv 1 (\text{mod} 8)$ we get the sum of all row vectors of $A$ and $B$ are 0, hence the only non-trivial linear dependence of $R$ is the sum of all row vectors is 0, whence we get rank of $R_i$ is also $k - 1$. From this we know that $2k - 2 \leq \text{rank} M'' \leq 2k - 1$, but the rank of $M$ and $M''$ are equal and rank $M$ must be even since $n \equiv 1 (\text{mod} 8)$ by the last line of §2.1, hence $\text{rank} M = 2k - 2$.

If $\text{rank} M = 2k - 2$, then so is $\text{rank} M''$, since $R_k$ has only $k - 1$ rows, hence from the rank of $M''$ we infer that $\text{rank} R_1^T \geq k - 1$, but we know that $\text{rank} R_1 \leq \text{rank} R \leq k - 1$ since the sum of all row vectors of $R$ are 0. This force $R$ has rank $k - 1$. So $s_2(n) = 2$ if and only if $h_4(n) = 1$.

Now assume that $h_4(n) = 1$: we suffice to find the corresponding 4 representatives of $\text{Sel}_2(E(n))/\text{Sel}_2(E(n))(Q)[2]$. By Monsky matrix, we reduce to find $y, z \in \mathbb{F}_2^k$ such that

$$M \begin{pmatrix} y \\ z \end{pmatrix} = \begin{pmatrix} A + D_2 & D_2 \\ D_2 & A + D_2 \end{pmatrix} \begin{pmatrix} y \\ z \end{pmatrix} = 0$$

From this we have: $Ay + D_2(y + z) = 0, A(y + z) = 0$, thus $y + z \in \ker A$. Now we divide into two cases according to A’s rank:

If $\text{rank} A = k - 2$, and if $y + z = 0$ then we have $Ay = 0, A$ thus in this case $y = z$ with $Ay = 0$ are the 4 solutions. Hence the following 2 elements generates the pure 2-Selmer group $\text{Sel}_2(E(n))/\text{Sel}_2(E(n))(Q)[2]$:

$$(d, d, 1), \quad (n, n, 1)$$

If $\text{rank} A = k - 1$, thus $y + z = 0$ or $x_0 := (1, \cdots, 1)^T$. If $y + z = 0$, then we have two solutions $y = z = 0$ or $y = z = x_0$; if $y + z = x_0$, then $Ay = D_2 \cdot x_0 = B$, and $B$ is indeed in Im $A$, as rank $(A|B) = \text{rank} A = k - 1$ thus $\{y, z\} = \{x, x_0 - x\}$ with $Ax = B$. Hence the following 2 elements generates $\text{Sel}_2(E(n))/\text{Sel}_2(E(n))(Q)[2]$:

$$(d, d^*, dd^*), \quad (n, n, 1)$$

Hence the Lemma is proved.

Now we begin to prove Theorem 1

**Proof.** From Lemma above, we get $s_2(n) = 2$ if and only if $h_4(n)=1$. Now begin the second step. From the following exact sequence:

$$0 \to E^{(n)}[2] \to E^{(n)}[4] \xrightarrow{2} E^{(n)}[2] \to 0$$

we have the corresponding long exact sequence:

$$0 \to E^{(n)}[2](Q)/2E^{(n)}[4](Q) \to \text{Sel}_2(E^{(n)}) \to \text{Sel}_4(E^{(n)}) \to \text{Sel}_2(E^{(n)})$$

And if we denote Im $\text{Sel}_4(E^{(n)})$ to be the image of $\text{Sel}_4(E^{(n)})$ in the last map of above long exact sequence, then we have $\text{rank}_2 E^{(n)}(Q) = 0$, $\text{III}(E^{(n)}(Q)/2\mathbb{Z}) \simeq (\mathbb{Z}/2\mathbb{Z})^2$ if and only if $\#\text{Sel}_2(E^{(n)}) = \#\text{Sel}_4(E^{(n)})$, which is equivalent to $\#\text{Im}_2(E^{(n)}) = \#E^{(n)}(Q)[2]$ by
above long exact sequence. Then by Cassels pairing, this holds if and only if the Cassels pairing on the pure 2-Selmer group $\text{Sel}_2(E^{(n)})/E^{(n)}(Q)[2]$ is non-degenerate. Hence if we denote $\Lambda = (d, d^*, dd^*)$, $\Lambda' = (-1, 1, -1)$, then we reduce to show when

$$\langle \Lambda, \Lambda' \rangle = -1$$

note here $\Lambda' \in (n, n, 1) + E^{(n)}(Q)[2]$.

Now we are in the third step to compute $\langle \Lambda, \Lambda' \rangle$ according to rank $A$:

(I): The rank of $A$ is $k - 2$: we claim that in this case

$$d \equiv 5 \pmod{8}$$

From $h_4(n) = 1$ we get $\text{rank} R = \text{rank}(A|B) = k - 1$, but $\text{rank} A = k - 2$, this shows that $B \not\in \text{Im} A$. Since $A$ is symmetric and ker $A$ is generated by $x_0, x$ which are defined in above Lemma, a vector $y \in F^5_5$ lies in Im $A$ if and only if $x_0^T y = 0, x^T y = 0$. But $x_0^T \cdot B = [\frac{2}{n}] = 0$, so we must have $x^T \cdot B = [\frac{2}{d}] \neq 0$, thus $d \equiv 5(\text{mod} 8)$.

For $\Lambda = (d, d, 1)$ the corresponding genus one curve $D_\Lambda$ is:

$$D_\Lambda = \begin{cases} H_1: & -nt^2 + du_2^2 - u_3^2 = 0 \\ H_2: & -nt^2 + u_3^2 - du_2^2 = 0 \\ H_3: & 2^{d'}t^2 + u_1^2 - u_2^2 = 0 \end{cases}$$

Here $d' := n/d$. According to Cassels pairing, we have to chose global points $Q_i$ on $H_1$: for $H_3$ we chose the global point $Q_3 = (0, 1, 1)$, then the tangent plane at $Q_3$ is

$$L_3 : u_1 - u_2$$

For $H_1$ we chose the global point $Q_1 = (b, c, da)$ on $H_1$, where $(a, b, c)$ is a primitive positive integer solution of

$$c^2 = da^2 + d^2b^2$$

(4.1)

The existence of this solution origins from $h_4(n) = 1$ and $d$ corresponds to $R \left( \begin{array}{c} x \\ 0 \end{array} \right) = 0$

by Proposition 2, 3. We may assume that $2|a$, since else $a$ is odd, $b$ is even and we have a new solution

$$(a, \tilde{b}, \tilde{c}) := (d'a - 2d'b - da, db - 2da - d'b, (d + d')c)$$

with $v_2(\tilde{a}) \geq 2$ and $v_2(\tilde{b}) = v_2(\tilde{c}) = 1$, hence by dividing the greatest common divisor, we get a new primitive solution with corresponding $a$ even. Then the corresponding tangent plane $L_1$ at this point is

$$L_1 : d'bt - cu_2 + au_3$$

Hence by Cassels pairing we have to compute

$$\langle \Lambda, \Lambda' \rangle = \prod_p \left( L_1L_3(P_p), -1 \right)_p$$

for any local point $P_p$ on $D_\Lambda(Q_p)$, here $p$ includes the real place.

By Lemma 2 we only have to compute those $p|2n\infty$. Note all $p|n$ are congruent to 1 (mod 4), so $-1$ is a square in $Q_p$, thus by Hilbert symbol we have these $\left( L_i(P_p), -1 \right)_p = 1$. Whence we only have to consider local solutions at $2\infty$, we can chose as follows:
For $p = \infty$: we chose $t = 0, u_1 = -u_2 = 1, u_3 = \sqrt{d}$, then

$$\left( L_1 L_3(P_\infty), -1 \right)_\infty = \left( 2(c + a\sqrt{d}), -1 \right)_\infty = 1$$

For $p = 2$, we chose $t = 2, u_1 = 1, u_2^2 = 1 + 8d', u_3^2 = d + 4n$ and we may assume $u_2 \equiv 3(\text{mod}8)$ as $u_2^2 = 1 + 8d' \equiv 9(\text{mod}16)$, so

$$\left( L_1 L_3(P_2), -1 \right)_2 = \left( (1 - u_2)(2bd' - cu_2 + au_3), -1 \right)_2 = (-2, -1)_2(c, -1)_2 = -(c, -1)_2$$

where we used the fact that $\frac{au_3}{2} \equiv bd'(\text{mod}2)$. Thus in this case we have

$$\langle \Lambda, \Lambda' \rangle = -\left( \frac{-1}{c} \right)$$

By modulo $c$ of the equation (4.1) we get $(\frac{n}{c}) = 1$: whence $\langle \Lambda, \Lambda' \rangle = -1$ if and only if $(\frac{n}{c}) = 1$.

Now we begin our last step is this case: use Gauss genus theory to reduce to 8-rank of the ideal class group of $\mathbb{Q}(\sqrt{-n})$. Since $R$ has rank $k - 1$ and $x_0^2 R = 0$, we know a vector $y \in \mathbb{F}_2^k$ lies in $\text{Im}R$ if and only if $x_0^2 y = 0$. From this we get $(\frac{n}{c}) = 1$ is equivalent to $Rz = C$ has a solution $z \in \mathbb{F}_2^k$, this is equivalent to $h_8(n) = 1$ by the argument before Remark [1] of §3.2. Hence under the condition $\text{rank}A = k - 2$ we know that the Cassels pairing is non-degenerate if and only if $h_8(n) = 1 \equiv \frac{d - 1}{4}(\text{mod}2)$ since $d \equiv 5(\text{mod}8)$.

(II): if $\text{rank}A = k - 1$, then $d$ corresponds to the solution of $Ax = B$. Since we have

$$R \begin{pmatrix} x \\ 1 \end{pmatrix} = Ax + B = 0$$

we know that $2d$ is a norm. Then $(d, d', n) \in (2d, 2d, 1) + E^{(n)}(\mathbb{Q})[2]$, so we still use $\Lambda$ to denote $(2d, 2d, 1)$ since this won’t effect $\langle \Lambda, \Lambda' \rangle$, then the corresponding genus 1 curve $D_\Lambda$ is given by:

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

For $H_3$ we chose the global point $Q_3 = (0, 1, 1)$, then the tangent plane $L_3$ of $H_3$ at $Q_3$ is

$$L_3 : u_1 - u_2$$

Since $2d$ is a norm, there is a positive primitive solution of the Diophantine equation

$$2c^2 = da^2 + d'b^2$$

So the global point $Q_1 : (b, c, ad)$ is on $H_1$, and the tangent plane $L_1$ of $H_1$ at $Q_1$ is

$$L_1 : d'bt - 2cu_2 + au_3$$

With the same reason as $\text{rank}A = k - 2$, we only need to consider at $2\infty$. For $p = \infty$ we chose local solution:

$$P_\infty : t = 0, u_1 = -u_2 = 1, u_3 = \sqrt{2d}$$

Then

$$\left( L_1 L_3(P_\infty), -1 \right)_\infty = \left( 2(2c + a\sqrt{2d}), -1 \right)_\infty = 1$$
For \( p = 2 \), we chose local solution

\[
P_2: t = 1, u_1 = 2 \left\lfloor \frac{d}{a} \right\rfloor, u_2 = d' + u_1^2, u_3^2 = n + 2du_1^2
\]

such that \( cv_2 \equiv 1 \pmod{4} \), \( 8|(bd' + au_3) \), since we have

\[
(bd')^2 - (au_3)^2 = b^2d'^2 - a^2n - 2a^2du_1^2 = (2c^2 - da^2)d' - a^2n - 2a^2du_1^2
\]

\[
= 2(c^2d' - a^2n - 2a^2du_1^2) \equiv 2(d' - n - du_1^2) \equiv 0 \pmod{16}
\]

so we may chose \( u_3 \) such that: \( 8|(bd' + au_3) \).

\[
\left( L_1L_3(P), -1 \right)_2 = \left( (u_1 - u_2)(d'b - 2cv_2 + au_3), -1 \right)_2 = (-2, -1)_2(u_1 - c, -1)_2
\]

\[
= (c - u_1, -1)_2 = (-1)\frac{d-1}{4} (c, -1)_2
\]

Similar argument as above, we know that \((c, -1)_2 = 1 \) if and only if \(( \frac{c}{n} \)\) = 1, this is equivalent to \( h_8(n) = 1 \), so Cassels pairing is non-degenerate in this case if and only if \( h_8(n) \equiv \frac{d-1}{4} \pmod{2} \).

Summarize these cases together we get: \( \text{rank}_2 E^{(n)}(\mathbb{Q}) = 0, \text{III}(E^{(n)}/\mathbb{Q})[2\infty] \simeq (\mathbb{Z}/2\mathbb{Z})^2 \) is equivalent to \( h_8(n) \equiv \frac{d-1}{4} \pmod{2} \). This completes the proof of Theorem 3.

To show the condition of Li-Tian is also sufficient as claimed in the introduction, we first introduce the quartic residue symbol used in Jung-Yue \([11]\): for \( p \) a prime congruent to 1 \pmod{4}, then there are two primitive Gaussian primes \( \pi, \pi' \) over \( p = \pi\pi' \), hence we have two quartic residue symbol \(( \frac{\cdot}{\pi} \), \(( \frac{\cdot}{\pi'} \) over \( \mathbb{Z}[i] \) such that their squares are the Legendre residue symbol \(( \frac{\cdot}{p} \) over \( \mathbb{Z} \). If \( q \in \mathbb{Z} \) such that \(( \frac{q}{p} ) = 1 \), then \(( \frac{q}{p} ) = ( \frac{q}{\pi} ) = \pm 1 \), and we denote by \(( \frac{q}{p} ) \) be either \(( \frac{q}{\pi} ) \) or \(( \frac{q}{\pi'} \). Similarly if \( d \) is a positive integer with all prime divisor \( p \equiv 1 \pmod{4} \) such that \(( \frac{d}{p} ) = 1 \), then

\[
\left( \frac{q}{p} \right)_4 := \prod_{p | d} \left( \frac{q}{p} \right)^{v_p(d)}
\]

**Theorem 3.** For \( p \equiv 1 \pmod{8} \) a prime, then there exists positive integers such that:

\[
p = u^2 + 8v^2 = a^2 + 16b^2 = x^2 - 32y^2.
\]

Then the following are equivalent:

1. \( 2 \nmid v \);
2. \( 2 \nmid \frac{p-1}{8} + b \);
3. \( 1 + i_p \) is not a \( p \)-adic square with \( i_p \in \mathbb{Q}_p \) such that \( i_p^2 = -1 \);
4. \( 1 + j_p \) is not a \( p \)-adic square with \( j_p \in \mathbb{Q}_p \) such that \( j_p^2 = 2 \);
5. \( \left( \frac{2}{p} \right)_4 = (-1)^{\frac{p-9}{8}} \);
6. \( x \equiv 3 \pmod{4} \);
7. \( h_8(p) = 0 \).
And we define $\delta_p = 1$ if $p$ satisfies the above equivalent conditions, else $\delta_p = 0$. For $n$ a square-free positive integer with all prime factors congruent to 1 (mod 8) and $h_4(n) = 1$, the following are equivalent:

(i) $2 \nmid \delta_n := \sum_{p|n} \delta_p$

(ii) $h_8(n) = 0$

(iii) $\text{rank}_Z E^{(n)}(\mathbb{Q}) = 0$, $\text{III}(E^{(n)}/\mathbb{Q})[2^\infty] \simeq (\mathbb{Z}/2\mathbb{Z})^2$.

Proof. The existence of $u, v, a, b$ follows from $p$ splits in $\mathbb{Q}(\sqrt{-2})$ and $\mathbb{Q}(i)$. Now we show the existence of $x, y$: since $p$ splits in $\mathbb{Q}(\sqrt{2})$, there are $x_0, y_0 \in \mathbb{Z}$ such that

$$p = x_0^2 - 2y_0^2$$

moreover $x_0$ is odd and $y_0$ is even as $p \equiv 1 \pmod{8}$. If $4|y_0$ then we define $x = x_0, y = \frac{y_0}{4}$. Else $4 \nmid y_0$, we can use the fundamental units $1 + \sqrt{2}$ to lift 2-divisibility. Concretely since $(1 + \sqrt{2})^2 = 3 + 2\sqrt{2}$ has norm 1, then

$$p = (3x_0 + 4y_0)^2 - 2\left(2x_0 + 3y_0\right)^2$$

and $4|(2x_0 + 3y_0)$, then we define $x = 3x_0 + 4y_0, y = \frac{2x_0 + 3y_0}{4}$. Then we get $p = x^2 - 32y^2$.

The equivalence from (1) to (5) are proved in Li-Tian [3]. (5) is equivalent to (6): From

$$p = x^2 - 32y^2$$

we get

$$\left(\frac{x}{p}\right) = \left(\frac{x^2}{p}\right)_4 = \left(\frac{-2y^2}{p}\right)_4 = \left(\frac{2}{p}\right)_4 \left(\frac{y}{p}\right) = \left(\frac{2}{p}\right)_4$$

where we used $\left(\frac{y}{p}\right)_4 = 1$ by the equation (4.2) modulo $y$. But if we modulo the equation (4.2) by $x$ we get

$$\left(\frac{x}{p}\right) = \left(\frac{-2}{x}\right) = \left(\frac{-1}{x}\right)(-1)^{\frac{x^2-1}{8}} = \left(\frac{-1}{x}\right)(-1)^{\frac{x-1}{8}}$$

since $p \equiv x^2 \pmod{32}$ by equation (4.2) modulo 32. Then by quadratic reciprocity law we know $\left(\frac{x}{p}\right) = \left(\frac{p}{x}\right)$, from this we know (5) is equivalent to (6).

(6) and (7) are equivalent because by considering $1 + \sqrt{2}$ similar as above

$$-p = N_{\mathbb{Q}(\sqrt{2})/\mathbb{Q}}((x + 8y) + (x + 4y)\sqrt{2}) = (x + 8y)^2 - 2(x + 4y)^2$$

then for the field $\mathbb{Q}(\sqrt{-p})$, its Redei matrix is the matrix $0_{1 \times 2}$, so we get 2 is a norm element, and in fact the equation $\left(\frac{p}{x}\right) = 1$ is the corresponding Diophantine equation, see Proposition 2. Hence by Proposition 1 with $c = x + 4y$ there we get: $h_8(p) = 0$ if and only if $\left(\frac{x + 4y}{p}\right) = -1$. But modulo the equation (4.3) by $x + 4y$ we get $\left(\frac{-p}{x + 4y}\right) = 1$, whence

$$\left(\frac{x + 4y}{p}\right) = \left(\frac{p}{x + 4y}\right) = \left(\frac{-1}{x + 4y}\right) = \left(\frac{-1}{x}\right)$$

From these we get (6) is equivalent to (7).
The equivalence of (ii) and (iii) follows from Theorem 1. For the equivalence of (i) and (ii): let \( x_i, y_i \) be positive integers such that \( p_i = x_i^2 - 32y_i^2 \) as above, then

\[
n = p_1 \cdots p_k = N_{\mathbb{Q}(\sqrt{2})/\mathbb{Q}}(x + 4y\sqrt{2}), \quad x + 4y\sqrt{2} = \prod_{i=1}^{k} (x_i + 4y_i\sqrt{2})
\]

and \( x \equiv x_1 \cdots x_k (\text{mod} \ 4) \). Similarly by considering the fundamental unit \( 1 + \sqrt{2} \), we have:

\[
2(x + 4y)^2 = (x + 8y)^2 + n
\]

Then using Gauss genus theory as above we get: \( h_8(n) = 0 \) if and only if \( \left( \frac{x+4y}{n} \right) = -1 \), we also have \( \left( \frac{-n}{x+4y} \right) = 1 \), so

\[
\left( \frac{x + 4y}{n} \right) = \left( \frac{n}{x + 4y} \right) = \left( \frac{-1}{x + 4y} \right) = \left( \frac{-1}{x_1 \cdots x_k} \right) = (−1)^{δ_n}
\]

From this we get the equivalence of (i) and (ii).

Hence we complete the proof.

\[ \qed \]

### 4.2 Second Main Theorem

In this subsection, we let \( n = d_1 \cdots d_k \) be a square-free positive integer with all prime factors congruent to 1 (mod 8), such that

1. \( h_4(d_i) = 1, 1 \leq i \leq k; \)
2. \( \left( \frac{p_i}{p_{i_2}} \right) = 1 \) for any prime divisor \( p_i \) of \( d_{i_2} \) with \( i_1 \neq i_2 \).

Since all prime divisors of \( n \) are congruent to 1 (mod 8), hence the corresponding \( D_2, D_{−2} \) matrix of \( n \) are 0, thus

\[
M_n = \text{diag}(A, A), \quad R_n = \begin{pmatrix} A & 0 \end{pmatrix}
\]

with \( A = \text{diag}(A_{d_1}, \ldots, A_{d_k}) \) as \( n \) satisfying (2), where \( A_{d_i} \) denotes the corresponding \( A \)-matrix in defining the corresponding Monsky matrix of \( d_i \). From \( h_4(d_i) = 1 \) and all prime divisors of \( d_i \) are congruent to 1 (mod 8) we get \( \text{rank}A_{d_i} = \omega(d_i) - 1 \) by Proposition 2 and 3.

Now we get \( s_2(n) = 2k \): since

\[
s_2(n) = 2 \sum_{i=1}^{k} \omega(d_i) - \text{rank}M = 2 \sum_{i=1}^{k} (\omega(d_i) - \text{rank}A_{d_i}) = 2k
\]

And the following is a base of \( \ker M_n \):

\[
\left( \begin{array}{c}
\omega(d_1 \cdots d_{i-1}) \\
\omega(d_i) \\
\omega(d_{i+1} \cdots d_k)
\end{array} \right), \left( \begin{array}{c}
\omega(n) \\
\omega(d_1 \cdots d_{i-1}) \\
\omega(d_{i+1} \cdots d_k)
\end{array} \right), \left( \begin{array}{c}
\omega(d_1 \cdots d_{i-1}) \\
\omega(d_i) \\
\omega(d_{i+1} \cdots d_k)
\end{array} \right), \left( \begin{array}{c}
\omega(n) \\
\omega(d_1 \cdots d_{i-1}) \\
\omega(d_{i+1} \cdots d_k)
\end{array} \right)
\]

with \( 1 \leq i \leq k \), consequently \( \text{Sel}_2(E^{(n)}/E^{(n)}(\mathbb{Q})) \) has a base consists of

\( \Lambda_i = (1, d_i, d_i), \quad \Lambda'_i = (d_i, d_i, 1), 1 \leq i \leq k \)

Now we can compute the Cassels pairings of this base, see:
Proposition 6. Let \( n, \Lambda, \Lambda' \) as above, we have the following Cassels pairings:

\[
\langle \Lambda, \Lambda_j \rangle = \left( \frac{c_j \gamma_i}{d_j} \right), \quad i \neq j
\]

\[
\langle \Lambda, \Lambda'_j \rangle = \left( \frac{c_i}{d_j} \right) = \left( \frac{\bar{c}_j}{d_i} \right), \quad i \neq j
\]

\[
\langle \Lambda, \Lambda'_i \rangle = (-1)^{\delta_{ii}} \left( \frac{c_i}{d_i} \right) = (-1)^{\delta_{ii}} \left( \frac{\bar{c}_i}{d_i} \right)
\]

\[
\langle \Lambda'_i, \Lambda'_j \rangle = \left( \frac{c_i \bar{c}_j}{d_j} \right), \quad i \neq j
\]

Where \( c_i \) consists a fixed primitive positive integer solution of

\[
c_i^2 = d_i a_i^2 + d'_i b_i^2
\]  \( (4.4) \)

with \( d'_i = n/d_i \), and \( \gamma_i, \bar{c}_i \) consist primitive positive integer solutions of

\[
\gamma_i^2 = d_i \alpha_i^2 + 2d'_i \delta_i^2, \quad \bar{c}_i^2 = d_i \bar{a}_i^2 - d'_i \bar{b}_i^2
\]  \( (4.5) \)

respectively such that:

\[
d'_i \left( a_i \gamma_i + c_i \alpha_i, \ a_i \bar{c}_i + c_i \bar{a}_i \right)
\]  \( (4.6) \)

Remark 3. We remark that we can always find solutions of the equations \( (4.5) \) satisfying the conditions \( (4.6) \), we will omit all the subscripts in this remark. If we define \( t = (d', a \gamma + c \alpha) \), then we have a new solution

\[
(t, \bar{t}, \bar{\gamma}) = \left( -d \alpha t^2 + 4d' \beta t + 2d' \alpha, \ d \beta t^2 + 2d \alpha t - 2d' \beta, \ \gamma(dt^2 + 2d') \right)
\]  \( (4.7) \)

of \( z^2 = dx^2 + 2d'y^2 \). Then

\[
a \bar{\gamma} + c \bar{\alpha} = dt^2(a \gamma - c \alpha) + 2d' \left( 2c \beta t + (a \gamma + c \alpha) \right)
\]

By modulo equations \( (4.4) \) and \( (4.5) \) by \( d' \) we get \( d' \mid (a \gamma + c \alpha)(a \gamma - c \alpha) \).

Then for any \( p \mid t = (d', a \gamma + c \alpha) \), we have \( v_p(a \bar{\gamma} + c \bar{\alpha}) \geq 2 \) and \( v_p(t) = 1 \) as \( p \nmid \alpha \). For \( p \mid t^2 \), then \( p \mid (a \gamma - c \alpha) \), therefore \( v_p(a \bar{\gamma} + c \bar{\alpha}) \geq 1 \) and \( v_p(t) = 0 \). Thus we get a solution of \( z^2 = dx^2 + 2d'y^2 \) satisfying the condition \( (4.6) \) by dividing the greatest common divisors of \( \alpha \) and \( \gamma \) in \( (4.7) \).

Similarly for \( (a, \bar{b}, \bar{c}) \) we can get a solution satisfying \( (4.6) \). In fact we choose \( s = (d', a \bar{c} + c \bar{a}) \), and we get a solution

\[
\left( -d \bar{a} s^2 + 2d' \bar{b} s - d' \bar{a}, \ d \bar{b} s^2 - 2d \bar{a} s + d' \bar{b}, \ \bar{c}(ds^2 - d') \right)
\]

Then do similarly as above.

Now we are ready to prove Proposition 0.

Proof. For \( \Lambda_i = (1, d_i, d_i) \) the corresponding genus one curve \( D_{\Lambda_i} \) is:

\[
\begin{align*}
H_1 : \quad & -nt^2 + d_i u_2^2 - d_i u_3^2 = 0 \\
H_2 : \quad & -nt^2 + d_i u_3^2 - u_1^2 = 0 \\
H_3 : \quad & 2nt^2 + u_1^2 - d_i u_2^2 = 0
\end{align*}
\]
Then we chose

\[ Q_1 = (0, 1, 1), \quad Q_2 = (b_i, c_i, d_ia_i), \quad Q_3 = (\beta_i, d_i\alpha_i, \gamma_i) \]

these global points are on \( H_i \) follows from equations (4.4) and (4.5). Then the corresponding tangent planes are

\[
L_1 : \quad u_2 - u_3 \\
L_2 : \quad d_i'b_i t - c_iu_3 + a_iu_1 \\
L_3 : \quad 2d_i'\beta_i t + \alpha_iu_1 - \gamma_iu_2
\]

By Lemma 2, we only need to compute \( p|2n\infty \). Since all \( d_i \) are bigger than 0 and congruent to 1 (mod 8), hence by properties of Hilbert symbol, they are trivial at \( p = 2, \infty \). So we only need to consider those \( p|n \):

We can chose local solutions \( P_p \in D_{\Lambda_i}(\mathbb{Q}_p) \) as following: For \( p|d_i' \):

\[
t = 0, \quad u_2 = -u_3 = 1, \quad u_1^2 = d_i
\]

such that \( p|(c_i - a_iu_1), p|(\alpha_iu_1 + \gamma_i) \), as \((c_i - a_iu_1)(c_i + a_iu_1) = d_i^2b_i^2 \), so we can chose \( u_1 \) such that \( p|(c_i - a_iu_1) \), thus we also have \( p|(\alpha_iu_1 + \gamma_i) \) follows from condition (4.6). For \( p|d_j \):

\[
t = 1, \quad u_1 = 0, u_3^2 = d_j', \quad u_2 = -j_pu_3
\]

such that \( p|(d_i'b_i + c_iu_3) \), since we have \((d_i'b_i + c_iu_3)(d_i'b_i - c_iu_3) = -na_i^2 \), and \( j_p \in \mathbb{Q}_p \) satisfying \( j_p^2 = 2 \) as in Theorem 3:

Now we begin to compute Cassels pairings:

First we compute \( \langle \Lambda_i, \Lambda_j \rangle \) with \( i \neq j \), then by Cassels pairing we have

\[
\langle \Lambda_i, \Lambda_j \rangle = \langle (1, d_i, d_i), (1, d_j, d_j) \rangle = \prod_p \left( L_{2L_3}(P_p), d_j \right)_p
\]

Note that \( \left( \frac{d_j}{P} \right) = 1 \) if \( p \nmid d_j \), so this pairing is trivial at \( p|d_j' \), thus we only need consider at those \( p|d_j \), and for \( p|d_j \):

\[
\left( L_{2L_3}(P_p), d_j \right)_p = \left( (c_i + a_iu_1)(\alpha_iu_1 - \gamma_i), d_j \right)_p = \left( -c_i\gamma_i, d_j \right)_p = \left( c_i\gamma_i \right)_p
\]

Thus we have:

\[
\langle (1, d_i, d_i), (1, d_j, d_j) \rangle = \left( \frac{c_i\gamma_i}{d_j} \right)
\]

Second we compute \( \langle \Lambda_i, \Lambda'_j \rangle \) with \( i \neq j \), then Cassels pairing implies that

\[
\langle \Lambda_i, \Lambda'_j \rangle = \langle (1, d_i, d_i), (d_j, d_j, 1) \rangle = \prod_p \left( L_{1L_2}(P_p), d_j \right)_p
\]

Since \( \left( \frac{d_j}{P} \right) = 1 \) if \( p \nmid d_j \), this pairing is trivial at \( p|d'_j \), therefore we suffice to consider at those \( p|d_j \), and for \( p|d_j \):

\[
\left( L_{1L_2}(P_p), d_j \right)_p = \left( 2(c_i + a_iu_1), d_j \right)_p = \left( c_i, d_j \right)_p = \left( \frac{c_i}{P} \right)
\]

21
Whence
\[ \langle (1, d_i, d_i), (d_j, d_j, 1) \rangle = \left( \frac{c_i}{d_j} \right) \]

Third we compute \( \langle \Lambda, \Lambda' \rangle \), from Cassels pairing we have
\[ \langle \Lambda, \Lambda' \rangle = \langle (1, d_i, d_i), (d_i, d_i), 1 \rangle = \prod_p \left( L_1 L_2(P_p), d_i \right)_p \]

From \( \left( \frac{d_i}{p} \right) = 1 \) if \( p \nmid d_i \) we know this pairing is trivial at \( p|d'_i \), thus we reduce to compute at those \( p|d_i \), and for \( p|d_i \):
\[ \left( L_1 L_2(P_p), d_i \right)_p = \left( (-j_p - 1)u_3(d'_i b_i - c_i u_3), d_i \right)_p = \left( c_i(1 + j_p), d_i \right)_p = (-1)^{\delta_p} \left( \frac{c_i}{d_i} \right) \]

Consequently
\[ \langle (1, d_i, d_i), (d_i, d_i), 1 \rangle = (-1)^{\delta_i} \left( \frac{c_i}{d_i} \right) \]

For \( \Lambda'_i = (d_i, d_i, 1) \), the corresponding \( D_{\Lambda'_i} \) is given by:
\[
\begin{align*}
H_1 : & \quad -nt^2 + d_i u_2^2 - u_3^2 = 0 \\
H_2 : & \quad -nt^2 + u_3^2 - d_i u_1^2 = 0 \\
H_3 : & \quad 2nt^2 + d_i u_1^2 - d_i u_2^2 = 0
\end{align*}
\]

From equations (4.4) and (4.5) we have global points \( Q_i \) on \( H_1 \) as follows
\[ Q_1 = (b_i, c_i, d_i a_i), \quad Q_2 = (\bar{b}_i, d_i \bar{a}_i, \bar{c}_i), \quad Q_3 = (0, 1, 1) \]

Then the tangent planes at these points are
\[
\begin{align*}
L_1 : & \quad d'_i b_i t - c_i u_2 + a_i u_3 \\
L_2 : & \quad d'_i \bar{b}_i t - \bar{a}_i u_3 + \bar{c}_i u_1 \\
L_3 : & \quad u_1 - u_2
\end{align*}
\]

Similarly the pairings are trivial outside of \( p|n \), hence we only have to consider for those \( p|n \). We can chose local solutions \( P_p \in D_{\Lambda'_i}(\mathbb{Q}_p) \) as following: For \( p|d'_i \):
\[ t = 0, \quad u_2 = -u_1 = 1, \quad u_3^2 = d_i \]
such that \( p|(c_1 + a_i u_3), p|((\bar{c}_i - \bar{a}_i)u_3) \), as \( (c_1 - a_i u_3)(c_1 + a_i u_3) = d'_i b_i^2 \), so we can chose \( u_3 \) such that \( p|(c_1 + a_i u_3) \), thus we also have \( p|((\bar{c}_i - \bar{a}_i)u_3) \) follows from condition (4.6). For \( p|d_i \):
\[ t = 1, \quad u_3 = 0, u_1^2 = -d'_i, \quad u_2 = -i_p u_1 \]
with \( p|(d'_i b_i - \bar{c}_i u_1) \), since we have \( (d'_i b_i - \bar{c}_i u_1)(d'_i b_i + \bar{c}_i u_1) = n\bar{a}_i^2 \), note here we have used \( i_p \in \mathbb{Q}_p \) such that \( i_p^2 = -1 \) as in Theorem 4.

Now we begin to compute Cassels pairings:
First we compute $\langle \Lambda'_i, \Lambda'_j \rangle$ with $i \neq j$, then by Cassels pairing:

$$\langle \Lambda'_i, \Lambda'_j \rangle = \langle (d_i, d_i, 1), (d_j, d_j, 1) \rangle = \prod_p \left( L_1L_2(P_p), d_j \right)_p$$

Note that $\left( \frac{d_i}{p} \right) = 1$ if $p \nmid d_j$, so this pairing is also trivial at $p|d_j$, thus we only need to consider at those $p|d_j$, and for $p|d_j$:

$$\left( L_1L_2(P_p), d_j \right)_p = \left( (-c_i + a_iu_3)(-\bar{a}_i u_3 - \bar{c}_i), d_j \right)_p = (c_i \bar{c}_i, d_j)_p = \left( \frac{c_i \bar{c}_i}{d_j} \right)_p$$

Thus we have:

$$\langle (d_i, d_i, 1), (d_j, d_j, 1) \rangle = \left( \frac{c_i \bar{c}_i}{d_j} \right)$$

Then we compute $\langle \Lambda'_i, \Lambda_j \rangle$ with $i \neq j$: then from Cassels pairing we have

$$\langle \Lambda'_i, \Lambda_j \rangle = \langle (d_i, d_i, 1), (1, d_j, d_j) \rangle = \prod_p \left( L_2L_3(P_p), d_j \right)_p$$

Since $\left( \frac{d_i}{p} \right) = 1$ if $p \nmid d_j$, so we only need to consider at those $p|d_j$, and for $p|d_j$:

$$\left( L_2L_3(P_p), d_j \right)_p = \left( -2(-\bar{a}_i u_3 - \bar{c}_i), d_j \right)_p = \left( \bar{c}_i, d_j \right)_p = \left( \frac{\bar{c}_i}{d_j} \right)_p$$

Whence

$$\langle (d_i, d_i, 1), (1, d_j, d_j) \rangle = \left( \frac{\bar{c}_i}{d_j} \right)$$

Finally we compute the pairing $\langle \Lambda'_i, \Lambda_i \rangle$, then by Cassels pairing

$$\langle \Lambda'_i, \Lambda_i \rangle = \langle (d_i, d_i, 1), (1, d_i, d_i) \rangle = \prod_p \left( L_2L_3(P_p), d_i \right)_p$$

From $\left( \frac{d_i}{p} \right) = 1$ if $p \nmid d_i$, we know this pairing is trivial at $p|2d_i \infty$, thus we suffice to compute at those $p|d_i$, and for $p|d_i$:

$$\left( L_2L_3(P_p), d_i \right)_p = \left( (1 + i_p)u_1(d_i' \bar{b}_i + \bar{c}_i u_1), d_i \right)_p = \left( \bar{c}_i(1 + i_p), d_i \right)_p = (-1)^{\delta_i} \left( \frac{\bar{c}_i}{d_i} \right)$$

Consequently

$$\langle (d_i, d_i, 1), (1, d_i, d_i) \rangle = (-1)^{\delta_i} \left( \frac{\bar{c}_i}{d_i} \right)$$

This completes the proof.

To give the matrix representation of Cassels pairing under the base $\Lambda_1, \cdots, \Lambda_k, \Lambda'_1, \cdots, \Lambda'_k$, we introduce two matrices over $F_2$:

$$\Psi = (\psi_{ij}), \quad D^* = \text{diag}(1 - h_8(d_1), \cdots, 1 - h_8(d_k))$$
where \( \psi_{ii} = \left[ \frac{c_i}{d_i} \right] \) and \( \psi_{ij} = \left[ \frac{\gamma_j}{d_i} \right] \) if \( i \neq j \). By Theorem 3, we have \( 1 - h_8(d_i) \equiv \delta_{d_i} \pmod{2} \). According to the definition of \( A^* \) is §3.3 and Proposition 6, we know the Cassels pairing under the base \( \Lambda_1, \cdots, \Lambda_k, \Lambda'_1, \cdots, \Lambda'_k \) has matrix representation of the form

\[
\begin{pmatrix}
  A^* + \Psi & A^*T + D^*
  \\
  A^* + D^* & A^* + A^*T
\end{pmatrix}
\]

(4.8)

where we used that Cassels pairing is symmetric to derive \( A^* + \Psi \) is symmetric. Then we have:

**Theorem 4.** Let \( n = d_1 \cdots d_k \) be a square-free positive integer with all prime factors congruent to 1 (mod 8), satisfying the following ideal class group conditions:

- \( h_4(d_i) = 1, 1 \leq i \leq k \);
- \( \left( \frac{p_{i_1}}{p_{i_2}} \right) = 1 \) for any prime divisor \( p_{i_1} \) of \( d_{i_1} \) with \( i_1 \neq i_2 \);

If \( A^* \) of \( n \) satisfying

1. \( A^* \) is symmetric;
2. \( A^* + D^* \) is non-singular;

Then:

\[
\text{rank}_Z E^{(n)}(\mathbb{Q}) = 0, \quad \text{III}(E^{(n)}/\mathbb{Q})[2^\infty] \simeq (\mathbb{Z}/2\mathbb{Z})^{2k}
\]

**Proof.** From \( A^* \) symmetric we know \( A^* + A^*T = 0 \), then the Cassels pairing has matrix representation

\[
\begin{pmatrix}
  * & A^*T + D^*
  \\
  A^* + D^* & A^* + A^*T
\end{pmatrix}
\]

by (4.8). Since \( A^* + D^* \) is non-singular, then the Cassels pairing on \( \text{Sel}_2(E^{(n)})/E^{(n)}(\mathbb{Q})[2] \) is non-degenerate, whence as explained in the introduction

\[
\text{rank}_Z E^{(n)}(\mathbb{Q}) = 0, \quad \text{III}(E^{(n)}/\mathbb{Q})[2^\infty] \simeq (\mathbb{Z}/2\mathbb{Z})^{2k}
\]

Now we can prove Theorem 2.

**Proof.** From \( h_8(n) = k \) or \( h_8(n) = k - 1 \) with \( [(2, \sqrt{-n})] \notin 4A \) we know \( A^* = 0 \) by the epimorphism (3.11) and Proposition 4, hence \( A^* \) is symmetric. From \( h_8(d_i) = 0 \) we get \( D^* = \text{diag}(1, \cdots, 1) \) and \( A^* + D^* \) is non-singular, whence (1) and (2) of Theorem 4 are satisfied in this case. Then from Theorem 4 we have

\[
\text{rank}_Z E^{(n)}(\mathbb{Q}) = 0, \quad \text{III}(E^{(n)}/\mathbb{Q})[2^\infty] \simeq (\mathbb{Z}/2\mathbb{Z})^{2k}
\]

The proof is completed.

For the case \( k = 2 \) of Theorem 4 can be characterized by:

**Corollary 1.** Let \( n = d_1d_2 \) be a square-free positive integer with all prime factors congruent to 1 (mod 8) with \( h_4(d_1) = h_4(d_2) = 1 \) such that: \( \left( \frac{p_{i_1}}{p_{i_2}} \right) = 1 \) for any prime divisor \( p_{i_1} \) of \( d_{i_1} \) with \( i_1 \neq i_2 \). Then the conditions (1), (2) on \( A^* \) in Theorem 4 are equivalent to:
\[ \left( \frac{d_1}{d_2} \right)_4 = \left( \frac{d_2}{d_1} \right)_4; \]

- Either exact one of \( h_8(d_1), h_8(d_2) \) is 0 and \( \left( \frac{d_1}{d_2} \right)_4 = -1 \), or both \( h_8(d_1), h_8(d_2) \) equal to 0.

**Proof.** By the definition of \( A^* \) with \( k = 2 \), we may chose \( c_1 = c_2 \) such that

\[ c_1^2 = d_1 a_1^2 + d_2 b_1^2 \quad (4.9) \]

then \( A^* \) is symmetric if and only if \( \left( \frac{c_1}{d_1} \right)_4 = \left( \frac{c_1}{d_1} \right)_4 \). Since

\[
\begin{align*}
\left( \frac{c_1}{d_1} \right)_4 &= \left( \frac{c_1^2}{d_1^4} \right)_4 = \left( \frac{d_1 a_1^2 + d_2 b_1^2}{d_1} \right)_4 = \left( \frac{d_2}{d_1} \right)_4 \cdot \left( \frac{b_1}{d_1} \right)_4 = \left( \frac{d_2}{d_1} \right)_4
\end{align*}
\]

where \( \left( \frac{b_1}{d_1} \right)_4 = 1 \) follows from equation (4.9) modulo \( b_1 \). Similarly we get \( \left( \frac{c_1}{d_1} \right)_4 = \left( \frac{d_2}{d_1} \right)_4 \), whence (1) is equivalent to \( \left( \frac{d_1}{d_2} \right)_4 = \left( \frac{d_2}{d_1} \right)_4 \). Then under this condition \( A^* \) has the form

\[ \begin{bmatrix} c_1 \\ d_1 \end{bmatrix} \cdot \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \]

If \( h_8(d_1) \neq h_8(d_2) \) then \( D^* = \text{diag}(1, 1) \) and \( A^* + D^* \) is non-singular. If \( h_8(d_1) = h_8(d_2) = 1 \), then \( D^* = 0 \) and \( A^* + D^* \) is singular. If exact one of \( h_8(d_1) \) and \( h_8(d_2) \) is 0, then \( A^* + D^* \) is non-singular if and only if \( \left( \frac{c_1}{d_1} \right)_4 = -1 \). Hence this corollary is proved.

**Remark 4.** For \( k = 2 \), the condition of Theorem 3 is non-empty. Since from Theorem 3 we know the 8-rank condition is equivalent to \( h_8(d_1) = h_8(d_2) = 0 \) and \( \left[ d_1 \right] \in 4A \), where the latter is equivalent to \( \left( \frac{d_1}{d_2} \right)_4 = \left( \frac{d_2}{d_1} \right)_4 = 1 \). By Theorem 3 we know \( h_8(d_i) = 0 \) is equivalent to \( \left[ \frac{2}{d_i} \right]_4 \equiv \frac{d_i - 2}{d_i} \) (mod 2), where \( \left[ \frac{2}{d_i} \right]_4 \) is defined similarly as additive Legendre symbol. Then everything reduces to find \( n \) satisfying certain residue symbol properties, then from independence of residue symbol property over \( \mathbb{Q}(i) \) in our coming paper \([7]\), we know there are infinitely many such \( n \), in particular we can get their density.

**Acknowledgements**

I am greatly indebted to Professor Ye Tian, my supervisor, for many instructions and suggestions! I would like to thank Li Cai and Zhe Zhang for carefully reading the paper and giving valuable comments. I also thank Professor Qin Yue for instructions on ideal class group.

**References**

[1] K. Heegner, ‘Diophantische analysis und modulfunctionen,’ *Mathematische Zeitschrift*, vol. 56 (1952) pp. 227–253.

[2] Y. Tian, ‘Congruent numbers and Heegner points,’ *Camb. J. Math.*, vol. 2, no. 1 (2014) pp. 117–161.

[3] D. Li, Y. Tian, ‘On the Birch-Swinnerton-Dyer conjecture of elliptic curves \( E_D : y^2 = x^3 - D^2x \),’ *Acta Math. Sin. (Engl. Ser.)*, vol. 16(2000) pp. 229–236.

25
[4] R. Rhoades, ‘2-Selmer groups and the Birch–Swinnerton-Dyer Conjecture for the congruent number curves,’ *J. Number Theory*, vol. 129, no. 6(2009)pp. 1379–1391.

[5] Y. Ouyang and S. Zhang, ‘On non-congruent numbers with 1 modulo 4 prime factors,’ *Sci. China Math.*, vol. 57, no. 3(2014)pp. 649–658.

[6] J. Cassels, ‘Second descents for elliptic curves,’ *J. Reine Angew. Math.*, vol. 494(1998)pp. 101–127.

[7] Z. Wang, ‘Congruent elliptic curves with non-trivial Shafarevich-Tate groups-distribution part,’ *preprint*.

[8] D. Heath-Brown, ‘The size of selmer groups for the congruent number problem II, with appendix by Monsky,’ *Invent. Math.*, vol. 118(1994)pp. 331–370.

[9] E. Hecke, *Lectures on the theory of algebraic numbers*, Graduate Texts in Mathematics, vol. 77(1981, Springer-Verlag)pp. xii+239.

[10] F. Nemenzo and H. Wada, ‘An elementary proof of Gauss’ genus theorem,’ *Proc. Japan Acad. Ser. A Math. Sci.*, vol. 68, no. 4(1992)pp. 94–95.

[11] H. Jung and Q. Yue, ‘8-ranks of class groups of imaginary quadratic number fields and their densities,’ *J. Korean Math. Soc.* vol. 48, no. 6(2011)pp. 1249–1268.

Zhangjie Wang,
Yau Mathematical Sciences Center,
Tsinghua University, Beijing 100084,China.
zjwang@math.tsinghua.edu.cn