PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 96, Number 4, April 1986

LOWER BOUNDS FOR CLASS NUMBERS OF REAL QUADRATIC FIELDS

R. A. MOLLIN[1]

ABSTRACT. Based on the fundamental units of real quadratic fields we provide lower bounds for their class numbers. These results extend work of H. Hasse [**2**] and generalize and *correct* results of H. Yokoi [**8, 9**]. Moreover, for certain real quadratic fields we provide criteria for their class numbers to be divisible by a specific integer.

We begin by introducing certain types of real quadratic fields, the first of which is attributable to C. Richaud [7] and G. Degert [**1**].

DEFINITION 1. If $n = m^2 + r \neq 5$ is a positive square-free integer, where r divides $4m$ and $r \in (-m, m]$, then n is said to be of (*wide*) *Richaud-Degert* (*R-D*) *type*. If $|r| = 1$ or 4, then n is said to be of *narrow R-D type*. (Note that when the norm $N(\varepsilon)$ of the fundamental unit ε of $Q(\sqrt{n})$ is -1, then n is necessarily of narrow R-D type, whereas if $N(\varepsilon) = 1$, then n may be of the more general wide R-D type.)

Types different from the above were studied by H. Yokoi in [**8, 9**]. These types are now described.

DEFINITION 2. Let n be a positive integer with no square factor except possibly 4. Then

(I) Let p be any prime congruent to 1 modulo 4, and let a, b denote the (unique) integers such that $a^2 + 4 = bp^2$ $(0 < a < p^2)$. If $n = p^2m^2 \pm 2am + b$, where $m > p + 1$ if n is square free and $m > 4p + 1$ otherwise, then if n is *not* of (wide) R-D type we say that n is of *Yokoi type* 1 (see [**8**]).

(II) Let p be any prime congruent to 3 modulo 4, and let $n = p^2m^2 \pm 4m$, where $m > p + 1$ if n is square-free and $m > 4p + 1$ otherwise. Then if n is *not* of (narrow) R-D type we say that n is of *Yokoi type* 2 (see [**9**]).

The following result is attributable to Davenport, Ankeny and Hasse (see [**2**]).

LEMMA 1. *Let $K = Q(\sqrt{n})$, where n is a positive square-free integer, and let $\varepsilon = (T + U\sqrt{n})/2$ be the fundamental unit of K. If there exist integers x and y such that $x^2 - ny^2 = \pm 4m$, where $m > 0$ and not a square, then $m \geqslant (T-2)/U^2$ for $N(\varepsilon) = 1$ and $m \geqslant T/U^2$ for $N(\varepsilon) = -1$.*

Now we use the above to establish lower bounds for class numbers of real quadratic fields. In what follows $h(n)$ denotes the class number of $Q(\sqrt{n})$.

Received by the editors February 27, 1985.
1980 *Mathematics Subject Classification*. Primary 12A50, 12A25; Secondary 12A95.
[1]The author's research is supported by N.S.E.R.C. Canada.

THEOREM 1. *Let n be a positive square-free integer and denote the fundamental unit of $K = Q(\sqrt{n})$ by $\varepsilon = (T + U\sqrt{n})/2$. If p is a prime which is not inert in K, and $h(n)$ is odd, then*

$$h(n) \geqslant \frac{\log(\sqrt{nU^2+4}-2) - 2\log(U)}{\log(p)} \quad \text{if } N(\varepsilon) = 1$$

and

$$h(n) \geqslant \frac{\log\sqrt{nU^2-4} - 2\log(U)}{\log(p)} \quad \text{if } N(\varepsilon) = -1.$$

PROOF. If P is a K-prime above p and k is the order of P in the class group of K, then k divides $h(n)$ and $N(P^k) = \pm 4p^k = a^2 - nb^2$, where a and b are integers. Also, k is odd, since p is not inert and $h(n)$ is odd. Thus we may invoke Lemma 1 to get

$$p^{h(n)} \geqslant p^k \geqslant \begin{cases} (T-2)/U^2 & \text{if } N(\varepsilon) = 1, \\ T/U^2 & \text{if } N(\varepsilon) = -1, \end{cases}$$

which implies

$$h(n) \geqslant \begin{cases} \dfrac{\log(T-2) - 2\log(U)}{\log(p)} & \text{if } N(\varepsilon) = 1, \\ \dfrac{\log(T) - 2\log(U)}{\log(p)} & \text{if } N(\varepsilon) = -1. \end{cases}$$

However, $T - 2 = \sqrt{nU^2+4} - 2$ if $N(\varepsilon) = 1$, and $T = \sqrt{nU^2-4}$ if $N(\varepsilon) = -1$. Q.E.D.

The following generalizes and *corrects* [**8**, Theorem 3, p. 147].

COROLLARY 1. *Let $n = p^2m^2 \pm 2am + b$ be of Yokoi type* I, *where p is not inert in K and $h(n)$ is odd. Then $h(n) > 1$, and the following provides a lower bound.*

$$h(n) \geqslant \begin{cases} \dfrac{\log\sqrt{np^2-4}}{\log(p)} - 2 & \textit{if } n \textit{ is square-free}, \\ \dfrac{\log\frac{1}{4}\sqrt{np^2-4}}{\log(p)} - 2 & \textit{otherwise}. \end{cases}$$

PROOF. By [**8**, Theorem 2, p. 144] $N(\varepsilon) = -1$, $T = p^2m \pm a$ and

$$U = \begin{cases} p & \text{if } n \text{ is square-free}, \\ 2p & \text{otherwise}. \end{cases}$$

Therefore by Theorem 1

$$h(n) \geqslant \begin{cases} \dfrac{\log\sqrt{np^2-4}}{\log(p)} - 2 & \text{if } n \text{ is square-free}, \\ \dfrac{\log\frac{1}{4}\sqrt{np^2-4}}{\log(p)} - 2 & \text{otherwise}. \end{cases}$$

Moreover, by Definition 2, $m > p + 1$ if n is square-free and $m > 4p + 1$ if $n \equiv 0 \pmod 4$. Thus $T/U^2 > p$, which implies $h(n) > 1$ as in the proof of Theorem 1. Q.E.D.

We note that in [**8**, Theorem 3, p. 147, bottom line] Yokoi invalidly uses Lemma 1 by ignoring the fact that $h(n)$ may be even (which is not the case in Hasse's use of Lemma 1 in [**2**, p. 59], wherein $h(n)$ is odd). This same error was made by Yokoi in [**9**, Theorem 2, pp. 111–112] (and there is a misprint in the statement thereof), which the following result generalizes and corrects. Please note that in a recent letter to the author Professor Yokoi has indicated that although his proofs are indeed incomplete he has found a proof of the omitted case to verify his results in their entirety.

COROLLARY 2. *Let $n = p^2m^2 \pm 4m$ be of Yokoi type* II, *where p is not inert in K and $h(n)$ is odd. Then $h(n) > 1$, and the following provides a lower bound.*

$$h(n) \geqslant \begin{cases} \dfrac{\log\left(\sqrt{np^2+4}-2\right)}{\log(p)} - 2 & \textit{if } n \textit{ is square-free}, \\[2ex] \dfrac{\log\frac{1}{4}\left(\sqrt{np^2+4}-2\right)}{\log(p)} - 2 & \textit{otherwise}. \end{cases}$$

PROOF. By [**9**, Theorem 1, p. 109] $N(\varepsilon) = 1$, $T = (p^2m \pm 2)$ and

$$U = \begin{cases} p & \text{if } n \text{ is square-free}, \\ 2p & \text{otherwise}. \end{cases}$$

Therefore by Theorem 1

$$h(n) \geqslant \begin{cases} \dfrac{\log\left(\sqrt{np^2+4}-2\right)}{\log(p)} - 2 & \text{if } n \text{ is square-free}, \\[2ex] \dfrac{\log\frac{1}{4}\left(\sqrt{np^2+4}-2\right)}{\log(p)} - 2 & \text{otherwise}. \end{cases}$$

Moreover, by Definition 2, $m > p + 1$ if n is square-free, and $m > 4p + 1$ otherwise. Thus $(T - 2)/U^2 > p$, which implies $h(n) > 1$, as in the proof of Theorem 1. Q.E.D.

The following results on R-D types generalize Hasse [**2**, Satzen 2a–2c, p. 38] (see also [**5**]).

COROLLARY 3. *Let $n = m^2 + r$, where $|r| = 1$, and let $h(n)$ be odd. If p is a prime which is not inert in K and $m > 2p$ for $r = 1$, whereas $m > 2$ for $r = -1$, then $h(n) > 1$, and the following bound holds*:

$$h(n) \geqslant \begin{cases} \dfrac{\log\sqrt{(n-1)/4}}{\log(p)} & \textit{if } r = 1, \\[2ex] \dfrac{\log\frac{1}{4}(\sqrt{4n+4}-2)}{\log(p)} & \textit{if } r = -1. \end{cases}$$

PROOF. By [1 and 7] $T = 2m$ and $U = 2$. Therefore by Theorem 1 the above inequalities hold. Since $m > 2p$ when $r = 1$ and $m > 2$ when $r = -1$, then by [5] $h(n) > 1$. Q.E.D.

COROLLARY 4. *Let $n = m^2 + 4$ and let $h(n)$ be odd. If p is a prime which is not inert in K and $m > p$, then $h(n) > 1$, and the following bound holds*:

$$h(n) \geqslant \left(\log\sqrt{n-4}\right)/\log(p).$$

PROOF. By [1 and 7] $T = m$ and $U = 1$. Therefore, by Theorem 1, the above inequality holds. Since $m > p$, then by [5] $h(n) > 1$. Q.E.D.

COROLLARY 5. *Let $n = m^2 - 4$ and let $h(n)$ be odd. If p is a prime which is not inert in K, then the following bound holds*:

$$h(n) \geqslant \left(\log(\sqrt{n+4} - 2)\right)/\log(p).$$

PROOF. As in Corollary 4, $T = m$ and $U = 1$. The result now follows from Theorem 1. Q.E.D.

The following final consequence of Theorem 1 extends the above three results to wide R-D types.

COROLLARY 6. *Let $n = m^2 + r$, where $|r| \neq 1$ or 4, and assume $h(n)$ is odd. If p is a prime which is not inert in K, then*

$$h(n) \geqslant \frac{\log\left(\sqrt{(4nm^2/r^2) + 4} - 2\right) - \log(4m^2/r^2)}{\log(p)}.$$

PROOF. By [1 and 7] $T = (2m^2 + r)/|r|$, $U = 2m/|r|$, and $N(\varepsilon) = 1$. Therefore by Theorem 1 the above inequality holds. Q.E.D.

We have the following further result on R-D types.

THEOREM 2. *Let $n = m^2 + r > 3$ be of (wide) R-D type with $n \not\equiv 1 \pmod 4$. If $n \pm 2$ are not perfect squares when $|r| > 1$, then $h(n) > 1$.*

PROOF. If $h(n) = 1$, then, since 2 is not inert in $Q(\sqrt{n})$, there exist integers a and b such that $a^2 - nb^2 = \pm 2$ (*not* ± 8 since $n \not\equiv 1 \pmod 4$)). Assume furthermore that $a \geqslant 0$ and $b > 0$ is chosen smallest. Now, by [1 and 7] the fundamental unit of $Q(\sqrt{n})$ is

(a) $T + U\sqrt{n} = m + \sqrt{n}$ if $|r| = 1$, and

(b) $T + U\sqrt{n} = (2m^2 + r + 2m\sqrt{n})/|r|$ if $|r| \neq 1$.

In case (a) if $a^2 - nb^2 = -2$, then from [6, Theorem 108(a), pp. 206–207] it follows that $0 < b \leqslant 1/\sqrt{m-1}$, a contradiction. If $a^2 - nb^2 = 2$, then from [6, Theorem 108, pp. 205–206] we have $0 \leqslant b \leqslant 1/\sqrt{m+1}$, another contradiction. In case (b) if $a^2 - nb^2 = \pm 2$, then from [6, ibid.] we get that either

$$0 < b \leqslant \left(4m^2/(2m^2|r| + r|r| - r^2)\right)^{1/2}$$

or

$$0 \leqslant b \leqslant \left(4m^2/(2m^2|r| + r|r| + r^2)\right)^{1/2}.$$

Each instance forces $b = 1$; i.e., $n \pm 2 = a^2$, contradicting the hypothesis. Q.E.D.

The above results continue work of the author [3–5]. Table 1 illustrates Theorem 2.

Table 1

n	r	m	$h(n)$
10	1	3	2
15	−1	4	2
26	1	5	2
30	5	5	2
35	−1	6	2
39	3	6	2
42	6	6	2
78	−3	9	2
82	1	9	4
87	6	9	2
95	−5	10	2
110	10	10	2
122	1	11	2
138	6	12	2
143	−1	12	2
170	1	13	4
195	1	14	4
203	7	14	2
215	−10	15	2
219	−6	15	4
222	−3	15	2
226	1	15	8
230	5	15	2
231	6	15	4
235	10	15	6
255	1	16	4

In what follows, O_K denotes the ring of integers of $K = Q(\sqrt{n})$, and $(x + y\sqrt{n})/2^\sigma \in O_K$ is called *primitive* if g.c.d.$(2^\sigma x, 2^\sigma y) = 1$, where $\sigma = 1$ if $n \equiv 1 \pmod 4$, and $\sigma = O$ otherwise. Also ε denotes the fundamental unit of K, and (α) denotes the principal ideal generated by $\alpha \in O_K$.

THEOREM 3. *Let $n = r^2 + s^t$ be a square-free integer with $t > 1$, $s > 1$ and s odd. Suppose that $\pm s^c$ is not the norm of a primitive element of O_K for all c properly dividing t. Then t divides $h(n)$.*

PROOF. Let $s = \prod_{i=1}^m p_i^{a_i}$, where the p_i are distinct primes and the a_i are positive. It is readily seen that $p_i O_K = \mathfrak{p}_i \mathfrak{q}_i$ for distinct primes $\mathfrak{p}_i$ and $\mathfrak{q}_i$. Thus

$$((r - \sqrt{n})(r + \sqrt{n})) = \prod_{i=1}^{m} (\mathfrak{p}_i^{a_i} \mathfrak{q}_i^{a_i})^t.$$

If some $\mathfrak{p}_i$ divides both $(r - \sqrt{n})$ and $(r + \sqrt{n})$, then $2r = r + \sqrt{n} + r - \sqrt{n}$ and $4n = (r + \sqrt{n} - (r - \sqrt{n}))^2$ are in $\mathfrak{p}_i$. Hence g.c.d.$(2r, 4n) = 2$ is in $\mathfrak{p}_i$ forcing s to be even, a contradiction. Therefore, for a suitable choice of $\mathfrak{t}_i = \mathfrak{p}_i$ or $\mathfrak{q}_i$ we have that

$$(r + \sqrt{n}) = \prod_{i=1}^{m} (\mathfrak{t}_i^{a_i})^t = A^t,$$

say, is principal. Now if $g =$ g.c.d.$(t, h(n))$, then there are integers u and v such that $tu + h(n)v = g$. Hence

$$A^g = A^{tu + h(n)v} = (A^t)^u (A^{h(n)})^v$$

is principal. If $A^g = (\alpha)$, then $N(\alpha) = \pm s^g$, which implies t divides $h(n)$, by hypothesis. Q.E.D.

Theorem 3 is the real quadratic field analogue of [**5**, Theorem 2.2]. Table 2 provides an illustration of Theorem 3.

Table 2

n	r	s	t	$h(n)$
10	1	3	2	2
26	1	5	2	2
82	1	3	4	4
347	2	7	3	3
1335	2	11	3	3
6863	2	19	3	3

References

1. G. Degert, *Über die Bestimmung der Grundeinheit gewisser reell-quadratischer Zahlkorper*, Abh. Mat. Sem. Univ. Hamburg **22** (1958), 92–97.

2. H. Hasse, *Über mehrklassige, aber eingeschlechtige reell-quadratische Zahlkorper*, Elem. Math. **20** (1965), 49–59.

3. R. Mollin, *Class numbers and a generalized Fermat theorem*, J. Number Theory **16** (1983), 420–429.

4. ______, *On the cyclotomic polynomial*, J. Number Theory **17** (1983), 165–175.

5. ______, *Diophantine equations and class numbers*, J. Number Theory (to appear).

6. T. Nagell, *Introduction to number theory*, Chelsea, New York, 1964.

7. C. Richaud, *Sur la resolution des equations* $x^2 - Ay^2 = \pm 1$, Atti. Accad. Pontif. Nuovi Lincei (1866), 177–182.

8. H. Yokoi, *On real quadratic fields containing units with norm* -1, Nagoya Math. J. **33** (1968), 139–152.

9. ______, *On the fundamental unit of real quadratic fields with norm* 1, J. Number Theory **2** (1970), 106–115.

University of Calgary, Department of Mathematics and Statistics, 2500 University Drive N.W., Calgary, Alberta, Canada T2N 1N4