8-RANKS OF CLASS GROUPS OF IMAGINARY QUADRATIC NUMBER FIELDS AND THEIR DENSITIES

HWANYUP JUNG AND QIN YUE

Abstract. For imaginary quadratic number fields $F = \mathbb{Q}(\sqrt{p_1 \cdots p_{t-1}})$, where $\varepsilon \in \{-1, -2\}$ and distinct primes $p_i \equiv 1 \mod 4$, we give conditions of 8-ranks of class groups $C(F)$ of $F$ equal to 1 or 2 provided that 4-ranks of $C(F)$ are at most equal to 2. Especially for $F = \mathbb{Q}(\sqrt{p_1p_2})$, we compute densities of 8-ranks of $C(F)$ equal to 1 or 2 in all such imaginary quadratic fields $F$. The results are stated in terms of congruence relations of $p_i$ modulo $2^n$, the quartic residue symbol $(\frac{p_1}{p_2^2})_4$ and binary quadratic forms such as $p_2 + (2p_1^2)x^2 - 2p_1 y^2$, where $h_+(2p_1)$ is the narrow class number of $\mathbb{Q}(\sqrt{2p_1})$. The results are also very useful for numerical computations.

1. Introduction

It is a classical topic to study the structure of 2-primary subgroups of the narrow class groups $C_+(F)$ for quadratic number fields $F ([1, 2, 3, 9, 12, 13, 14])$. Gerth gave a method to compute their densities ([4, 5, 6, 15, 16]). By genus theory, we have known 2-rank of $C_+(F)$; by Rédei’s matrix, we have got 4-rank of $C_+(F)$ clearly. In this paper, we always assume that $F = \mathbb{Q}(\sqrt{p_1 \cdots p_{t-1}})$, where $\varepsilon \in \{-1, -2\}$, are imaginary quadratic number fields with distinct primes $p_i \equiv 1 \mod 4$. We will mainly obtain conditions for 8-ranks of class groups $C(F)$ equal to 1 or 2 provided that 4-ranks of $C(F)$ are at most equal to 2. Especially for $F = \mathbb{Q}(\sqrt{p_1p_2})$, we compute densities of 8-ranks of $C(F)$ equal to 1 or 2 in all such fields.

In §2, we describe some well-known facts. We support the degree 4 extension $N_+$ over $K = \mathbb{Q}(\sqrt{2p_1})$ with prime $p_1 \equiv 1 \mod 8$, in which all finite primes of $K$ are unramified. We set up relations between the Galois group $\text{Gal}(N_+/K)$ and the narrow class group $C_+(K)$ of $K$. We represent general Legendre symbols

Received July 13, 2010; Revised December 13, 2010.

2010 Mathematics Subject Classification. 11R29, 11R45.

Key words and phrases. class group, unramified extension, quartic residue, density.

The first author was supported by Basic Science Research Program through the National Research Foundation of Korea(NRF) funded by the Ministry of Education, Science and Technology(2011-0005138).

The second author was partly supported by NNSF of China(No. 10771100, No. 10971250).

©2011 The Korean Mathematical Society
by binary quadratic forms \( q^{h_+(2p)/4} = x^2 - 2py^2 \) and \( \pm p_2^{h_+(2p_1)/4} = 2x^2 - p_1y^2 \) over \( \mathbb{Z} \), where \( h_+(2p_1) \) is the narrow class number of \( K \). Meanwhile, we give some quartic reciprocity laws.

In \( \S 3 \), we investigate 8-ranks of class groups \( C(F) \) for imaginary quadratic fields \( F = \mathbb{Q}(\sqrt{\varepsilon p_1 \cdots p_i - 1}) \), where \( \varepsilon \in \{-1, -2\} \) and distinct primes \( p_i \equiv 1 \mod 4 \). We give the necessary and sufficient conditions for 8-ranks of \( C(F) \) equal to 1 or 2 provided that 4-ranks of \( C(F) \) are at most equal to 2. Their results are expressed by congruence relations of \( p \) equal to 1 or 2 provided that 4-ranks of \( p \) are at most equal to 2 in such quadratic number fields (Theorem 4.1). These results are very useful for numerical calculations.

In \( \S 4 \), especially for \( F = \mathbb{Q}(\sqrt{p_1p_2}) \), we compute densities for 8-ranks of \( C(F) \) equal to 1 or 2 in such quadratic number fields (Theorem 4.1).

We use the following notation:

\[
\begin{align*}
\mathcal{O}_F & \quad \text{ring of integers of a quadratic number field } F = \mathbb{Q}(\sqrt{d}), \\
C(F), C_+(F) & \quad \text{ideal class group, narrow ideal class group of } F, \\
h(d), h_+(d) & \quad \text{class number, narrow class number of } F = \mathbb{Q}(\sqrt{d}), \\
p_a & \quad \text{ideal of } F \text{ over an integer } a \in \mathbb{Z}, \\
[p_a] & \quad \text{class of an ideal } p_a \subseteq \mathcal{O}_F \text{ in } C_+(F), \\
t & \quad \text{ideals of } F = \mathbb{Q}(\sqrt{d}) \text{ over prime } 2, \\
_2 A & \quad \text{subgroup of elements of order } \leq 2 \text{ of an abelian group } A, \\
r_{2^n}(A) & \quad 2^n\text{-rank of } A, \\
R_F & \quad \text{Rédéi’s matrix of } F, \\
A^+ & \quad \text{set of primes } p \equiv 1 \mod 8 \text{ represented by } x^2 + 32y^2 \text{ over } \mathbb{Z}, \\
A^- & \quad \text{set of primes } p \equiv 1 \mod 8 \text{ not represented by } x^2 + 32y^2 \text{ over } \mathbb{Z}, \\
B^+ & \quad \text{set of primes } p \equiv 1 \mod 8 \text{ represented by } x^2 + 64y^2 \text{ over } \mathbb{Z}, \\
B^- & \quad \text{set of primes } p \equiv 1 \mod 8 \text{ not represented by } x^2 + 64y^2 \text{ over } \mathbb{Z}, \\
(\frac{\xi}{2}), (\frac{\xi}{7})_4 & \quad \text{Legendre symbol, quartic residue symbol.}
\end{align*}
\]

2. Preliminaries

First, for a prime \( p_1 \equiv 1 \mod 8 \), we find the cyclic extension \( N_+ \) of degree 4 over \( K = \mathbb{Q}(\sqrt{2p_1}) \), in which no finite prime of \( K \) ramifies. In terms of norm from \( L = \mathbb{Q}(\sqrt{2}) \) over \( Q \), \( p_1 = u_1^2 - 2w_1^2 \) with \( u_1, w_1 \in \mathbb{Z} \) and, without loss of generality, we shall always assume that

\[
\pi_1 = u_1 + w_1\sqrt{2} \in L \text{ with } u_1 \equiv 1 \mod 4, \ w_1 \equiv 0 \mod 4,
\]

which is called a primary element in \( L \). In fact, \( w_1 \) is even and we can multiply \( u_1 + w_1\sqrt{2} \) by the element \( (1 + \sqrt{2})^2 = 3 + 2\sqrt{2} \) of norm 1, if necessary. By genus theory, 2-primary subgroup of the narrow class group \( C_+(K) \) of \( K \) is a cyclic and \( 4|h_+(2p_1) \). Let \( N_+ = \mathbb{Q}(\sqrt{2}, \sqrt{p_1}, \sqrt{\pi_1}) \). It is clear that \( N_+ \) is a normal extension of degree 8 over \( Q \). Consider the tower of relative quadratic
extensions:

\[ N_+ = \mathbb{Q}(\sqrt{2}, \sqrt{p_1}, \sqrt{\overline{p}_1}) \]

\[ K_1 = \mathbb{Q}(\sqrt{2}, \sqrt{p_1}) \]

\[ K = \mathbb{Q}(\sqrt{2p_1}) \]

\[ \mathbb{Q}. \]

Let \( t \) and \( p_1 \) be the prime ideals of \( K \) over 2 and \( p_1 \), respectively. We can verify that \( t \) and \( p_1 \) are unramified in \( N_+ \), so all finite primes of \( K \) are unramified in \( N_+ \) (in details, see [3]). Moreover, if \( p_1 \in A^+ \), then \( u_1 \in \mathbb{N} \) by [1], so \( N_+ \) is the unramified cyclic extension of degree 4 over \( K \).

Let \( p_2 \equiv 1 \mod 8 \) be a prime. Then \( p_2 = u_2^2 - 2w_2^2 \) with \( u_2, w_2 \in \mathbb{Z} \), and

\[ \pi_2 = u_2 + w_2\sqrt{2} \in L \text{ with } u_2 \equiv 1 \mod 4, \quad w_2 \equiv 0 \mod 4. \]

Suppose \( \left( \frac{\pi_1}{p_2} \right) = 1 \), so \( p_2 \) splits completely in \( K_1 \). Let \( \mathfrak{p}_2 = \pi_2\mathcal{O}_L = (\pi_2) \) be a prime ideal of \( L \) over \( p_2 \) and \( \mathfrak{p}_2 \) be a prime ideal of \( K_1 \) over \( \mathfrak{p}_2 \), i.e., \( \mathfrak{p}_2|p_2 \) and \( \mathfrak{p}_2|\mathfrak{p}_2 \). Then \( \mathcal{O}_{K_1}/\mathfrak{p}_2 \cong \mathcal{O}_L/\mathfrak{p}_2 \cong \mathbb{Z}/(p_2) \). Hence the general Legendre symbol ([8, p. 196])

\[ \left( \frac{\pi_1}{p_2} \right) = \left( \frac{\pi_1}{p_2} \right), \]

which is denoted by \( \left( \frac{\pi_1}{p_2} \right) \). In fact,

\[ \left( \frac{\pi_1}{p_2} \right) = 1 \leftrightarrow x^2 \equiv \pi_1 \mod \pi_2\mathcal{O}_L \text{ has a solution in } \mathcal{O}_L. \]

Since \( \mathcal{O}_L/\mathfrak{p}_2 \cong \mathbb{Z}/(p_2) \) and \( \left( \frac{\mathfrak{p}_1}{p_2} \right) = 1, \left( \frac{\pi_1}{\mathfrak{p}_2} \right) = \left( \frac{w_1}{\mathfrak{p}_2} \right) \), where \( \pi_1 = u_1 - w_1\sqrt{2} \) is the conjugate element of \( \pi_1 \). Hence \( p_2 \) splits completely in \( L_1 = \mathbb{Q}(\sqrt{2}, \sqrt{\overline{p}_1}) \) if and only if \( \left( \frac{\pi_1}{p_2} \right) = 1 \). By the reciprocity law ([8, Theorem 165]), we have \( \left( \frac{\pi_1}{\mathfrak{p}_2} \right) = \left( \frac{\pi_1}{\mathfrak{p}_2} \right) \). Therefore \( p_2 \) splits completely in \( N_+ \) if and only if \( \left( \frac{\pi_1}{\mathfrak{p}_2} \right) = 1 \). We have proved:

**Lemma 2.1.** Let \( p_1 \equiv p_2 \equiv 1 \mod 8 \) be primes with \( \left( \frac{\pi_1}{p_2} \right) = 1 \) and \( \pi_1, \pi_2 \) be defined as above. Then

(i) \( p_2 \) splits completely in \( N_+ \) if and only if \( \left( \frac{\pi_1}{p_2} \right) = 1 \).

(ii) \( p_2 \) splits completely in \( K_1 \) but does not in \( N_+ \) if and only if \( \left( \frac{\pi_1}{p_2} \right) = -1 \).

In the following, we use the binary quadratic form to describe the value of \( \left( \frac{\pi_1}{p_2} \right) \). Let \( H_+(K) \) be the narrow Hilbert class field of \( K \), which is the maximal abelian extension over \( K \) in which no finite prime of \( K \) ramifies. Then \( \text{Gal}(H_+(K)/K) \cong C_+(K) \) and \( K \subset K_1 \subset N_+ \subset H_+(K) \). Especially, if \( p_1 \in A^+ \), then \( N_+ \subset H(K) \), which is the Hilbert class field of \( K \). By restriction there is an epimorphism: \( C_+(K) \rightarrow \text{Gal}(N_+/K) \), where \( \text{Gal}(N_+/K) \) is cyclic of order 4. Hence

\[ C_+(K)/C_+(K)^4 \cong \text{Gal}(N_+/K) \]
and analogously

\[ C_+(K)/C_+(K)^2 \cong \text{Gal}(K_1/K). \]

Let \( p \) be a prime ideal of \( \mathcal{O}_K \). We have that \( p \) splits completely in \( N_+ \Leftrightarrow \) the Artin symbol \( (N_+)_p = 1 \in \text{Gal}(N_+/K) \Leftrightarrow [p] \in C_+(K)^4 \) (see [11, p. 104]). Let \( p_2 \) be a prime ideal of \( \mathcal{O}_K \) over \( p_2 \). Then we conclude that \( p_2 \) splits completely in \( N_+ \Leftrightarrow (\frac{\pi}{p_2}) = 1 \Leftrightarrow [p_2] \in C_+(K)^3 \Leftrightarrow [p_2]^{h_+(2p_1)/4} = 1 \Leftrightarrow p_2^{h_+(2p_1)/4} = x^2 - 2p_1y^2 \) for some \( x, y \in \mathbb{Z} \).

Let \( t \) and \( p_1 \) be prime ideals of \( \mathcal{O}_K \) over \( 2 \) and \( p_1 \), respectively. By genus theory, \([t], [p_1]\) and \([tp_1]\) are of order at most 2 and only one of them is the unit in \( C_+(K) \). Suppose \([t]\) is of order 2. Then we have that \( p_2 \) splits completely in \( K_1 \) but does not in \( N_+ \Leftrightarrow (\frac{\pi}{p_2}) = -1 \Leftrightarrow [p_2] \in C_+(K)^2 \) and \([p_2] \notin C_+(K)^4 \)

\( \Leftrightarrow [t][p_2]^{h_+(2p_1)/4} = 1 \in C_+(K) \Leftrightarrow p_2^{h_+(2p_1)/4} = 2x^2 - p_2y^2 \) for some \( x, y \in \mathbb{Z} \).

Suppose \([t]\) is of order 2 and \([p_1]\) is of order 2. Then, similarly, we have that \((\frac{\pi}{p_2}) = -1 \Leftrightarrow [p_1][p_2]^{h_+(2p_1)/4} = 1 \in C_+(K) \Leftrightarrow p_2^{h_+(2p_1)/4} = p_1x^2 - 2y^2 \) for some \( x, y \in \mathbb{Z} \).

Hence we have proved:

**Lemma 2.2.** Let \( p_1 \equiv p_2 \equiv 1 \mod 8 \) be primes with \((\frac{p_1}{p_2}) = 1\). Then

\begin{enumerate}
  \item \((\frac{p_1}{p_2}) = 1 \) if and only if \( p_2^{h_+(2p_1)/4} = x^2 - 2p_1y^2 \) for some \( x, y \in \mathbb{Z} \).
  \item \((\frac{p_1}{p_2}) = -1 \) if and only if \( \pm p_2^{h_+(2p_1)/4} = 2x^2 - p_1y^2 \) for some \( x, y \in \mathbb{Z} \).
\end{enumerate}

Moreover, for \( p_2 = u_2^2 - 2w_2^2 \equiv 1 \mod 8 \), we have that \( (\frac{p_2}{p_1}) = 1 = (\frac{p_2}{p_1}) \).

Since \( p_2 = 2(u_2 + w_2)^2 - (u_2 + 2w_2)^2 \) and \( u_2 + w_2 \equiv w_2(1 - \sqrt{-1}) \mod p_2 \mathfrak{O}_L \), by [1], we conclude that

\[ p_2 \in A^+ \Leftrightarrow u_2 > 0, u_2 + w_2 > 0 \Leftrightarrow \left( \frac{u_2 + w_2}{p_2} \right) = \left( \frac{1 - \sqrt{2}}{p_2} \right) = 1; \]

\[ \left( \frac{u_2}{p_2} \right) = 1 \Leftrightarrow \left( \frac{2}{p_2} \right)_4 = 1 \Leftrightarrow p_2 \in B^+. \]

Now we describe some results about quartic reciprocity law. Let \( p_1 \equiv p_2 \equiv 1 \mod 4 \) be distinct primes. Then \( p_1 = a_1^2 + b_1^2, p_2 = a_2^2 + b_2^2, b_1 \equiv b_2 \equiv 0 \mod 2 \), over \( \mathbb{Z} \) in terms of norm from \( L_1 = \mathbb{Q}(i) \), where \( i = \sqrt{-1} \). We shall always assume that

\[ \lambda_1 = a_1 + ib_1, \lambda_2 = a_2 + ib_2 \text{ with } a_1 + b_1 \equiv a_2 + b_2 \equiv 1 \mod 4, \]

which are called primary elements in \( L_1 \).

For any \( \alpha \in \mathbb{Z}[i] \) with \( \lambda_1 \nmid \alpha \), there exists a unique integer \( j \) (0 ≤ j ≤ 3) such that

\[ \alpha^{N(\lambda_1)^{-1}} \equiv i^j \mod \lambda_1 \mathfrak{O}_{L_1}. \]

We will define by \((\frac{\alpha}{\lambda_1})_4 = i^j \) the quartic residue symbol of \( \alpha \) modulo \( \lambda_1 \). There is a fact that \((\frac{\alpha}{\lambda_1})_4 = 1 \) if and only if \( x^4 \equiv p_2 \mod p_1 \) has a solution with \( x \in \mathbb{Z} \),
which is denoted by \( (\frac{p}{a})_4 = 1 \). There is the law of quartic reciprocity (see [10, p.123]):

\[
\left( \frac{\lambda_1}{\lambda_2} \right)_4 = \left( \frac{\lambda_2}{\lambda_1} \right)_4 (-1)^{\frac{(p_1-1)(p_2-1)}{4}}.
\]

**Lemma 2.3.** Let \( p_1 \equiv p_2 \equiv 1 \mod 4 \) be distinct primes, \( p_1 = a_1^2 + b_1^2, p_2 = a_2^2 + b_2^2 \), and \( \lambda_1 = a_1 + ib_1, \lambda_2 = a_2 + ib_2 \) be primary elements as above.

(i) If \( (\frac{p_1}{p_2})_4 = 1 \), then \( (\frac{p_2}{p_1})_4 (\frac{p_1}{p_2})_4 = (\frac{\lambda_2}{\lambda_1})_4 \).

(ii) Suppose \( p_1 \equiv p_2 \equiv 5 \mod 8 \) and \( (\frac{p_1}{p_2})_4 = -1 \). Then

\[
\left( \frac{2p_1}{p_2} \right)_4 \left( \frac{2p_2}{p_1} \right)_4 = i^{a_1 + a_2 - b_1 - b_2} \left( \frac{\lambda_2}{\lambda_1} \right)_4,
\]

where we take \( a_1 + b_1 \equiv a_2 + b_2 \equiv 1 \mod 8 \).

**Proof.** (i) Let \( p_1 = \lambda_1 \bar{\lambda}_1 \) and \( p_2 = \lambda_2 \bar{\lambda}_2 \), where \( \lambda_1 \) and \( \lambda_2 \) are the conjugate elements of \( \lambda_1 \) and \( \lambda_2 \), respectively. By the quartic reciprocity law, we have that

\[
\left( \frac{p_1}{p_2} \right)_4 \left( \frac{p_2}{p_1} \right)_4 = \left( \frac{p_1}{p_2} \right)_4 (\frac{p_2}{p_1})_4 = \left( \frac{\lambda_1}{\lambda_2} \right)_4 \left( \frac{\lambda_2}{\lambda_1} \right)_4 \left( \frac{\lambda_2}{\lambda_1} \right)_4 \left( \frac{\bar{\lambda}_1}{\bar{\lambda}_2} \right)_4 = \left( \frac{\lambda_2}{\lambda_1} \right)_4 \left( \frac{\lambda_2}{\lambda_1} \right)_4 \left( \frac{\bar{\lambda}_1}{\bar{\lambda}_2} \right)_4 \left( \frac{\bar{\lambda}_1}{\bar{\lambda}_2} \right)_4 = \left( \frac{\lambda_2}{\lambda_1} \right)_4 \left( \frac{\lambda_2}{\lambda_1} \right)_4 .
\]

where \( \left( \frac{\lambda_2}{\lambda_1} \right)_4 \left( \frac{\lambda_2}{\lambda_1} \right)_4 = 1 \).

(ii) Similarly, we have that

\[
\left( \frac{2p_1}{p_2} \right)_4 \left( \frac{2p_2}{p_1} \right)_4 = \left( \frac{2p_1}{p_2} \right)_4 (\frac{2p_2}{p_1})_4 = \left( \frac{2}{\lambda_1 \lambda_2} \right)_4 \left( \frac{p_1}{p_2} \right)_4 \left( \frac{p_2}{p_1} \right)_4 = \left( \frac{2}{\lambda_1 \lambda_2} \right)_4 \left( \frac{\lambda_2}{\lambda_1} \right)_4 .
\]

Since \( p_1 \equiv 5 \mod 8 \) and \( 2p_1 = (a_1 + b_1)^2 + (a_1 - b_1)^2 \), we assume that \( a_1 + b_1 \equiv 1 \mod 8 \) and \( a_1 - b_1 \equiv 5 \mod 8 \). Similarly, we may assume that \( a_2 + b_2 \equiv 1 \mod 8 \) and \( a_2 - b_2 \equiv 5 \mod 8 \). By [10, p. 136, Ex.37], we have \( \left( \frac{1+i}{\lambda_1} \right)_4 = i^{(a_1 - b_1 - b_1^2 - 1)/4} \). Since \( 2 = i^3(1 + i)^2 \) and \( \left( \frac{1+i}{\lambda_1} \right)_4 = i^{(p-1)/4} \), we have

\[
\left( \frac{2}{\lambda_1} \right)_4 \left( \frac{2}{\lambda_2} \right)_4 = i^{3(p_1+1+p_1+1)+(a_1+b_1)-b_1^2-1} = i^{p_1+2p_2-2} = i^{p_1+2p_2-2} .
\]

In fact, since \( a_1 + b_1 \equiv a_2 + b_2 \equiv 1 \mod 8 \), \( a_1 - b_1 - b_1^2 - 1 = a_1 + b_1 - (b_1 + 1)^2 \equiv 0 \mod 8 \) and \( a_2 - b_2 - b_2^2 - 1 = a_2 + b_2 - (b_2 + 1)^2 \equiv 0 \mod 8 \). \( \square \)
Then we have that
\[ R \text{ trivial solution over } \mathbb{Z} \]
\[ \text{class group distinct primes } p \]
\[ \text{phantine equations } qz \]
We know the method of Rédei’s matrix to determine the solutions of the Diophantine equations.\[ (\frac{D}{p^*}) \]
Then the Rédei matrix \( R_F = (a_{ij}) \) of \( F \) is the \( t \times t \) matrix with \( a_{ij} \in \mathbb{F}_2 \) given by
\[ a_{ij} = \begin{cases} 
(\frac{p^*}{q})_i^j & \text{if } i \neq j, \\
(\frac{D}{p^*})_i & \text{if } i = j, 
\end{cases} \quad \text{for } 1 \leq i, j \leq t. \]
Note that the sum of all rows of \( R_F \) is equal to 0. Let \( R_F' \) be the \((t-1) \times t\) matrix obtained from \( R_F \) by deleting the \( t \)-th row. Then rank \( R_F' = \text{rank } R_F \), where the rank is always meant to the rank over \( \mathbb{F}_2 \).

Let \( D(F) \) be the set of all positive square-free divisors \( q \) of the discriminant \( D \). Then \( D(F) \) is an elementary abelian 2-group with multiplication \( q_1 \cdot q_2 = q_1 q_2/(q_1, q_2)^2 \), where \( (q_1, q_2) \) is the greatest common divisor of \( q_1, q_2 \). For \( q \in D(F) \), we define \( X_q = (x_1, \ldots, x_t)^T \in \mathbb{F}_2^t \) by
\[ x_i = \begin{cases} 
1 & \text{if } p_i \mid q, \\
0 & \text{if } p_i \nmid q, 
\end{cases} \quad \text{for } 1 \leq i \leq t. \]
Then we have that \( R_F' X_q = 0 \iff (\frac{q}{p}) = 1 \) for every odd prime \( p \mid (D/q) \) and \( (\frac{-D/q}{p}) = 1 \) for every odd prime \( p \mid q \iff x^2 - Dy^2 = qz^2 \) is solvable over \( \mathbb{Z} \iff q \in D(F) \cap N_{F/Q}(F^*) \). Hence,
\[ \theta : D(F) \cap N_{F/Q}(F^*) \to \{ X_q : R_F' X_q = 0 \}, \quad q \mapsto X_q, \]
is an isomorphism. By genus theory, \( \alpha : D(F) \cap N_{F/Q}(F^*) \to 2C(F) \cap C(F)^2 \)
is surjective and \( |\text{Ker}(\alpha)| = 2 \). We have the Rédei’s criterion:
\[ r_2(C_+(F)) = r_2(D(F) \cap N_{F/Q}(F^*)) - 1 = t - 1 - \text{rank } R_F. \]
We know the method of Rédei’s matrix to determine the solutions of the Diophantine equations \( qz^2 = x^2 - Dy^2 \) over \( \mathbb{Z} \). For convenience, if it has a non-trivial solution over \( \mathbb{Z} \), then it will be called solvable.

Let \( F = \mathbb{Q}(\sqrt{-d}) \) be an imaginary quadratic field with \( d = p_1 \cdots p_{t-1} \) and distinct primes \( p_i \equiv 1 \mod 4 \). Then the narrow class group \( C_+(F) \) is just the class group \( C(F) \) and \( r_2(C(F)) = t - 1 \) by genus theory. The Rédei’s matrix

3. Elements of order 8

Let \( F = \mathbb{Q}(\sqrt{D}) \) be a quadratic field and \( D \) be the discriminant of \( F \). The prime discriminant is either \( p^* = (-1)^{(p-1)/2} p \) if \( p \) is an odd prime or \( p^* = -4,8,-8 \) if \( p = 2 \). Then \( D \) has the unique decomposition \( D = p_1^\alpha \cdots p_t^\beta \)
into a product of prime discriminants and \( p_i = 2 \) if \( 2 \mid D \). By genus theory, \( r_2(C_+(F)) = t - 1 \).

We will denote by \( (\frac{p}{n}) \) the Legendre symbol if \( p \) is an odd prime and by \( (\frac{q}{2}) \) the Kronecker symbol. If \( (\frac{p}{n}) = (-1)^n \) with \( a \in \mathbb{F}_2 \), we shall write \( (\frac{q}{2})' = a \).
Then the Rédei matrix \( R_F = (a_{ij}) \) of \( F \) is the \( t \times t \) matrix with \( a_{ij} \in \mathbb{F}_2 \) given by
\[ a_{ij} = \begin{cases} 
(\frac{p^*}{q})_i^j & \text{if } i \neq j, \\
(\frac{D}{p^*})_i & \text{if } i = j, 
\end{cases} \quad \text{for } 1 \leq i, j \leq t. \]
Note that the sum of all rows of \( R_F \) is equal to 0. Let \( R_F' \) be the \((t-1) \times t\) matrix obtained from \( R_F \) by deleting the \( t \)-th row. Then rank \( R_F' = \text{rank } R_F \), where the rank is always meant to the rank over \( \mathbb{F}_2 \).

Let \( D(F) \) be the set of all positive square-free divisors \( q \) of the discriminant \( D \). Then \( D(F) \) is an elementary abelian 2-group with multiplication \( q_1 \cdot q_2 = q_1 q_2/(q_1, q_2)^2 \), where \( (q_1, q_2) \) is the greatest common divisor of \( q_1, q_2 \). For \( q \in D(F) \), we define \( X_q = (x_1, \ldots, x_t)^T \in \mathbb{F}_2^t \) by
\[ x_i = \begin{cases} 
1 & \text{if } p_i \mid q, \\
0 & \text{if } p_i \nmid q, 
\end{cases} \quad \text{for } 1 \leq i \leq t. \]
Then we have that \( R_F' X_q = 0 \iff (\frac{q}{p}) = 1 \) for every odd prime \( p \mid (D/q) \) and \( (\frac{-D/q}{p}) = 1 \) for every odd prime \( p \mid q \iff x^2 - Dy^2 = qz^2 \) is solvable over \( \mathbb{Z} \iff q \in D(F) \cap N_{F/Q}(F^*) \). Hence,
\[ \theta : D(F) \cap N_{F/Q}(F^*) \to \{ X_q : R_F' X_q = 0 \}, \quad q \mapsto X_q, \]
is an isomorphism. By genus theory, \( \alpha : D(F) \cap N_{F/Q}(F^*) \to 2C(F) \cap C(F)^2 \)
is surjective and \( |\text{Ker}(\alpha)| = 2 \). We have the Rédei’s criterion:
\[ r_2(C_+(F)) = r_2(D(F) \cap N_{F/Q}(F^*)) - 1 = t - 1 - \text{rank } R_F. \]
We know the method of Rédei’s matrix to determine the solutions of the Diophantine equations \( qz^2 = x^2 - Dy^2 \) over \( \mathbb{Z} \). For convenience, if it has a non-trivial solution over \( \mathbb{Z} \), then it will be called solvable.
Hence, since \( R(\text{independent of all rows of} \ 1 \mod 8), \) we need to prove rank \( R \) by column vectors of \( R \) row vectors of \( R \) 1, then \( R \) is a symmetric matrix, the addition with the first \( s \) columns (rows) of \( R \) is equal to zero vector, so \( \left( \frac{2}{p_1 \cdots p_s} \right) = 1 \), i.e., \( q = p_1 \cdots p_s \equiv 1 \mod 8 \).

Conversely, since \( d = p_1 \cdots p_{t-1} \in D(E), d \equiv 1 \mod 8 \) and \( \left( \frac{2}{p_1 \cdots p_{t-1}} \right) = 1 \), we need to prove rank \( R(\text{independent of all rows of} \ 1 \mod 8) \). Without loss of generality, we assume that the first \( k = t-1-r \) rows \( \beta_1, \ldots, \beta_k \) of \( R \) is a maximal subset of linearly independent of all rows of \( R \). If, for a row \( \beta_i (k < i \leq t-1) \) of \( R \), we have \( \beta_1 + \cdots + \beta_k + \beta_i = 0 \), then \( q = p_1 \cdots p_k p_i \in D(E) \) and \( q \equiv 1 \mod 8 \). Let

\[
M' = \begin{pmatrix}
(\beta_1 \left( \frac{2}{p_1} \right))' \\
\vdots \\
(\beta_k \left( \frac{2}{p_k} \right))' \\
(\beta_i \left( \frac{2}{p_i} \right))'
\end{pmatrix}.
\]
Then \((\frac{2}{p_1})^r + \cdots + (\frac{2}{p_k})^r = 0\) and rank \(M' = k\), so the last row of \(M'\) is linearly represented by the first \(k\) rows of \(M'\). Hence \(\text{rank}(R_E, \alpha) = \text{rank} R_E\) and \(\alpha\) is linearly represented by column vectors of \(R_E\).

Write \(D^*(F) = D(F) \cap N_{F/Q}(F^*)\) for simplicity.

Remark 3.2. By the process of proving Proposition 3.1, we have that

(i) \(\nu = \nu(C(E))\) if and only if \(D^*(F) = D^*(E)\);

(ii) \(\nu = \nu(C(E)) + 1\) if and only if there is some \(q|p_1 \cdots p_{r-1}\) such that \(2qz^2 = x^2 + p_1 \cdots p_{r-1}y^2\) is solvable if and only if \(2q \in D^*(F)\).

By Proposition 3.1, we have that \(r_4(C(F)) = 1\) if and only if one of the following conditions holds:

1. \(\text{rank } R_E = \text{rank } R_E + 1 = t - 2\) and \(D^*(F) = D^*(E) = \{1, q_1, q_2, d\}\), where at least one of \(q_1 = p_1 \cdots p_r\) and \(q_2 = p_{r+1} \cdots p_{r-1}\) is congruent to 5 modulo 8 \((1 \leq r < t - 1)\);

2. \(\text{rank } R_E = \text{rank } R_E = t - 2\) and \(p_1 \cdots p_{r-1} \equiv 1 \mod 8\), so \(D^*(F) = \{1, 2q_1, 2q_2, d\}\), where \(q_1 = p_1 \cdots p_r\) and \(q_2 = p_{r+1} \cdots p_{r-1}\) \((0 \leq r < t - 1)\) and \(q_1 = 1\) if \(r = 0\).

Theorem 3.3. Let \(F = \mathbb{Q}(\sqrt{-d})\), where \(d = p_1 \cdots p_{r-1}\) with distinct primes \(p_i \equiv 1 \mod 4\), be an imaginary quadratic field and \(r_4(C(F)) = 1\).

(i) Suppose \(D^*(F) = \{1, q_1, q_2, d\}\), where \(q_1 = p_1 \cdots p_r \equiv 1 \mod 8\) and \(q_2 = p_{r+1} \cdots p_{r-1} \equiv 5 \mod 8\). Then \(r_8(C(F)) = 1\) if and only if \((\frac{q_1}{q_2})_4 = 1\).

(ii) Suppose \(D^*(F) = \{1, q_1, q_2, d\}\), where \(q_1 = p_1 \cdots p_r \equiv 5 \mod 8\) and \(q_2 = p_{r+1} \cdots p_{r-1} \equiv 5 \mod 8\). Then \(r_8(C(F)) = 1\) if and only if either \(d \equiv 9 \mod 16\) and \((\frac{q_1}{q_2})_4(\frac{q_2}{q_1})_4 = -1\) or either \(d \equiv 1 \mod 16\) and \((\frac{q_1}{q_2})_4(\frac{q_2}{q_1})_4 = 1\).

(iii) Suppose \(D^*(F) = \{1, 2q_1, 2q_2, d\}\), where \(q_1 = p_1 \cdots p_r \equiv 5 \mod 8\) and \(q_2 = p_{r+1} \cdots p_{r-1} \equiv 5 \mod 8\). Then \(r_8(C(F)) = 1\) if and only if either \(d \equiv 9 \mod 16\) and \((\frac{q_1}{q_2})_4(\frac{q_2}{q_1})_4 = -1\) or either \(d \equiv 1 \mod 16\) and \((\frac{q_1}{q_2})_4(\frac{q_2}{q_1})_4 = 1\).

Proof. (i) Suppose rank \(R_E = t - 2\), \(D^*(F) = \{1, q_1, q_2, d\}\) and \(q_1 = p_1 \cdots p_r \equiv 1 \mod 8\), \(q_2 = p_{r+1} \cdots p_{r-1} \equiv 5 \mod 8\). Then the sum of the first \(r\) row vectors of \(R_E\) is equal to zero vector. Let \(q_1^2 = q_1O_F\). Then \(1 \not\equiv [q_1] \in 2C(F) \cap C(F)^2\).

By Rédei’s criterion, \(z^2 = q_1x^2 + q_2y^2\) has a relatively prime solution \((x, y, z) = (a, b, c)\) over \(\mathbb{N}\), so \([q_1] = [c]^2 \in C(F)^2\), where \(c\) is an ideal of \(O_F\) over \(c\).

Since \(c^2 = q_1a^2 + q_2b^2\) and \(q_1 \equiv 1 \mod 8\), we have that the Jacobi symbols \((\frac{c}{q_1}) = 1\) and \((\frac{c}{q_2}) = (\frac{q_2}{q_1})_4\), where \((\frac{q_1}{q_2})_4 = (\frac{q_2}{q_1})_4(\frac{q_2}{q_1})_4\). We conclude that \(r_8(C(F)) = 1 \iff [q_1] \in C(F)^4 \iff [c][m] \in C(F)^2\), where \(m\) is an ambiguous
ideal of \( F \) over \( m|2d \Leftrightarrow mcz^2 = x^2 + dy^2 \) is solvable over \( \mathbb{Z} \Leftrightarrow \) the following system of equations is solvable over \( \mathbb{F}_2 \)

\[
R'_F X = \left( \begin{array}{c} (\frac{a}{p_1})' \\ \vdots \\ (\frac{c}{p_{r-1}})'
\end{array} \right)
\]

\( \Leftrightarrow (\frac{x}{q_1}) = (\frac{a}{p_1 \cdots p_r}) = 1 = (\frac{z}{q_1})_4 \) (since rank \( R'_F = t - 2 \)).

(ii) Suppose rank \( R_F = t - 2 \), \( D^*(F) = \{1, q_1, q_2, d\} \) and \( q_1 = p_1 \cdots p_r \equiv 5 \text{ mod } 8, \quad q_2 = p_r+1 \cdots p_{r-1} \equiv 5 \text{ mod } 8 \). Then the sum of the first \( t - 1 \) row vectors of \( R_F \) is equal to zero vector and the sum of the first \( r \) row vectors of \( M \) is also equal to zero. Let \( z^2 = q_1 x^2 + q_2 y^2 \) have a non-trivial solution \((x, y, z) = (a, b, c)\) over \( \mathbb{N} \). Then, by Rédei’s criterion, \( r_4(C(F)) = 1 \) and \( 1 \neq [q_1] = [c]^2 \in xC(F) \cap C(F)^2 \), where \( q_1 \mathcal{O}_F = q_1 \mathcal{O}_F \) and \( c \) is an ideal of \( F \) over \( c \). Since \( q_1 \equiv q_2 \equiv 5 \text{ mod } 8 \), without loss of generality, \( c^2 = q_1 a_2 + 4q_2 b^2 \), where \( b = 2y' \) and \( a \equiv b' \equiv 1 \text{ mod } 2 \). Hence the Jacobi symbol \((\frac{a}{q_1}) = 1 = (\frac{b}{q_1}) = -(\frac{c}{q_1}) \).

Since \( c^2 = q_1 a^2 + q_2 b^2 \), we have that \((\frac{c}{q_1}) = (\frac{a}{q_1})_4 (\frac{b}{q_1})_4 \) and \((\frac{c}{q_2}) = (\frac{a}{q_2})_4 (\frac{b}{q_2})_4 \).

Similarly, we conclude that \( r_8(C(F)) = 1 \Leftrightarrow [q_1] \in C(F)^4 \Leftrightarrow (\frac{c}{q_1}) = (\frac{a}{q_1})_4 \Leftrightarrow (\frac{q_1}{q_2})_4 (\frac{q_2}{q_1})_4 = -1. \)

(iii) Suppose rank \( R_F = t - 2 \) and \( D^*(F) = \{1, q_1, q_2, d\} \), where \( q_1 = p_1 \cdots p_r \equiv 5 \text{ mod } 8 \) and \( q_2 = p_r+1 \cdots p_{r-1} \equiv 5 \text{ mod } 8 \). Then the sum of the first \( t - 1 \) row vectors of \( R_F \) is equal to zero vector, i.e., \((\frac{a}{q_1})_4 \). Let \( 2z^2 = q_1 x^2 + q_2 y^2 \) have a non-trivial solution \((x, y, z) = (a, b, c)\) over \( \mathbb{N} \), where \( a, b, c \) are all odd. Then \( 1 \neq [q_1] = [c]^2 \in C(F)^2 \), where \( t^2 = 2\mathcal{O}_F, q_1 = q_1 \mathcal{O}_F \), and \( c \) is an ideal of \( F \) over \( c \). Since \( 2c^2 = q_1 a^2 + q_2 b^2 \), we have that Jacobi symbols \((\frac{a}{q_2}) = (\frac{b}{q_2}) = 1 \)

\[
(\frac{c}{q_1}) = (\frac{a}{q_2})_4 (\frac{b}{q_2})_4.
\]

Since \((q_1a)^2 + db^2 = 2q_1a^2 \equiv 10 \text{ mod } 16 \), we have that \( d \equiv 9 \text{ mod } 16 \Leftrightarrow 9a^2 + 9b^2 \equiv 10 \text{ mod } 16 \Leftrightarrow ab \equiv \pm 3 \text{ mod } 8 \Leftrightarrow (\frac{a}{q_2}) = - (\frac{a}{q_1}) = -(\frac{c}{q_1}) \); in other word, \( d \equiv 1 \text{ mod } 16 \Leftrightarrow (\frac{b}{q_2})_4 = (\frac{c}{q_1})_4. \) We conclude that \( r_8(C(F)) = 1 \Leftrightarrow [q_1] \in C(F)^4 \Leftrightarrow (\frac{a}{q_2}) = 1, \) i.e., \((\frac{a}{q_1}) = (\frac{a}{q_2}) \Leftrightarrow \) either \( d \equiv 9 \text{ mod } 16 \) with \((\frac{q_1}{q_2})_4 (\frac{q_2}{q_1})_4 = -1 \) or \( d \equiv 1 \text{ mod } 16 \) with

\[
(\frac{2q_1}{q_1})_4 (\frac{2q_1}{q_2})_4 = 1.
\]

(iv) It is clear from the process of proving (iii).

Let \( F = \mathbb{Q}(\sqrt{-p_1p_2}) \) be an imaginary quadratic field with \( p_1 \equiv p_2 \equiv 1 \text{ mod } 4 \). By Rédei’s criterion, we have that \( r_4(C(F)) = 1 \) if and only if one of the following four conditions holds:

\[
R'_F X = \left( \begin{array}{c} (\frac{a}{p_1})' \\ \vdots \\ (\frac{c}{p_{r-1}})'
\end{array} \right)
\]
Theorem 3.6. Suppose \( p_1 \equiv 1 \mod 8 \) and \( (\frac{p_1}{p_2}) = 1 \);
(2) \( p_1 \equiv p_2 \equiv 5 \mod 8 \) and \( (\frac{p_1}{p_2}) = 1 \);
(3) \( p_1 \equiv p_2 \equiv 5 \mod 8 \) and \( (\frac{p_1}{p_2}) = -1 \);
(4) \( p_1 \equiv p_2 \equiv 1 \mod 8 \) and \( (\frac{p_1}{p_2}) = -1 \).

By Theorem 3.3 and Lemma 2.3, we have proved:

Corollary 3.4. Let \( F = \mathbb{Q}(\sqrt{-p_1 p_2}) \) be an imaginary quadratic field.
(i) Suppose \( p_1 \equiv 1 \mod 8 \), \( p_2 \equiv 5 \mod 8 \) and \( (\frac{p_1}{p_2}) = 1 \). Then \( r_8(C(F)) = 1 \)
if and only if \( (\frac{p_1}{p_2})_4 = 1 \).
(ii) Suppose \( p_1 \equiv p_2 \equiv 5 \mod 8 \) and \( (\frac{p_1}{p_2}) = 1 \). Then \( r_8(C(F)) = 1 \)
if and only if \( (\frac{p_1}{p_2})_4 = -1 \) if and only if \( (\frac{p_1}{p_2})_4 = 1 \), where \( \lambda_1 \) and \( \lambda_2 \) are defined as Lemma 2.3.
(iii) Suppose \( p_1 \equiv p_2 \equiv 5 \mod 8 \) and \( (\frac{p_1}{p_2}) = -1 \). Then \( r_8(C(F)) = 1 \)
if and only if either \( p_1 p_2 \equiv 9 \mod 16 \) and \( (\frac{p_1 p_2}{p_1})_4 = 1 \) or \( p_1 p_2 \equiv 1 \mod 16 \) and \( (\frac{p_1 p_2}{p_1})_4 = 1 \) if and only if \( (\frac{p_1}{p_2})_4 = 1 \), where \( \lambda_1 \) and \( \lambda_2 \) are defined as Lemma 2.3.
(iv) Suppose \( p_1 \equiv p_2 \equiv 1 \mod 8 \) and \( (\frac{p_1}{p_2}) = -1 \). Then \( r_8(C(F)) = 1 \)
if and only if either \( p_1, p_2 \in A^+ \) or \( p_1, p_2 \in A^- \) if and only if \( (\frac{\sqrt{-7}}{p_1 p_2}) = 1 \), where \( p_1 \) and \( p_2 \) are defined as in \( \S 2 \).

Example 3.5. In Corollary 3.4, let \( F = \mathbb{Q}(\sqrt{-p_1 p_2}) \) with distinct primes \( p_1 \equiv p_2 \equiv 1 \mod 4 \). Let \( C(F)_2 \) denote the 2-primary subgroup of \( C(F) \).
(i) For \( p_1 = 17 \) and \( p_2 = 13 \), \( (\frac{17}{13}) = 1 \), \( 3^4 = 13 + 17 \cdot 4 \), \( (\frac{13}{17})_4 = 1 \), so \( r_8(C(F)) = 1 \) by Theorem 3.3(i). In fact, \( C(F)_2 \cong \mathbb{Z}/(8) \oplus \mathbb{Z}/(2) \) by Pari-GP.
(ii) For \( p_1 = 13 \) and \( p_2 = 29 \), \( (\frac{13}{29}) = 1 \), \( 13 = 3^2 + 2^2 \), \( 29 = 5^2 + 2^2 \), \( (\frac{13}{29})_4 = -1 \) by quartic reciprocity, so \( r_8(C(F)) = 1 \) by Theorem 3.3(ii). In fact, \( C(F)_2 \cong \mathbb{Z}/(8) \oplus \mathbb{Z}/(2) \) by Pari-GP.
(iii) For \( p_1 = 13 \) and \( p_2 = 37 \), \( (\frac{13}{37}) = -1 \), \( p_1 \cdot p_2 \equiv 1 \mod 16 \), \( 2 \cdot 37 = 4^2 - 14 \cdot 37 \), \( 2 \cdot 37 = 11^2 - 395 \cdot 37 \), \( (\frac{2}{11})_4 = (\frac{2}{37})_4 = 1 \), so \( r_8(C(F)) = 1 \) by Theorem 3.3(iii). In fact, \( C(F)_2 \cong \mathbb{Z}/(8) \oplus \mathbb{Z}/(2) \) by Pari-GP.
(iv) For \( p_1 = 17 \) and \( p_2 = 73 \), \( p_1, p_2 \in A^- \), \( r_8(C(F)) = 1 \) by Theorem 3.3(iv). In fact, \( C(F)_2 \cong \mathbb{Z}/(16) \oplus \mathbb{Z}/(2) \) by Pari-GP.

In Proposition 3.1, we know that \( r_4(C(F)) = 2 \) if and only if one of the following conditions holds:
(1) \( \text{rank } R_F = \text{rank } R_E + t - 3 \) and \( D(F) = (q_1) \times (2q_1') \times (d) \), where \( q_1 = p_1 \cdots p_r \equiv 1 \mod 8 \) \( (1 \leq r < t - 1) \) and \( q_1' | d \).
(2) \( \text{rank } R_F = \text{rank } R_E + t - 3 \) and \( D(F) = D(E) = (q_1) \times (q_2) \times (q_3) \), where \( q_1 = p_1 \cdots p_r, q_2 = p_{r+1} \cdots p_s \text{ and } q_3 = p_{s+1} \cdots p_{t-1} \).

Theorem 3.6. Let \( F = \mathbb{Q}(\sqrt{-d}) \), where \( d = p_1 \cdots p_{t-1} \) and distinct primes \( p_i \equiv 1 \mod 8 \), be an imaginary quadratic field. Let \( \text{rank } R_F = t - 3 \) and \( D(F) = (q_1) \times (2) \times (d) \), where \( q_1 = p_1 \cdots p_{r} \) \( (1 \leq r < t - 1) \).
(i) Let \( q_1^2 = q_1 \mathcal{O}_F \). Then \([q_1] \in C(F)^4\) if and only if \((\frac{q_1}{q_1})_4 = (\frac{q_1}{q_1})_4 = 1\).

(ii) Let \( p_i = u_i^2 - 2w_i^2 \equiv 1 \mod 8 \) and \( \pi_i = u_i + w_i \sqrt{2} \) for \( 1 \leq i \leq t - 1 \). Let \( \pi_1^t = \prod_{i=1}^{t} \pi_i = u_1' + w_1' \sqrt{2}, \pi_2^t = \prod_{i=r+1}^{t} \pi_i = u_2' + w_2' \sqrt{2} \) and \( t^2 = 2 \mathcal{O}_F \). Then \([t] \in C(F)^4\) if and only if \((\frac{1-x^2}{\pi_1}) = (\frac{1-x^2}{\pi_2}) = (\frac{x}{\pi_2})\) if and only if both \( p_1, \ldots, p_r \) and \( p_{r+1}, \ldots, p_{t-1} \) belonging to \( A^- \) are two even numbers and \((\frac{z}{\pi_2}) = 1\) or both \( p_1, \ldots, p_r \) and \( p_{r+1}, \ldots, p_{t-1} \) belonging to \( A^- \) are two odd numbers and \((\frac{z}{\pi_2}) = -1\). Moreover, \( r_{s}(C(F)) = 2 \) if and only if \([q_1], [t] \in C(F)^4\) if and only if \((\frac{q_1}{q_1})_4 = (\frac{q_1}{q_1})_4 = 1\).

Proof. (i) Suppose rank \( R_F = t - 3 \) and \( D(F) = (q_1) \times (2) \times (d) \), where \( q_1 = p_1 \cdots p_r \) ( \( 1 \leq r < t - 1 \)). Then the two sums of both the first \( r \) row vectors and the first \( t - 1 \) row vectors of \( R_F \) are equal to zero. Let \( z^2 = q_1 x^2 + q_2 y^2, q_2 = d/q_1 \), have a non-trivial solution \((x, y, z) = (a, b, c) \mod 2 \). Then \( 1 \neq [q_1] = [c]^2 \in C(F)^2 \), where \( q_1^2 = q_1 \mathcal{O}_F \) and \( \mathcal{O} \) is an ideal of \( F \) over \( \mathcal{O} \). Since \( c^2 = q_1 a^2 + q_2 b^2 \) and \( q_1 \equiv q_2 \equiv 1 \mod 8 \), the Jacobi symbols \( (\frac{c}{q_1}) = (\frac{c}{q_2}) = 1 \) and \( (\frac{c}{q_1}) = (\frac{q_2}{q_1})_4 \). We conclude that \([q_1] \in C(F)^4 \leftrightarrow [c][m] \in C(F)^2 \), where \( m \) is an ambiguous ideal of \( F \) over \( m|2d \leftrightarrow mcez^2 = x^2 + dy^2 \) is solvable over \( \mathbb{Z} \leftrightarrow \) the following system of equations is solvable over \( \mathbb{F}_2 \)

\[
R_F X = \begin{pmatrix} (\frac{c}{q_1}) \vdots (\frac{c}{q_2}) \end{pmatrix}
\]

\( \leftrightarrow (\frac{c}{q_1}) = (\frac{q_1}{q_2})_4 = 1 \) and \((\frac{c}{q_2}) = (\frac{q_1}{q_2})_4 = 1\).

(ii) Since \( q_1 q_2 = N_{L/Q}(\pi_i \pi_2) = u^2 - 2w^2 = 2(u + w)^2 - (u + 2w)^2 \), where \( u = u_1' u_2' + 2w_1' w_2' \) and \( w = u_1' w_2' + u_2' w_1' \), we have \([t] = [p_{u+w}]^2 \in C(F)^2\), where \( p_{u+w} \) is an ideal of \( F \) over \( u + w \). For each \( p_i \) \( 1 \leq i \leq r \), \( \mathcal{O}_L/(\pi_i) \cong \mathbb{Z}/(p_i) \) and \((\frac{u+w}{p_i}) = (\frac{u+w}{p_i}) \). On the other hand,

\[
\begin{align*}
u + w &= u_1' u_2' + 2w_1' w_2' + u_1' w_2' + u_2' w_1' \\ &\equiv w_1' u_2' \sqrt{2} + 2w_1' w_2' - w_1' w_2' \sqrt{2} + u_2' w_1' \\ &\equiv w_1'(1 - \sqrt{2})(u_2' - u_2' \sqrt{2}) \mod \pi_i,
\end{align*}
\]

so

\[
(\frac{u+w}{p_i}) = (\frac{u+w}{p_i}) (\frac{1-\sqrt{2}}{\pi_i}) (\frac{\pi_i}{\pi_i}), \ 1 \leq i \leq r.
\]
Similarly, we get:
\[
\left(\frac{u+w}{p_j}\right) = \left(\frac{u+w'}{p_j}\right) \left(\frac{1-\sqrt{2}}{\pi_j}\right)^r, \quad r + 1 \leq j \leq t - 1.
\]
Since \(q_1 = u_1^2 - 2u_1', \left(\frac{u_1'w}{q_1}\right) = 1\), similarly, \(\left(\frac{w_1^j}{q_2}\right) = \left(\frac{w_1'^{j}}{q_2}\right) = 1\). Note the fact that \(p_1 \in A^+\) if and only if \(\left(\frac{1-\sqrt{2}}{\pi_1}\right) = 1\). By reciprocity law, we know that \(\left(\frac{t}{\pi_1}\right) = \left(\frac{t}{q_1}\right)\). Since rank \(R_F = t - 2\) and \(p_1 \equiv 1 \mod 8\), we conclude that \([t] \in C(F)^4 \iff\) the following system of equations is solvable over \(\mathbb{F}_2\):
\[
R'_F X = \begin{pmatrix}
\left(\frac{u+w}{p_1}\right) \\
\vdots \\
\left(\frac{u+w}{p_{t-1}}\right)
\end{pmatrix}
\]
\(\iff \left(\frac{u+w}{q_1}\right) = 1 \text{ and } \left(\frac{u+w}{q_2}\right) = 1 \iff\) either both \(p_1, \ldots, p_r\) and \(p_{r+1}, \ldots, p_{t-1}\) belonging to \(A^+\) are two even numbers and \(\left(\frac{t}{\pi_1}\right) = 1\) or both \(p_1, \ldots, p_r\) and \(p_{r+1}, \ldots, p_{t-1}\) belonging to \(A^-\) are two odd numbers and \(\left(\frac{t}{\pi_1}\right) = -1\). □

Let \(F = \mathbb{Q}(\sqrt{-p_1p_2})\) be an imaginary quadratic field with \(p_1 \equiv p_2 \equiv 1 \mod 4\). By Rédei’s criterion, we have that \(r_4(C(F)) = 2\) if and only if \(p_1 \equiv p_2 \equiv 1 \mod 8\) and \(\left(\frac{p_1}{p_2}\right) = 1\). By Theorem 3.6 and Lemma 2.2, we have proved:

**Corollary 3.7.** Let \(F = \mathbb{Q}(\sqrt{-p_1p_2})\) be an imaginary quadratic field with primes \(p_1 \equiv p_2 \equiv 1 \mod 8\) and \(\left(\frac{p_1}{p_2}\right) = 1\). Let \(p_2^2 = p_1\mathcal{O}_F\) and \(t^2 = 2\mathcal{O}_F\). Then

(i) \([p_1] \in C(F)^4\) if and only if \(\left(\frac{p_1}{p_2}\right)_4 = \left(\frac{p_1}{p_1}\right)_4 = 1\).

(ii) \([t] \in C(F)^4\) if and only if \(\left(\frac{p_1}{p_2}\right)_4 = \left(\frac{1-\sqrt{2}}{\pi_2}\right) = \left(\frac{1-\sqrt{2}}{\pi_2}\right)\) if and only if either \(p_1, p_2 \in A^+\) and \(\left(\frac{t}{\pi_1}\right) = -1\) if and only if either \(p_1, p_2 \in A^-\) and \(\left(\frac{t}{\pi_1}\right) = 1\) for some \(x, y \in \mathbb{Z}\) or \(p_1, p_2 \in A^+\) and \(\left(\frac{t}{\pi_1}\right) = -1\) if and only if either \(p_1, p_2 \in A^-\) and \(\left(\frac{t}{\pi_1}\right) = 1\) for some \(x, y \in \mathbb{Z}\), where \(\pi_1\) and \(\pi_2\) are defined as in §2. Moreover, \(r_4(C(F)) = 2\) if and only if \([p_1], [t] \in C(F)^4\) if and only if \(\left(\frac{p_1}{p_2}\right)_4 = \left(\frac{p_1}{p_1}\right)_4 = 1\) and \(\left(\frac{t}{\pi_1}\right) = \left(\frac{1-\sqrt{2}}{\pi_2}\right) = \left(\frac{1-\sqrt{2}}{\pi_2}\right)\).

We now turn to another imaginary quadratic fields \(F = \mathbb{Q}(\sqrt{-2d})\) with \(d = p_1 \cdots p_{t-1}\) and distinct primes \(p_i \equiv 1 \mod 4\). We know that \(r_4(C(F)) = t - 1\) by genus theory and the Rédei’s matrix \(R_F\) is a symmetric matrix. We have that \(r_4(C(F)) = 1\) if and only if rank \(R_F = t - 2\) and \(D^*(F) = \{1, q_1, 2q_2, 2d\}\), where \(q_1 = p_1 \cdots p_r\) and \(q_2 = p_{r+1} \cdots p_{t-1}\).

**Theorem 3.8.** Let \(F = \mathbb{Q}(\sqrt{-2d})\) be an imaginary quadratic field with \(d = p_1 \cdots p_{t-1}\) and distinct primes \(p_i \equiv 1 \mod 4\). Let rank \(R_F = t - 2\) and \(D^*(F) = \{1, q_1, 2q_2, 2d\}\).
Suppose \( q_1 = p_1 \cdots p_r \equiv 1 \mod 8 \), \( q_2 = p_{r+1} \cdots p_{r+1} - 1 \) and \( 1 \leq r < t - 1 \). Then \( r_8(C(F)) = 1 \) if and only if \( \left( \frac{2q_1}{q_1} \right)_4 = 1 \).

(ii) Suppose \( p_i \equiv 1 \mod 8 \) for \( 1 \leq i \leq t - 1 \), that is, \( q_1 = d \) and \( q_2 = 1 \). Then \( r_8(C(F)) = 1 \) if and only if an even number of the primes \( p_1, \ldots, p_{t-1} \) belong to \( B^- \).

Proof. (i) Suppose rank \( R_F = t - 2 \) and \( q_1 = p_1 \cdots p_r \in D(F) \). Then the sum of the first \( r \) rows of the \( t \times t \) matrix is equal to zero. Let \( z^2 = q_1 x^2 + 2q_2 y^2 \) have a relatively prime solution \((x, y, z) = (a, b, c)\) over \( \mathbb{N} \). Then \( [q_1] = [p_1]^2 \in C(F)^2 \), where \( q_1^2 = q_1 O_F \) and \( p_1 \) is an ideal of \( F \) over \( c \). Since \( c^2 = q_1 a^2 + 2q_2 b^2 \) and \( q_1 \equiv 1 \mod 8 \), we have that \( \left( \frac{2q_1}{q_1} \right)_4 = 1 \). Similarly, we conclude that
\[
 r_8(C(F)) = 1 \Leftrightarrow [q_1] \in C(F)^4 \Leftrightarrow \left( \frac{c}{q_1} \right)_4 = \left( \frac{2q_2}{q_1} \right)_4 = 1.
\]

(ii) Let \( t^2 = 2O_F \). Then by the process of proving (i), we conclude that \( r_8(C(F)) = 1 \Leftrightarrow [t] \in C(F)^4 \Leftrightarrow \left( \frac{2}{p_{t-1}} \right)_4 = 1 \Leftrightarrow \) \( r_8(C(F)) = 1 \) if and only if one of the following conditions holds:

1. \( p_1 \equiv p_2 + 4 \equiv 1 \mod 8 \) and \( \left( \frac{p_1}{p_2} \right)_4 = 1 \);
2. \( p_1 \equiv p_2 \equiv 1 \mod 8 \) and \( \left( \frac{p_1}{p_2} \right)_4 = -1 \).

By Theorem 3.8, we get:

**Corollary 3.9.** Let \( F = \mathbb{Q}(\sqrt{2p_1p_2}) \) be an imaginary quadratic field.

(i) Suppose \( p_1 \equiv p_2 + 4 \equiv 1 \mod 8 \) and \( \left( \frac{p_1}{p_2} \right)_4 = 1 \). Then \( r_8(C(F)) = 1 \) if and only if \( \left( \frac{2}{p_1} \right)_4 = 1 \).

(ii) Suppose \( p_1 \equiv p_2 \equiv 1 \mod 8 \) and \( \left( \frac{p_1}{p_2} \right)_4 = -1 \). Then \( r_8(C(F)) = 1 \) if and only if \( \left( \frac{2}{p_1p_2} \right)_4 = 1 \) if and only if either \( p_1, p_2 \in B^+ \) or \( p_1, p_2 \in B^- \).

**Example 3.10.** In Corollary 3.9, let \( F = \mathbb{Q}(\sqrt{-2p_1p_2}) \) with distinct primes \( p_1 \equiv p_2 \equiv 1 \mod 4 \). Let \( C(F)_2 \) denote the 2-primary subgroup of \( C(F) \).

(i) For \( p_1 = 17 \) and \( p_2 = 53 \), \( \left( \frac{p_1}{p_2} \right)_4 = \left( \frac{17}{53} \right)_4 = 1 \), \( \left( \frac{2}{p_1} \right)_4 = \left( \frac{2}{53} \right)_4 = \left( \frac{2}{17} \right)_4 = 1 \), so \( r_8(C(F)) = 1 \) by Corollary 3.9(i). In fact, \( C(F)_2 \cong \mathbb{Z}/(16) \oplus \mathbb{Z}/(2) \) by Pari-GP.

(ii) For \( p_1 = 17 \) and \( p_2 = 97 \), \( \left( \frac{p_1}{p_2} \right)_4 = \left( \frac{17}{97} \right)_4 = -1 \) and \( 17, 97 \in B^- \), so \( r_8(C(F)) = 1 \) by Corollary 3.9(ii). In fact, \( C(F)_2 \cong \mathbb{Z}/(8) \oplus \mathbb{Z}/(2) \) by Pari-GP.

Let \( F = \mathbb{Q}(\sqrt{-2d}) \) be an imaginary quadratic field with \( d = p_1 \cdots p_{t-1} \) and distinct primes \( p_i \equiv 1 \mod 8 \). Then the Rédei’s matrix is
\[
R_F = \begin{pmatrix}
M & 0 \\
0 & 0
\end{pmatrix},
\]
where the \((t-1) \times (t-1)\) matrix \(M\) is equal to the Rédei’s matrix \(R_E\) of \(E = \mathbb{Q}(\sqrt{d})\). Let \(p_i = u_i^2 - 2w_i^2\) and \(\pi_i = u_i + w_i\sqrt{2}\) for \(1 \leq i \leq t - 1\).

**Theorem 3.11.** Let \(F = \mathbb{Q}(\sqrt{-2d})\) be an imaginary quadratic field with \(d = p_1 \cdots p_{t-1}\) and distinct primes \(p_i \equiv 1 \mod 8\). Suppose rank \(R_F = t - 3\), that is, \(D(F) = (2) \times (q_1) \times (2d)\), where \(q_1 = p_1 \cdots p_r\) and \(q_2 = p_{r+1} \cdots p_{t-1}\). Let \(q_1^2 = q_1 \mathcal{O}_F, q_2^2 = 2 \mathcal{O}_F, \pi_1' = \prod_{i=1}^{t-1} \pi_i = u_1 + w_1\sqrt{2}\) and \(\pi_2' = \prod_{i=r+1}^{t-1} \pi_i = u_2 + w_2\sqrt{2}\).

Then we have

(i) \([t] \in C(F)^4\) if and only if \((\frac{u_2}{q_1'})^4 = (\frac{u_1}{q_2'})^4\) if and only if either both \(p_1, \ldots, p_r\) and \(p_{r+1}, \ldots, p_{t-1}\) belonging to \(B^\prime\) are two even numbers and \((\frac{u_2}{q_1'})^r = 1\) or both \(p_1, \ldots, p_r\) and \(p_{r+1}, \ldots, p_{t-1}\) belonging to \(B^\prime\) are two odd numbers and \((\frac{u_1}{q_2'})^r = -1\).

(ii) \([q_1] \in C(F)^4\) if and only if \((\frac{2q_1}{q_1})^4 = (\frac{q_1}{q_2})^4(\frac{q_1}{q_2})^2 = 1\).

**Proof.** (i) By the assumption, we know that the two sums of both the first \(r\) row vectors and the first \(t - 1\) row vectors of \(R_F\) are equal to zero. Since \(d = q_1q_2 = u^2 - 2w^2\), where \(u = u_1'u_2' + 2u_1'u_2'\) and \(w = u_1'w_2' + u_2'w_1'\), \(2u^2 = 4u^2 + 2d\) and \([t] = [p_u]^2 \in C(F)^2\), where \(p_u\) is an ideal of \(F\) over \(u\).

Similarly, we conclude that

\[ [t] \in C(F)^4 \iff \left(\frac{u}{q_1}\right) = \left(\frac{u}{q_2}\right) = 1. \]

On the other hand, for each \(p_i\) (1 \leq i \leq r), \(\mathcal{O}_F/(\pi_i) \cong \mathbb{Z}/(p_i), u = u_1'u_2' + 2u_1'u_2' \equiv u_1'(u_2' - w_2'\sqrt{2})\) mod \((\pi_i)\) and \((\frac{\pi_i}{u_1'}) = \left(\frac{u_1'}{p_i}\right)\) since \((\frac{u_2'}{\pi_i}) = (\frac{u_2'}{\pi_i}) = 1\). Then

\[ \left(\frac{u}{p_i}\right) = \left(\frac{u_1}{\pi_i}\right) = \left(\frac{u_1}{\pi_i}\right) \left(\frac{\pi_i}{u_1}\right) = \left(\frac{u_1}{p_i}\right) \left(\frac{\pi_i}{u_1}\right). \]

Similarly, for each \(p_j\) (r + 1 \leq j \leq t - 1),

\[ \left(\frac{u}{p_j}\right) = \left(\frac{u_2}{\pi_j}\right) = \left(\frac{u_2}{\pi_j}\right) \left(\frac{\pi_j}{u_2}\right) = \left(\frac{u_2}{p_j}\right) \left(\frac{\pi_j}{u_2}\right). \]

Since \(q_1 = u_1'^2 - 2w_1'^2\), we have that \((\frac{u_1'}{q_1})^4 = 1\) and \((\frac{u_1'}{q_1})^4 = (\frac{u_1'}{q_1})^2\). Hence we conclude that \([t] \in C(F)^4 \iff (\frac{u_2}{q_1'})^4 = (\frac{u_1}{q_2'})^4 \iff\) either both \(p_1, \ldots, p_r\) and \(p_{r+1}, \ldots, p_{t-1}\) belonging to \(B^\prime\) are two even numbers and \((\frac{u_2}{q_1'})^r = 1\) or both \(p_1, \ldots, p_r\) and \(p_{r+1}, \ldots, p_{t-1}\) belonging to \(B^\prime\) are two odd numbers and \((\frac{u_1}{q_2'})^r = -1\).

(ii) Let \(z^2 = q_1x^2 + 2q_2y^2\), where \(q_1 = p_1 \cdots p_r\) and \(q_2 = d/q_1\), have a relatively prime solution \((x, y, z) = (a, b, c)\) over \(\mathbb{N}\). Then \([q_1] = [p_c]^2 \in C(F)^2\), where \(q_1^2 = q_1 \mathcal{O}_F\) and \(p_c\) is an ideal of \(F\) over \(c\). Since \(c^2 = q_1a^2 + 2q_2b^2\), we
have that \((\frac{b}{q_1}) = 1\) and \((\frac{c}{q_2}) = (\frac{2d}{q_1} + 1)\). Similarly, we have that \([q_1] \in C(F) \iff (\frac{c}{q_2}) = (\frac{3}{q_2})\). We need to determine the value of the Jacobi symbol \((\frac{a}{q_1})\). Let \(2u^2 = 4w^2 + 2d\) and \(q_1u^2 = (q_1a)^2 + 2db^2\). Then \(2q_1u^2c^2 = \mathbb{N}_{F/\mathbb{Q}}(q_1a + b\sqrt{-2d})\mathbb{N}_{F/\mathbb{Q}}(2w + \sqrt{-2d})\), i.e.,

\[
2q_1u^2c^2 = 4q_1(aw - q_2b)^2 + 2d(q_1a + 2bw)^2.
\]

We can choose a solution \((x, y, z) = (a, b, c)\) of the equation \(z^2 = q_1x^2 + 2q_2y^2\) such that the greatest common divisor \((uc, aw - q_2b) = 1\). In fact, in \(F = \mathbb{Q}(\sqrt{-2d})\), let \(tp_1^2 = (2w + \sqrt{-2d})\mathcal{O}_F\), where \(t\) is the dyadic ideal of \(F\) and \(p_i\) is an ideal of \(F\) over \(u\). Since \([q_1] \in C(F)^2\), there is an ideal \(p_i\) of \(F\) over positive integer number \(c\) such that \([q_1][p_i]^2 = 1\) and \(p_c = \mathcal{O}_F = p_a + p_c\), where \(p_c\) is the conjugate ideal of \(p_a\). Hence \(q_1p_2^2 = (a + b\sqrt{-2d})\mathcal{O}_F\) and we get such \((x, y, z) = (a, b, c)\) satisfying \((uc, aw - q_2b) = 1\).

By (3.2), we have the Jacobi symbol \((\frac{aw - q_2b}{q_2}) = (\frac{aw}{q_2}) = \frac{(w_q)}{q_2}\).

On the other hand,

\[
q_1q_2 = \mathbb{N}_{L/\mathbb{Q}}(u_1' + w_1\sqrt{2})\mathbb{N}_{L/\mathbb{Q}}(u_2' + w_2'\sqrt{2}) = (u_1'w_2' + 2u_1'w_2')^2 - 2(u_1'w_2' + u_2'w_1')^2 = u^2 - 2w^2
\]

where \(u = u_1'u_2' + 2u_1'w_2'\) and \(w = u_1'w_2' + u_2'w_1'\). For each \(p_j (r + 1 \leq j \leq t - 1)\), \(\mathcal{O}_L/(\pi_j) \cong \mathbb{Z}/(p_j)\), \(w = u_1'w_2' + u_2'w_1' \equiv \frac{u_2'(u_1' - w_1\sqrt{2})}{\pi_j}\). Hence

\[
\left(\frac{w}{\pi_j}\right) = \left(\frac{u_2'}{\pi_j}\right) = \left(\frac{u_1' - u_1'\sqrt{2}}{\pi_j}\right) = \left(\frac{u_2'}{p_j}\right)
\]

Since \(q_2 = u_2^2 - 2u_2'^2\), the Jacobi symbol \((\frac{u_2'}{q_2}) = 1\); by \((\frac{u_2}{q_2}) = 1\), \((\frac{u_2'}{\pi_j}) = (\frac{u_1' - u_1'\sqrt{2}}{\pi_j})\). Hence \((\frac{w}{q_2}) = (\frac{w}{q_2}) = (\frac{u_2'}{q_2})\).

As a conclusion, we get that

\[
[q_1] \in C(F)^4 \iff \frac{2q_2}{q_1} = \frac{q_1}{q_2} \iff (\frac{u_2'}{q_2}) = 1.
\]

Let \(F = \mathbb{Q}(\sqrt{-2p_1p_2})\) be an imaginary quadratic field with distinct primes \(p_1, p_2 \equiv 1 \mod 4\). By Rédei’s criterion, we have that \(r_4(C(F)) = 2\) if and only if \(p_1 \equiv p_2 \equiv 1 \mod 8\) and \((\frac{p_1}{p_2}) = 1\). By Theorem 3.11 and Lemma 2.2, we get:

**Corollary 3.12.** Let \(F = \mathbb{Q}(\sqrt{-2p_1p_2})\) be an imaginary quadratic field with distinct primes \(p_1, p_2 \equiv 1 \mod 8\) and \((\frac{p_1}{p_2}) = 1\). Let \(t^2 = 2\mathcal{O}_F\) and \(p_1^2 = p_1\mathcal{O}_F\). Then

(i) \([t] \in C(F)^4\) if and only if \(\left(\frac{p_1}{p_2}\right) = \left(\frac{p_2}{p_1}\right) = 1\).

(ii) if either \(p_1, p_2 \in B^+\), \(p_2^{h_b(2p_1)/4} = x^2 - 2p_1y^2\) over \(\mathbb{Z}\) or \(p_1, p_2 \in B^-\), \(\pm p_2^{h_b(2p_1)/4} = 2x^2 - p_1y^2\) over \(\mathbb{Z}\).
Let \( F \) be an elliptic curve in \( C(F)^4 \) if and only if \((\frac{2a}{p^4}) = (\frac{2a}{p^4}) \cdot (\frac{a}{p^4}) = 1 \). Moreover, \( r_s(C(F)) = 2 \) if and only if \((\frac{2a}{p^4}) = (\frac{2a}{p^4}) = (\frac{a}{p^4}) = (\frac{a}{p^4}) \).

**Example 3.13.** Let \( F = \mathbb{Q}(\sqrt{-241}) \), \((\frac{241}{q}) = 1 \). Then \( C(F)_2 \cong \mathbb{Z}/(8) \oplus \mathbb{Z}/(8) \) by PARI-GP. We also verify the condition of Corollary 3.12. It is clear that \( 41 = 3^2 + 32, 41 \in A^+ \), \( 41, 241 \in B^- \) and \((\frac{241}{41}) = (\frac{3}{41}) = (\frac{2}{41}) = -1 \).

In terms of norm from \( \mathbb{Q}(\sqrt{-1}) \), \( 41 = 5^2 + 4^2, 241 = 15^2 + 2^2 \), \((\frac{241}{41}) = (\frac{15}{41}) = (\frac{15}{41}) = (\frac{1}{41}) = -1 \). By 41 = 13^2 - 2 \cdot 8^2, 241 = 29^2 - 2 \cdot 20^2, let \( p_1 = 13 - 8\sqrt{2} \) and \( p_2 = 29 - 20\sqrt{2} \), then \((\frac{2a}{p_1}) = (\frac{2a}{p_2}) = (-\frac{241}{41}) = -1 \). Hence, the 8-rank of \( C(F) \) is equal to 2 by Corollary 3.12.

**4. Densities**

In the section, we use a Gerth’s method (see [4, 5, 6, 16]) to investigate the densities of 8-rank of \( C(F) \) equal to 1 or 2 in all quadratic number fields \( F = \mathbb{Q}(\sqrt{-p_1p_2}) \), where \( p_1 \equiv p_2 \equiv 1 \) mod 4. For a positive real number \( x \), let

\[
A_x = \{ p_1p_2 : \text{distinct primes } p_1 \equiv p_2 \equiv 1 \text{ mod } 4, p_1 < p_2 \text{ and } p_1p_2 \leq x \},
\]

\[
A_{1,x} = \{ F = \mathbb{Q}(\sqrt{-p_1p_2}) : r_4(C(F)) = r_s(C(F)) = 1 \text{ and } p_1p_2 \in A_x \},
\]

\[
A_{2,x} = \{ F = \mathbb{Q}(\sqrt{-p_1p_2}) : r_4(C(F)) = r_s(C(F)) = 2 \text{ and } p_1p_2 \in A_x \},
\]

\[
A_{3,x} = \{ F = \mathbb{Q}(\sqrt{-2p_1p_2}) : r_4(C(F)) = r_s(C(F)) = 1 \text{ and } p_1p_2 \in A_x \},
\]

\[
A_{4,x} = \{ F = \mathbb{Q}(\sqrt{-2p_1p_2}) : r_4(C(F)) = r_s(C(F)) = 2 \text{ and } p_1p_2 \in A_x \}.
\]

We define densities \( d_i \) \((1 \leq i \leq 4) \) as follows:

\[
d_i = \lim_{x \to \infty} \frac{|A_{i,x}|}{|A_x|}.
\]

**Theorem 4.1.** Let \( d_1, d_2, d_3 \) and \( d_4 \) be defined as (4.1). Then

\[
d_1 = \frac{5}{16}, d_2 = \frac{1}{128}, d_3 = \frac{3}{16}, d_4 = \frac{1}{128}.
\]

**Proof.** We know that, by ([7, Theorem 437]) and \( p_1 \equiv p_2 \equiv 1 \) mod 4, \( p_1 < p_2 \),

\[
|A_x| = \sum_{p_1,p_2 \in A_x} 1 = \frac{x \log \log x}{4 \log x} + o\left(\frac{x \log \log x}{\log x}\right).
\]

Let \( F = \mathbb{Q}(\sqrt{-p_1p_2}) \in A_{1,x} \). Then by Corollary 3.4, we have that \( r_4(C(F)) = r_s(C(F)) = 1 \) if and only if one of the following five conditions holds:

1. \( p_1 \equiv p_2 + 4 \equiv 1 \text{ mod } 8, (\frac{2}{p_1}) = 1 \text{ and } (\frac{2}{p_2}) = 1 \);
2. \( p_1 + 4 \equiv p_2 \equiv 1 \text{ mod } 8, (\frac{2}{p_1}) = 1 \text{ and } (\frac{2}{p_2}) = 1 \);
3. \( p_1 \equiv p_2 \equiv 5 \text{ mod } 8, (\frac{2}{p_1}) = 1 \text{ and } (\frac{2}{p_2}) = 1 \), where \( \lambda_1, \lambda_2 \) are defined as Lemma 2.3.
8-RANKS OF CLASS GROUPS OF IMAGINARY QUADRATIC NUMBER FIELDS 1265

(4) \( p_1 \equiv p_2 \equiv 5 \mod 8 \), \( \left( \frac{p_2}{p_1} \right) = -1 \) and \( \left( \frac{\lambda_2}{\lambda_1} \right) = 1 \), where \( \lambda_1, \lambda_2 \) are defined as Lemma 2.3;

(5) \( p_1 \equiv p_2 \equiv 1 \mod 8 \), \( \left( \frac{p_2}{p_1} \right) = -1 \) and \( \left( \frac{1-\sqrt{2}}{\pi_1 \pi_2} \right) = 1 \), where \( \pi_1, \pi_2 \) are defined as §2.

Hence

\[
|A_{1,x}(F)| = \sum_{\substack{p_1, p_2 \in A_x \\ p_1 \equiv p_2 \equiv 3 \mod 8}} \frac{1}{4} \left( 1 + \left( \frac{p_2}{p_1} \right) \right) \left( 1 + \left( \frac{p_2}{p_1} \right) \right)
\]

\[
+ \sum_{\substack{p_1, p_2 \in A_x \\ p_1 + 4p_2 \equiv 1 \mod 8}} \frac{1}{4} \left( 1 + \left( \frac{p_2}{p_1} \right) \right) \left( 1 + \left( \frac{p_2}{p_1} \right) \right)
\]

\[
+ \sum_{\substack{p_1, p_2 \in A_x \\ p_1 \equiv p_2 \equiv 5 \mod 8}} \frac{1}{4} \left( 1 + \left( \frac{p_2}{p_1} \right) \right) \left( 1 + \left( \frac{\lambda_2}{\lambda_1} \right) \right)
\]

\[
+ \sum_{\substack{p_1, p_2 \in A_x \\ p_1 \equiv p_2 \equiv 5 \mod 8}} \frac{1}{4} \left( 1 - \left( \frac{p_2}{p_1} \right) \right) \left( 1 + \left( \frac{\lambda_2}{\lambda_1} \right) \right)
\]

\[
= \sum_{p \equiv 1 \mod 8} \left( \frac{1}{16} + \frac{1}{16} + \frac{1}{16} + \frac{1}{16} \right) + o \left( \frac{x \log \log x}{\log x} \right)
\]

\[
= \frac{5}{64} x \log \log x + o \left( \frac{x \log \log x}{\log x} \right).
\]

An intuitive explanation of the formula might proceed as follows. In the second equation, a factor of \( \frac{1}{4} \) is introduced by each congruence relation of \( p_1, p_2 \mod 8 \). This is considered in detail in [4, 6].

For the sake of completeness, we give a sketch of proof.

\[
\sum_{\substack{p_1, p_2 \in A_x \\ p_1 \equiv p_2 \equiv 3 \mod 8}} \frac{1}{4} \left( 1 + \left( \frac{p_2}{p_1} \right) \right) \left( 1 + \left( \frac{p_2}{p_1} \right) \right)
\]

\[
= \frac{1}{16} \sum_{p_1, p_2 \in A_x} 1 + O \left( \sum_{\substack{p_1, p_2 \in A_x \\ p_1 + 4p_2 \equiv 1 \mod 8}} \left( \chi_1(p_2) + \chi_2(p_2) + \chi_3(p_2) \right) \right)
\]

\[
= \frac{x \log \log x}{64 \log x} + o \left( \frac{x \log \log x}{\log x} \right),
\]

where \( \chi_1(p_2) = \left( \frac{p_2}{p_1} \right), \chi_2(p_2) = \left( \frac{p_2}{p_1} \right) \), \( \chi_3(p_2) = \left( \frac{p_2}{p_1} \right) \), \( \chi_4(p_2) = \left( \frac{p_2}{p_1} \right) \) are Dirichlet characters modulo \( p_1 \). By [6, Theorem 2], we have that

\[
\sum \chi_i(p_2) = o \left( \frac{x \log \log x}{\log x} \right) \quad \text{for } i = 1, 2, 3.
\]
Similarly, we have above character sum estimate for the product of characters: 
\( (\frac{p_2}{p_1}), (\frac{p_2}{p_1})_4, (\frac{3}{p_1})_4, (\frac{4}{p_1p_2})_4 \).

Hence

\[
d_1 = \lim_{x \to \infty} \frac{|A_{1,x}|}{|A_x|} = \frac{5}{16}.
\]

Let \( F = \mathbb{Q}(\sqrt{-p_1p_2}) \in A_{2,x} \). Then, by Corollary 3.7, we have that \( r_4(C(F)) = r_8(C(F)) = 2 \) if and only if \( p_1 \equiv 1 \pmod{8} \), \( (\frac{p_1}{p_2})_4 = (\frac{p_2}{p_1})_4 = 1 \) and \( (\frac{p_2}{p_1})_2 = (\frac{1}{p_2})_2 = (\frac{1}{p_1})_2 \). Hence

\[
|A_{2,x}(F)| = \sum_{p_1, p_2 \in A_x \atop p_1, p_2 \equiv 1 \pmod{8}} \frac{1}{32} \left( 1 + \left( \frac{p_2}{p_1} \right)_4 \right) \left( 1 + \left( \frac{p_1}{p_2} \right)_4 \right) \left( 1 + \left( \frac{1}{p_1} \right)_2 \right) \left( 1 + \left( \frac{1}{p_2} \right)_2 \right)
\]

\[
= \sum_{p_1, p_2 \in A_x \atop p_1, p_2 \equiv 1 \pmod{8}} \frac{1}{32} + o\left( \frac{x \log \log x}{\log x} \right)
\]

\[
= \frac{x \log \log x}{512 \log x} + o\left( \frac{x \log \log x}{\log x} \right).
\]

Thus

\[
d_2 = \lim_{x \to \infty} \frac{|A_{2,x}|}{|A_x|} = \frac{1}{128}.
\]

Let \( F = \mathbb{Q}(\sqrt{-2p_1p_2}) \in A_{3,x} \). Then, by Corollary 3.9, we have that \( r_4(C(F)) = r_8(C(F)) = 1 \) if and only if one of the following three conditions holds:

1. \( p_1 \equiv 2 \pmod{4} \), \( (\frac{p_1}{p_2})_4 = 1 \) and \( (\frac{2}{p_2})_4 = 1 \);
2. \( p_2 \equiv 1 \pmod{4} \), \( (\frac{p_1}{p_2})_4 = 1 \) and \( (\frac{2}{p_1})_4 = 1 \);
3. \( p_1 \equiv p_2 \equiv 1 \pmod{8} \), \( (\frac{p_1}{p_2})_4 = 1 \) and \( (\frac{2}{p_1p_2})_4 = 1 \).

Hence

\[
|A_{3,x}| = \sum_{p_1, p_2 \in A_x \atop p_1 \equiv 2 \pmod{4} \atop p_2 \equiv 1 \pmod{8}} \frac{1}{4} \left( 1 + \left( \frac{p_2}{p_1} \right)_4 \right) \left( 1 + \left( \frac{2p_1}{p_2} \right)_4 \right)
\]

\[
+ \sum_{p_1, p_2 \in A_x \atop p_2 \equiv 2 \pmod{4} \atop p_1 \equiv 1 \pmod{8}} \frac{1}{4} \left( 1 + \left( \frac{p_1}{p_2} \right)_4 \right) \left( 1 + \left( \frac{2p_2}{p_1} \right)_4 \right)
\]

\[
+ \sum_{p_1, p_2 \in A_x \atop p_1 \equiv 2 \pmod{4} \atop p_2 \equiv 1 \pmod{8}} \frac{1}{4} \left( 1 - \left( \frac{p_1}{p_2} \right)_4 \right) \left( 1 + \left( \frac{2}{p_1p_2} \right)_4 \right)
\]

\[
= \sum_{p_1, p_2 \in A_x} \left( \frac{1}{16} + \frac{1}{16} + \frac{1}{16} + \frac{1}{16} \right) + o\left( \frac{x \log \log x}{\log x} \right)
\]
\[ \frac{3}{64} \cdot \frac{x \log \log x}{\log x} + o\left(\frac{x \log \log x}{\log x}\right). \]

Hence

\[ d_3 = \lim_{x \to \infty} \frac{|A_{3,x}|}{|A_x|} = \frac{3}{16}. \]

Let \( F = \mathbb{Q}(\sqrt{-2p_1p_2}) \in A_{4,x} \). Then by Corollary 3.12, we have that \( r_4(C(F)) = r_8(C(F)) = 2 \) if and only if \( p_1 \equiv p_2 \equiv 1 \mod 8 \), \( (\frac{p_1}{p_2})_4 = (\frac{p_2}{p_1})_4 = (\frac{2}{p_1})_4 = (\frac{2}{p_2})_4 = (\frac{1}{p_1})_4 \). Hence

\[
|A_{4,x}| = \sum_{p_1 \leq x} \frac{1}{32} \left( 1 + \left( \frac{p_1}{p_2} \right)_4 \right) \left( 1 + \left( \frac{2p_1}{p_2} \right)_4 \right) \left( 1 + \left( \frac{2p_2}{p_1} \right)_4 \right)
\times \left( 1 + \left( \frac{2}{p_2} \right)_4 \right) \left( 1 + \left( \frac{2}{p_1} \right)_4 \right) \left( \frac{71}{\pi_2} \right)
\]

\[ = \frac{1}{512} \cdot \frac{x \log \log x}{\log x} + o\left(\frac{x \log \log x}{\log x}\right). \]

Hence

\[ d_4 = \lim_{x \to \infty} \frac{|A_{4,x}|}{|A_x|} = \frac{1}{128}. \]

\[ \square \]

References


Hwanyup Jung
Department of Mathematics Education
Chungbuk National University
Cheongju 361-763, Korea
E-mail address: hyjung@chungbuk.ac.kr

Qin Yue
Department of Mathematics
Nanjing University of Aeronautics and Astronautics
Nanjing, 210016, P. R. China
E-mail address: yueqin@nuaa.edu.cn