ON 2-CLASS FIELD TOWERS FOR QUADRATIC NUMBER FIELDS WITH 2-CLASS GROUP OF TYPE (2, 2)

by FRANK GERTH III

(Received 25 July, 1996)

1. Introduction. Let K be a quadratic number field with 2-class group of type (2, 2). Thus if S_K is the Sylow 2-subgroup of the ideal class group of K, then $S_K \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Let

$$K \subset K_1 \subset K_2 \subset K_3 \subset \ldots$$

be the 2-class field tower of K. Thus K_1 is the maximal abelian unramified extension of K of degree a power of 2; K_2 is the maximal abelian unramified extension of K_1 of degree a power of 2; etc. By class field theory the Galois group $\mathrm{Gal}(K_1/K) \cong S_K \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, and in this case it is known that $\mathrm{Gal}(K_2/K_1)$ is a cyclic group (cf. **[3]** and **[10]**). Then by class field theory the class number of K_2 is odd, and hence $K_2 = K_3 = K_4 = \ldots$. We say that the 2-class field tower of K terminates at K_1 if the class number of K_1 is odd (and hence $K_1 = K_2 = K_3 = \ldots$); otherwise we say that the 2-class field tower of K terminates at K_2. Our goal in this paper is to determine how likely it is for the 2-class field tower of K to terminate at K_1, and how likely it is for the 2-class field tower of K to terminate at K_2. We shall consider separately the imaginary quadratic fields and the real quadratic fields.

Suppose first that $K = \mathbb{Q}(\sqrt{-m})$, where $m = p_1 p_2 \ldots p_r$ with primes $p_1 < p_2 < \ldots < p_r$. We let

$$A = \{K = \mathbb{Q}(\sqrt{-m}) \colon \text{the 2-class group } S_K \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}\} \tag{1.1}$$

$$A_i = \{K \in A \colon \text{the 2-class field tower of } K \text{ terminates at } K_i\} \tag{1.2}$$

for $i = 1, 2$. For positive real numbers x and for $i = 1, 2$, we let

$$A_x = \{K \in A \colon m \leq x\} \tag{1.3}$$

$$A_{i,x} = \{K \in A_i \colon m \leq x\}. \tag{1.4}$$

We then define relative densities d_i as follows. Let

$$d_i = \lim_{x \to \infty} \frac{|A_{i,x}|}{|A_x|} \tag{1.5}$$

for $i = 1, 2$, where $|C|$ denotes the cardinality of a set C. In the next section we shall prove the following theorem.

THEOREM 1. *Let d_1 and d_2 be the relative densities defined by equation* (1.5). *Then*

$$d_1 = \frac{1}{7} \quad \text{and} \quad d_2 = \frac{6}{7}.$$

Now we consider real quadratic fields $K = \mathbb{Q}(\sqrt{m})$, where $m = p_1 p_2 \dots p_r$ with primes $p_1 < p_2 < \dots < p_r$. We let

$$A' = \{K = \mathbb{Q}(\sqrt{m}) : \text{the 2-class group } S_K \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}\} \tag{1.6}$$

$$A'_i = \{K \in A' : \text{the 2-class field tower of } K \text{ terminates at } K_i\} \tag{1.7}$$

for $i = 1, 2$. For positive real numbers x and for $i = 1, 2$, we let

$$A'_x = \{K \in A' : m \le x\} \tag{1.8}$$

$$A'_{i,x} = \{K \in A'_i : m \le x\} \tag{1.9}$$

and then we define relative densities d'_i for $i = 1, 2$ by

$$d'_i = \lim_{x \to \infty} \frac{|A'_{i,x}|}{|A'_x|}. \tag{1.10}$$

In the last section we shall prove the following theorem.

THEOREM 2. *Let d'_1 and d'_2 be the relative densities defined by equation* (1.10). *Then*

$$d'_1 = \frac{7}{19} \quad \text{and} \quad d'_2 = \frac{12}{19}.$$

2. Proof of Theorem 1. Let $K = \mathbb{Q}\sqrt{-m})$, where $m = p_1 p_2 \dots p_r$ with primes $p_1 < p_2 < \dots < p_r$. For the 2-class group $S_K \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, we know from genus theory that m must have one of the following forms:

$$m = \begin{cases} p_1 p_2 p_3 \text{ with each } p_i \equiv 3 \pmod 4 \\ p_1 p_2 p_3 \text{ with two of the } p_i \equiv 1 \pmod 4 \text{ and the other } p_i \equiv 3 \pmod 4 \\ p_1 p_2 \text{ with } p_1 \equiv p_2 \pmod 4 \\ 2 p_1 p_2 \end{cases} \tag{2.1}$$

(cf. section 2 of [**8**]). Moreover, there are additional restrictions imposed on the primes dividing m in order that $S_K \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. These restrictions can be specified by indicating the values of certain Legendre symbols used to form Rédei matrices (cf. [**9**]). The appropriate values for the Legendre symbols are given in various cases in [**8**].

Now recalling the specification of A in equation (1.1) and the forms of m in (2.1), we let

$$B_1 = \{K \in A : m = p_1 p_2 p_3 \text{ with each } p_i \equiv 3 \pmod 4\} \tag{2.2}$$

$$B_2 = \{K \in A : m = p_1 p_2 p_3 \text{ with two of the } p_i \equiv 1 \pmod 4$$
$$\text{and the other } p_i \equiv 3 \pmod 4\} \tag{2.3}$$

$$B_3 = \{K \in A : m = p_1 p_2 \text{ or } 2 p_1 p_2\}. \tag{2.4}$$

Next for positive real numbers x, we let

$$B_{i,x} = \{K \in B_i : m \le x\} \tag{2.5}$$

https://doi.org/10.1017/S0017089500032353 Published online by Cambridge University Press

for $i = 1, 2, 3$. It is a standard calculation that

$$|B_{3,x}| = O\left(\frac{x \log \log x}{\log x}\right) \qquad (\text{as } x \to \infty) \tag{2.6}$$

(cf. [7], Theorem 437).

For B_1, the relevant case in section 2 in [8] is case (iii). Then for the Legendre symbols we need

$$\left(\frac{p_2}{p_1}\right) = 1, \qquad \left(\frac{p_3}{p_1}\right) = -1, \qquad \left(\frac{p_3}{p_2}\right) = 1 \tag{2.7}$$

or

$$\left(\frac{p_2}{p_1}\right) = -1, \qquad \left(\frac{p_3}{p_1}\right) = 1, \qquad \left(\frac{p_3}{p_2}\right) = -1. \tag{2.8}$$

Next we let $u_{ij} = 0$ or 1 for $1 \leq i < j \leq 3$. (We shall specify below how we want to choose the u_{ij}.) Then we let

$$\begin{aligned} B_{1,x}(0,1,0) = \{p_1p_2p_3 \leq x : p_1 < p_2 < p_3 &\text{ are primes with each} \\ p_i \equiv 3 (\text{mod } 4), \quad \left(\frac{p_j}{p_i}\right) &= (-1)^{u_{ij}} \text{ for } 1 \leq i < j \leq 3 \\ \text{with } u_{12} = 0, \quad u_{13} = 1, \quad u_{23} &= 0\} \end{aligned} \tag{2.9}$$

and

$$\begin{aligned} B_{1,x}(1,0,1) = \{p_1p_2p_3 \leq x : p_1 < p_2 < p_3 &\text{ are primes with each} \\ p_i \equiv 3 (\text{mod } 4), \quad \left(\frac{p_j}{p_i}\right) &= (-1)^{u_{ij}} \text{ for } 1 \leq i < j \leq 3 \\ \text{with } u_{12} = 1, \quad u_{13} = 0, \quad u_{23} &= 1\}. \end{aligned} \tag{2.10}$$

From equations (2.2), (2.5), and (2.7) through (2.10), we see that

$$|B_{1,x}| = |B_{1,x}(0,1,0)| + |B_{1,x}(1,0,1)|. \tag{2.11}$$

Now given a set of values u_{ij} $(1 \leq i < j \leq 3)$ as above, for arbitrary distinct odd primes p_i and p_j, we let $\delta(p_i, p_j) = 1$ if $\left(\frac{p_j}{p_i}\right) = (-1)^{u_{ij}}$, and we let $\delta(p_i, p_j) = 0$ if $\left(\frac{p_j}{p_i}\right) \neq (-1)^{u_{ij}}$. For the set of values $u_{12} = 0$, $u_{13} = 1$, $u_{23} = 0$, we get

$$\begin{aligned} |B_{1,x}(0,1,0)| &= \sum_{\substack{p_1 \leq x^{1/3} \\ p_1 \equiv 3 (\text{mod } 4)}} \sum_{\substack{p_1 < p_2 \leq (x/p_1)^{1/2} \\ p_2 \equiv 3 (\text{mod } 4)}} \delta(p_1, p_2) \sum_{\substack{p_2 < p_3 \leq x/p_1p_2 \\ p_3 \equiv 3 (\text{mod } 4)}} \delta(p_1, p_3)\delta(p_2, p_3) \\ &\sim 2^{-6} \cdot \frac{1}{2!} \frac{x(\log \log x)^2}{\log x} \qquad (\text{as } x \to \infty) \end{aligned} \tag{2.12}$$

(cf. (2.11) and (2.12) in [5]). The analytic machinery for this type of calculation appears in Section 4 of [**4**] and Section 5 of [**6**]. Alternately, one can use the analytic machinery developed in Section 3 of [**2**]. An intuitive explanation for (2.12) is that

$$\sum_{\substack{p_1,p_2,p_3\\ p_1<p_2<p_3\\ p_1p_2p_3\le x}} 1 \sim \frac{1}{2!}\frac{x(\log\log x)^2}{\log x} \qquad (\text{as } x\to\infty)$$

and a factor of $\frac{1}{2}$ is introduced by each of the congruence conditions $p_i \equiv 3 (\bmod 4)$ for $i=1,2,3$ and by each of the factors $\delta(p_i,p_j)$ for $1\le i<j\le 3$. A similar calculation shows that

$$|B_{1,x}(1,0,1)| \sim 2^{-6}\cdot\frac{1}{2!}\frac{x(\log\log x)^2}{\log x} \qquad (\text{as } x\to\infty). \tag{2.13}$$

Then from (2.11), (2.12), and (2.13), we get

$$|B_{1,x}| \sim 2\,.\,2^{-6}\cdot\frac{1}{2!}\frac{x(\log\log x)^2}{\log x} \qquad (\text{as } x\to\infty). \tag{2.14}$$

For the calculation of $|B_{2,x}|$, the formula analogous to (2.14) is

$$|B_{2,x}| \sim 12\,.\,2^{-6}\cdot\frac{1}{2!}\frac{x(\log\log x)^2}{\log x} \qquad (\text{as } x\to\infty). \tag{2.15}$$

The factor "12" can be explained as follows. First we note that there are three distinct arrangements for the congruence conditions 1(mod 4), 1(mod 4), 3(mod 4) in (2.3). For each of these arrangements, there are four allowable sets of values for the Legendre symbols $\left(\frac{p_2}{p_1}\right)$, $\left(\frac{p_3}{p_1}\right)$, $\left(\frac{p_3}{p_2}\right)$ in case (iv) in section 2 in [**8**], and then $3\cdot 4=12$. For example, when $p_1\equiv p_2\equiv -p_3\equiv 1(\bmod 4)$, the allowable sets of Legendre symbol values are

$$\left(\frac{p_2}{p_1}\right)=1,\quad \left(\frac{p_3}{p_1}\right)=-1,\quad \left(\frac{p_3}{p_2}\right)=-1$$

and

$$\left(\frac{p_2}{p_1}\right)=-1,\qquad \left(\frac{p_3}{p_i}\right)=-1 \text{ for at least one of } p_i=p_1,p_2.$$

(The last line actually corresponds to three distinct sets.) Now from the discussion of case (iii) in Section 2 in [**8**], we have $B_1\subset A_1$, and from the discussion of case (iv) in Section 2 in [**8**], we have $B_2\subset A_2$. Then $B_{1,x}\subset A_{1,x}$ and $B_{2,x}\subset A_{2,x}$. Since $A=B_1\cup B_2\cup B_3$ and B_1,B_2,B_3 are disjoint sets, then from equations (1.3), (1.4), (2.5), (2.6), and formulas (2.14) and (2.15), we get

$$|A_{1,x}| \sim |B_{1,x}| \sim 2\,.\,2^{-6}\cdot\frac{1}{2!}\frac{x(\log\log x)^2}{\log x} \qquad (\text{as } x\to\infty) \tag{2.16}$$

$$|A_{2,x}| \sim |B_{2,x}| \sim 12\,.\,2^{-6}\cdot\frac{1}{2!}\frac{x(\log\log x)^2}{\log x} \qquad (\text{as } x\to\infty) \tag{2.17}$$

$$|A_x| \sim |B_{1,x}|+|B_{2,x}| \sim 14\,.\,2^{-6}\cdot\frac{1}{2!}\frac{x(\log\log x)^2}{\log x} \qquad (\text{as } x\to\infty). \tag{2.18}$$

Then from equation (1.5) and formulas (2.16) through (2.18), we get $d_1 = \frac{1}{7}$ and $d_2 = \frac{6}{7}$, which completes the proof of Theorem 1.

3. Proof of Theorem 2. Let $K = \mathbb{Q}(\sqrt{m})$, where $m = p_1 p_2 \ldots p_r$ with primes $p_1 < p_2 < \ldots < p_r$. In order that the 2-class group $S_K \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, genus theory requires that m must have one of the following forms:

$$m = \begin{cases} p_1 p_2 p_3 p_4 \text{ with each } p_i \equiv 3 (\text{mod } 4) \\ p_1 p_2 p_3 p_4 \text{ with two } p_i \equiv 1 (\text{mod } 4) \text{ and two } p_i \equiv 3 (\text{mod } 4) \\ m' \text{ with } m' \text{ divisible by at most three odd primes.} \end{cases} \tag{3.1}$$

An example of the last case is $m' = p_1 p_2 p_3$ with each $p_i \equiv 1 (\text{mod } 4)$. There are additional requirements on the primes dividing m in order that $S_K \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, and we shall consider those requirements later in this section.

With A' defined by (1.6), we next define

$$B_1' = \{K \in A' : m = p_1 p_2 p_3 p_4 \text{ with each } p_i \equiv 3 (\text{mod } 4)\}, \tag{3.2}$$

$$B_2' = \{K \in A' : m = p_1 p_2 p_3 p_4 \text{ with two } p_i \equiv 1 (\text{mod } 4) \text{ and two } p_i \equiv 3 (\text{mod } 4)\}, \tag{3.3}$$

$$B_3' = \{K \in A' : \text{at most three odd primes divide } m\}, \tag{3.4}$$

For positive real numbers x, we let

$$B_{i,x}' = \{K \in B_i' : m \le x\} \tag{3.5}$$

for $i = 1,2,3$. It is straightforward to calculate that

$$|B_{3,x}'| = O\left(\frac{x(\log \log x)^2}{\log x}\right) \qquad (\text{as } x \to \infty). \tag{3.6}$$

To calculate $|B_{1,x}'|$ and $|B_{2,x}'|$, we need to specify the additional conditions on p_1, p_2, p_3, p_4 that are required for $S_K \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. These conditions come from Rédei matrices that have rank $= 3$, and these matrices are determined by the values $\left\{\left(\frac{p_i}{p_j}\right) : 1 \le i < j \le 4\right\}$.

For fields $K \in B_2'$, we can use the type 4 case of Proposition 1 in [**1**]. We first let $p_1 \equiv p_2 \equiv 1 (\text{mod } 4)$ and $p_3 \equiv p_4 \equiv 3 (\text{mod } 4)$ to match the type 4 case of Proposition 1 in [**1**]. Then the relevant conditions on Legendre symbols are

$$\text{(a)}: \left(\frac{p_1}{p_2}\right) = 1 \ \& \ \left[\left(\frac{p_1}{p_3}\right) = -1 \text{ or } \left(\frac{p_1}{p_4}\right) = -1\right] \ \& \ \left[\left(\frac{p_2}{p_3}\right) = -1 \text{ or } \left(\frac{p_2}{p_4}\right) = -1\right]$$
$$\& \text{ not } \left(\frac{p_1}{p_3}\right) = \left(\frac{p_1}{p_4}\right) = \left(\frac{p_2}{p_3}\right) = \left(\frac{p_2}{p_4}\right)$$

or

$$\text{(b)}: \left(\frac{p_1}{p_2}\right) = -1 \ \& \text{ not } \left(\frac{p_1}{p_3}\right) = \left(\frac{p_2}{p_3}\right) = \left(\frac{p_1}{p_4}\right) = \left(\frac{p_2}{p_4}\right).$$

https://doi.org/10.1017/S0017089500032353 Published online by Cambridge University Press

In cases (a) and (b), $\left(\frac{p_3}{p_4}\right)$ can be either $+1$ or -1. An enumeration of all of the possibilities in these cases $\left(\text{including the value of } \left(\frac{p_3}{p_4}\right)\right)$ yields 16 possibilities for case (a) and 28 possibilities for case (b). So there are 44 possibilities for the set of values $\left\{\left(\frac{p_i}{p_j}\right): 1 \leq i < j \leq 4\right\}$ that produce fields $K = \mathbb{Q}(\sqrt{p_1 p_2 p_3 p_4}) \in B_2'$.

Next we observe that if we order the primes so that $p_1 < p_2 < p_3 < p_4$, there are 6 distinct arrangements of the congruence conditions $1 \pmod 4$, $1 \pmod 4$, $3 \pmod 4$, $3 \pmod 4$. Now since

$$\sum_{\substack{p_1, p_2, p_3, p_4 \\ p_1 < p_2 < p_3 < p_4 \\ p_1 p_2 p_3 p_4 \leq x}} 1 \sim \frac{1}{3!} \frac{x(\log\log x)^3}{\log x} \qquad (\text{as } x \to \infty)$$

then the analog of Formula (2.15) is

$$|B_{2,x}'| \sim 6 \,.\, 44 \,.\, 2^{-10} \,.\, \frac{1}{3!} \frac{x(\log\log x)^3}{\log x} \qquad (\text{as } x \to \infty). \tag{3.7}$$

The factor 2^{-10} comes from a factor of $\frac{1}{2}$ for each of the four congruence conditions and the particular values for the six Legendre symbols $\left(\frac{p_i}{p_j}\right)$ with $1 \leq i < j \leq 4$.

Now we consider $K \in B_1'$. Then each $p_i \equiv 3 \pmod 4$. The relevant Rédei matrices are antisymmetric in this case. (In equation (5.5) of **[5]**, this means $\left(\frac{-p_j}{p_i}\right) = -\left(\frac{-p_i}{p_j}\right)$ for each $i \neq j$.) Then we can use Proposition 5.7(iii) in **[5]** to calculate the appropriate number of Rédei matrices with rank = 3. (In Proposition 5.7(iii) of **[5]**, take $r = 1$, $n = 1$, and $\bar{M} = [1 \;\; 0]$ or $[1 \;\; 1]$.) Proposition 5.7(iii) gives 40 possibilities, 20 corresponding to each of the two choices for $\bar{M}$. Alternately, one can examine the Rédei matrices corresponding to each set of values for $\left\{\left(\frac{p_i}{p_j}\right): 1 \leq i < j \leq 4\right\}$, and then discover that 40 of these 64 matrices have rank = 3. Hence

$$|B_{1,x}'| \sim 40 \,.\, 2^{-10} \,.\, \frac{1}{3!} \frac{x(\log\log x)^3}{\log x} \qquad (\text{as } x \to \infty). \tag{3.8}$$

Then from equations (1.6), (1.8), (3.1) through (3.6) and formulas (3.7) and (3.8), we get

$$|A_x'| = |B_{1,x}'| + |B_{2,x}'| + |B_{3,x}'| \sim 304 \,.\, 2^{-10} \,.\, \frac{1}{3!} \frac{x(\log\log x)^3}{\log x} \qquad (\text{as } x \to \infty). \tag{3.9}$$

Now from Theorem 1 in **[1]**, we see that $B_1' \subset A_1'$. However, $B_2' \not\subset A_2'$ since some of the fields in B_2' are in A_1', as we see by examining the graphs for the type 4 case on p. 175 of **[1]**. More precisely, there are three graph types (i.e., c_{12}, c_{13}, c_{14} on p. 175 in **[1]**) that correspond to fields in A_1'. Furthermore, we can easily check that there are four graphs equivalent to one another in each of these three graph types. ("Equivalent" in this sense is defined on p. 172 of [**1**].) Hence there are 12 graphs altogether that correspond to fields in B_2' that are also in A_1'. Then we can split up $|B_{2,x}'|$ as follows (see (3.7)):

$$|B_{2,x}' \cap A_{1,x}'| \sim 6\,.\,12\,.\,2^{-10}\,.\,\frac{1}{3!}\frac{x(\log\log x)^3}{\log x} \qquad (\text{as } x \to \infty) \tag{3.10}$$

and

$$|B_{2,x}' \cap A_{2,x}'| \sim 6\,.\,32\,.\,2^{-10}\,.\,\frac{1}{3!}\frac{x(\log\log x)^3}{\log x} \qquad (\text{as } x \to \infty). \tag{3.11}$$

Then since $B_1' \subset A_1'$, we can use (3.8) and (3.10) to get

$$\begin{aligned}|A_{1,x}'| &\sim |B_{1,x}'| + |B_{2,x}' \cap A_{1,x}'| \\ &\sim 112\,.\,2^{-10}\,.\,\frac{1}{3!}\frac{x(\log\log x)^3}{\log x} \qquad (\text{as } x \to \infty).\end{aligned} \tag{3.12}$$

Using (3.11), we see that

$$\begin{aligned}|A_{2,x}'| &\sim |B_{2,x}' \cap A_{2,x}'| \\ &\sim 192\,.\,2^{-10}\,.\,\frac{1}{3!}\frac{x(\log\log x)^3}{\log x} \qquad (\text{as } x \to \infty).\end{aligned} \tag{3.13}$$

Then from (1.10) (3.9), (3.12), and (3.13), we get $d_1' = \frac{7}{19}$ and $d_2' = \frac{12}{19}$, which completes the proof of Theorem 2.

REFERENCES

1. E. Benjamin and C. Snyder, Real quadratic number fields with 2-class group of type (2, 2), *Math. Scand.* **76** (1995), 161–178.

2. J. Cremona and R. Odono, Some density results for negative Pell equations; an application of graph theory, *J. London Math. Soc.* **39** (1989), 16–28.

3. P. Furtwängler, Über das Verhalten der Ideale des Grundkörpers im Klassenkörper, *Monatsh. Math. Phys.* **27** (1916), 1–15.

4. F. Gerth, Counting certain number fields with prescribed l-class numbers, *J. Reine Angew. Math.* **337** (1982), 195–207.

5. F. Gerth, The 4-class ranks of quadratic fields, *Invent. Math.* **77** (1984), 489–515.

6. F. Gerth, Densities for ranks of certain parts of p-class groups, *Proc. Amer. Math. Soc.* **99** (1987), 1–8.

7. G. Hardy and E. Wright, *An Introduction to the Theory of Numbers*, 4th edition, (Oxford Univ. Press, London, 1965).

8. H. Kisilevsky, Number fields with class number congruent to 4 mod 8 and Hilbert's theorem 94, *J. Number Theory* **8** (1976), 271–279.

9. L. Rédei, Arithmetischer Beweis des Satzes über die Anzahl der durch vier teilbaren Invarianten der absoluten Klassengruppe im quadratischen Zahlkörper, *J. Reine Angew. Math.* **171** (1934), 55–60.

10. O. Taussky, A remark on the class field tower, *J. London Math. Soc.* **12** (1937), 82–85.

Department of Mathematics
The University of Texas at Austin
Austin, Texas 78712-1082
U.S.A.