COMPARISON OF 4-CLASS RANKS OF CERTAIN QUADRATIC FIELDS

FRANK GERTH III

(Communicated by David E. Rohrlich)

Abstract. Let $m$ be a square-free positive integer. Let $r_4(K)$ denote the 4-class rank of a quadratic field $K$. This paper examines how likely it is for $r_4(\mathbb{Q}(\sqrt{-m})) = r_4(\mathbb{Q}(\sqrt{m}))$ and for $r_4(\mathbb{Q}(\sqrt{-m})) = r_4(\mathbb{Q}(\sqrt{m})) + 1$.

1. Introduction

Let $K$ be a quadratic extension of the field of rational numbers $\mathbb{Q}$. Let $C(K)$ denote the 2-class group of $K$ in the narrow sense. It is well known that $\text{rank } C(K) = t - 1$, where $t$ is the number of primes that ramify in $K/\mathbb{Q}$. Let $r_4(K)$ denote the 4-class rank of $K$ in the narrow sense; i.e.,

\begin{equation}
(1.1) \quad r_4(K) = \dim_{\mathbb{F}_2} \left( (C(K))^2/(C(K))^4 \right)
\end{equation}

where $(C(K))^i = \{ c^i : c \in C(K) \}$ for positive integers $i$, and $\mathbb{F}_2$ is the finite field with two elements. In Equation (1.1), we are viewing the elementary abelian 2-group $(C(K))^2/(C(K))^4$ as a vector space over $\mathbb{F}_2$.

Now let $m$ be a square-free positive integer. It is known (cf. \[2\], \[4\]) that

\begin{equation}
(1.2) \quad r_4(\mathbb{Q}(\sqrt{-m})) \leq r_4(\mathbb{Q}(\sqrt{m})) \leq r_4(\mathbb{Q}(\sqrt{m})) + 1.
\end{equation}

We will consider the following question: how likely is it that $r_4(\mathbb{Q}(\sqrt{-m})) = r_4(\mathbb{Q}(\sqrt{m}))$, and how likely is it that $r_4(\mathbb{Q}(\sqrt{-m})) = r_4(\mathbb{Q}(\sqrt{m})) + 1$? A direct answer could be obtained if we could compute

\[
\lim_{x \to \infty} \frac{|\{\text{square-free } m \leq x : r_4(\mathbb{Q}(\sqrt{-m})) = r_4(\mathbb{Q}(\sqrt{m}))\}|}{|\{\text{square-free } m \leq x\}|}
\]

or

\[
\lim_{x \to \infty} \frac{|\{\text{square-free } m \leq x : r_4(\mathbb{Q}(\sqrt{-m})) = r_4(\mathbb{Q}(\sqrt{m})) + 1\}|}{|\{\text{square-free } m \leq x\}|}
\]

where $|S|$ denotes the cardinality of a set $S$. However, computing these limits appears to be very difficult. Instead, we shall use a somewhat different approach. Although the limits we compute are not guaranteed to equal the above limits, our results do provide some insight into this question.

Received by the editors January 19, 2000.

2000 Mathematics Subject Classification. Primary 11R11, 11R29, 11R45.

©2001 American Mathematical Society

2547
First we introduce some notation. For positive integers $t$, nonnegative integers $i$, positive real numbers $x$, and square-free positive integers $m$, we define

\[ A_{t,x} = \{ \mathbb{Q}(\sqrt{-m}) : \text{exactly } t \text{ primes ramify in } \mathbb{Q}(\sqrt{-m})/\mathbb{Q} \text{ and } m \leq x \}, \]
\[ A_{t,i,x} = \{ \mathbb{Q}(\sqrt{-m}) \in A_{t,x} : r_4(\mathbb{Q}(\sqrt{-m})) = i \}, \]
\[ A_{t,1,x}^{(1)} = \{ \mathbb{Q}(\sqrt{-m}) \in A_{t,i,x} : r_4(\mathbb{Q}(\sqrt{-m})) = r_4(\mathbb{Q}(\sqrt{m})) \}, \]
\[ A_{t,1,x}^{(2)} = \{ \mathbb{Q}(\sqrt{-m}) \in A_{t,i,x} : r_4(\mathbb{Q}(\sqrt{-m})) = r_4(\mathbb{Q}(\sqrt{m})) + 1 \}. \]

We then define the following densities:

(1.3) \[ a_{t,i} = \lim_{x \to \infty} \frac{|A_{t,i,x}|}{|A_{t,x}|}, \]

(1.4) \[ a_{t,1}^{(1)} = \lim_{x \to \infty} \frac{|A_{t,1,x}^{(1)}|}{|A_{t,x}|}, \]

(1.5) \[ a_{t,1}^{(2)} = \lim_{x \to \infty} \frac{|A_{t,1,x}^{(2)}|}{|A_{t,x}|}. \]

Next we define the limit densities:

(1.6) \[ a_{\infty,i} = \lim_{t \to \infty} a_{t,i}, \]

(1.7) \[ a_{\infty,1}^{(1)} = \lim_{t \to \infty} a_{t,1}^{(1)}, \]

(1.8) \[ a_{\infty,1}^{(2)} = \lim_{t \to \infty} a_{t,1}^{(2)}. \]

It is known (cf. Equation (1.5) in [4]) that

(1.9) \[ a_{\infty,i} = 2^{-i^2} \prod_{k=1}^{\infty} \frac{1}{(1 - 2^{-k})^2} \]

for $i = 0, 1, 2, \ldots$. Furthermore, $\sum_{i=0}^{\infty} a_{\infty,i} = 1$, and, of course, $a_{\infty,i} = a_{\infty,1}^{(1)} + a_{\infty,1}^{(2)}$. To obtain the likelihood that $r_4(\mathbb{Q}(\sqrt{-m})) = r_4(\mathbb{Q}(\sqrt{m}))$ and that $r_4(\mathbb{Q}(\sqrt{-m})) = r_4(\mathbb{Q}(\sqrt{m})) + 1$, we let

(1.10) \[ \alpha_1 = \sum_{i=0}^{\infty} a_{\infty,1}^{(1)}, \]

(1.11) \[ \alpha_2 = \sum_{i=0}^{\infty} a_{\infty,1}^{(2)}. \]

We shall prove the following theorem.
**Theorem 1.** Let \( \alpha_1 \) and \( \alpha_2 \) be defined by Equations (1.10) and (1.11), and let \( a_{\infty,i} \) be given by Equation (1.9). Then

\[
\alpha_1 = \sum_{i=0}^{\infty} 2^{-i} a_{\infty,i} \approx 0.610321 ;
\]

\[
\alpha_2 = \sum_{i=0}^{\infty} (1 - 2^{-i}) a_{\infty,i} \approx 0.389679 .
\]

**Remark.** Theorem 1 is also valid if we use the 4-class rank in the usual sense rather than the narrow sense (cf. discussion on p. 491 of [4]).

**2. Proof of Theorem 1**

From the discussion on p. 491 of [4], it suffices to consider \( m = p_1 \cdots p_t \) with distinct odd primes \( p_1, \ldots, p_t \) and with an odd number of primes \( p_i \equiv 3 \pmod{4} \) when analyzing \( A_{t;x} \) and its subsets in our counting arguments. For convenience we label the primes so that

\[(2.1) \quad p_i \equiv 1 \pmod{4} \text{ for } 1 \leq i \leq s,
\]

\[(2.2) \quad p_i \equiv 3 \pmod{4} \text{ for } s + 1 \leq i \leq t
\]

where \( s \geq 0 \) and \( t - s \) is odd. Now the 4-class rank of \( K = \mathbb{Q}(\sqrt{-m}) \) satisfies

\[(2.3) \quad r_4(K) = t - 1 - \text{rank } M'_K
\]

where \( M'_K = [b_{ij}] \) is the \( t \times (t - 1) \) matrix with entries in \( \mathbb{F}_2 \) defined by Legendre symbols as follows:

\[(2.4) \quad (-1)^{b_{ij}} = \begin{cases} 
\left( \frac{P_i}{P_j} \right), & \text{if } i \neq j, \\
\left( \frac{-m/P_j}{P_i} \right), & \text{if } i = j,
\end{cases}
\]

for \( 1 \leq i \leq t \) and \( 1 \leq j \leq t - 1 \) (cf. Equation (2.6) in [4]). Here \( P_j = p_j \) if \( p_j \equiv 1 \pmod{4} \), and \( P_j = -p_j \) if \( p_j \equiv 3 \pmod{4} \). As discussed on p. 492 in [4], it is also true that

\[(2.5) \quad r_4(K) = t - 1 - \text{rank } M_K
\]

where \( M_K \) is the \( t \times t \) matrix with entries defined by Equation (2.4), except with \( 1 \leq j \leq t \) instead of \( 1 \leq j \leq t - 1 \). Furthermore, the sum of the entries in each row of \( M_K \) is zero, and the sum of the entries in each column of \( M_K \) is zero.

Now we let \( L = \mathbb{Q}(\sqrt{m}) \). Since there are an odd number of primes \( p_i \equiv 3 \pmod{4} \) that divide \( m \), then \( m \equiv 3 \pmod{4} \). So \( t + 1 \) primes ramify in \( L/\mathbb{Q} \); namely \( p_1, \ldots, p_t \) and 2. The 4-class rank of \( L \) satisfies

\[(2.6) \quad r_4(L) = (t + 1) - 1 - \text{rank } M'_L
\]

where \( M'_L = [c_{ij}] \) is the \((t + 1) \times t\) matrix over \( \mathbb{F}_2 \) whose entries satisfy

\[(2.7) \quad c_{ij} = \begin{cases}
 b_{ij} \text{ if } (i \neq j \text{ and } 1 \leq i \leq t, \ 1 \leq j \leq t) \text{ or if } (i = j \text{ and } 1 \leq i \leq s), \\
b_{ij} + 1 \text{ if } i = j \text{ and } s + 1 \leq i \leq t, \\
0 \text{ if } i = t + 1 \text{ and } 2 \text{ splits in } \mathbb{Q}(\sqrt{P_j}), \\
1 \text{ if } i = t + 1 \text{ and } 2 \text{ remains prime in } \mathbb{Q}(\sqrt{P_j}).
\end{cases}
\]
Let $M_L$ denote the $t \times t$ matrix consisting of the first $t$ rows of $M'_L$.

**Lemma 1.** $\text{Rank } M_L = \text{rank } M_K + 1$.

**Proof.** Write

$$M_K = \begin{bmatrix} B_1 & B_2 \\ B_3 & B_4 \end{bmatrix}$$

where $B_1$ is an $s \times s$ symmetric matrix over $\mathbb{F}_2$, $B_2$ is an $s \times (t-s)$ matrix over $\mathbb{F}_2$, $B_3$ is the $(t-s) \times s$ matrix which equals $B_2^T$ (the transpose of $B_2$), and $B_4$ is a $(t-s) \times (t-s)$ antisymmetric matrix over $\mathbb{F}_2$ (i.e., $b_{ij} = b_{ji} + 1$ for $i \neq j$). These properties follow from Equation (2.4) and quadratic reciprocity. Note that

$$M_K^T = \begin{bmatrix} B_1^T & B_3^T \\ B_2^T & B_4^T \end{bmatrix} = \begin{bmatrix} B_1 & B_2 \\ B_3 & B_4 + I + J \end{bmatrix}$$

where $I$ is the $(t-s) \times (t-s)$ identity matrix, and $J$ is the $(t-s) \times (t-s)$ matrix with each entry equal to 1. Now from Equations (2.7) and (2.8) and our definition of $M_L$,

$$M_L = \begin{bmatrix} B_1 & B_2 \\ B_3 & B_4 + I \end{bmatrix} = \begin{bmatrix} B_1 & B_2 \\ B_3 & B_4 + I + 2J \end{bmatrix} = M_K^T + H$$

since $2J$ is a zero matrix over $\mathbb{F}_2$, and where

$$H = \begin{bmatrix} O & 0 \\ 0 & J \end{bmatrix}.$$

Now let $v \in \mathbb{F}_2^t$. (Think of $v$ as a column vector.) If the last $(t-s)$ entries in $v$ contain an even number of 1’s, then

$$M_L v = M_K^T v + H v = M_K v.$$

Let

$$W = \{ M_K^T v : v \in \mathbb{F}_2^t \text{ with an even number of 1’s in the last } (t-s) \text{ entries in } v \}.$$ 

If the last $(t-s)$ entries in $v$ contain an odd number of 1’s, let $v_1 = v + v_2$, where $v_2 = [0, \ldots, 0, 1]^T$. Note that the last $(t-s)$ entries in $v_1$ contain an even number of 1’s, and $v = v_1 + v_2$. Then

$$M_K^T v = M_K^T v_1 + M_K^T v_2.$$

Clearly $M_K^T v_1 \in W$. Next, note that $M_K^T v_2 = M_K^T v_3$, where $v_3 = [1, \ldots, 1, 0]^T$, since the sum of the entries in each row of $M_K^T$ is zero. But then $M_K^T v_3 \in W$ since $v_3$ has an even number of 1’s in its last $(t-s)$ entries. Thus

$$M_K^T v = M_K^T v_1 + M_K^T v_3 \in W.$$

So $W$ is the column space of $M_K^T$, and from Equation (2.11), we know that the column space of $M_L$ contains $W$. Also, since the matrix $H$ in Equation (2.10) has rank equal to 1, then from Equation (2.9), we know that

$$\text{rank } M_K^T \leq \text{rank } M_L \leq \text{rank } M_K^T + 1.$$

Now let $v_4$ be the vector in $\mathbb{F}_2^t$ with each component equal to 1. Then $M_K^T v_4$ is the zero vector in $\mathbb{F}_2^t$ since the sum of the entries in each row of $M_K^T$ is zero. Then from
Equations (2.9) and (2.10), $M_L v_4$ is the vector in $\mathbb{F}_2^t$ whose first $s$ components are 0’s and whose last $(t-s)$ components are 1’s since $t-s$ is odd. Then the sum of the entries in $M_L v_4$ is 1. But then $M_L v_4$ does not belong to the column space of $M_K^T$ since the sum of the entries in each column of $M_K^T$ is zero. Thus from (2.13), we see that

$$\text{rank } M_L = \text{rank } M_K^T + 1 = \text{rank } M_K + 1$$

which completes the proof of Lemma 1.

We let

$$w = \text{rank } M_K = \text{rank } M_L - 1 .$$

We now consider the $(t+1) \times t$ matrix $M_L'$ whose first $t$ rows form the matrix $M_L$. From Equation (2.7), we observe that the entries in the last row of $M_L'$ satisfy

$$c_{(t+1)j} = \begin{cases} 0, & \text{if } p_j \equiv \pm 1 \pmod{8}, \\ 1, & \text{if } p_j \equiv \pm 3 \pmod{8}. \end{cases}$$

Since the primes are equally distributed among the residue classes $\pm 1 \pmod{8}$ and $\pm 3 \pmod{8}$, it is intuitively clear that each entry in the last row of $M_L'$ is equally likely to be a 0 or a 1. (This can be proved using character sums similar to those used to prove Propositions 2.1 and 5.1 in [4]. See [3] and [5] (or [1]) for more details on character sum calculations.) Then, of the possible $2^t$ matrices $M_L'$ whose first $t$ rows form $M_L$, $2^{1+w}$ satisfy $\text{rank } M_L' = \text{rank } M_L$, and $(2^t - 2^{1+w})$ satisfy $\text{rank } M_L' = \text{rank } M_L + 1$. From Equation (2.6) and the above discussion,

$$r_4(L) = \begin{cases} t - 1 - w & \text{with probability } 2^{-(t-1-w)} \\ t - 2 - w & \text{with probability } 1 - 2^{-(t-1-w)}. \end{cases}$$

Then Equations 2.5, 2.14, and 2.15 give

$$r_4(K) = \begin{cases} r_4(L) & \text{with probability } 2^{-(t-1-w)} \\ r_4(L) + 1 & \text{with probability } 1 - 2^{-(t-1-w)}. \end{cases}$$

Then letting $i = t - 1 - w$ and using Equations 1.3, 1.4, and 1.5, we get

$$a_{t,i}^{(1)} = 2^{-i} a_{t,i} \quad \text{and} \quad a_{t,i}^{(2)} = (1 - 2^{-i}) a_{t,i} .$$

Taking the limit as $t \to \infty$, we get

$$a_{\infty,i}^{(1)} = 2^{-i} a_{\infty,i} \quad \text{and} \quad a_{\infty,i}^{(2)} = (1 - 2^{-i}) a_{\infty,i} .$$

Then summing over all $i \geq 0$, we get Theorem 1.

REFERENCES


Department of Mathematics, The University of Texas at Austin, Austin, Texas 78712-1082
E-mail address: gerth@math.utexas.edu