# Class Numbers of Quadratic Fields Determined by Solvability of Diophantine Equations

### By R. A. Mollin*

*Dedicated to Professor Dan Shanks on the occasion of his 70th birthday*

**Abstract.** In the literature there has been considerable attention given to the exploration of relationships between certain diophantine equations and class numbers of quadratic fields. In this paper we provide criteria for the insolvability of certain diophantine equations. This result is then used to determine when related real quadratic fields have class number bigger than 1. Moreover, based on criteria which we find for the solvability of a certain class of diophantine equations, we are able to determine when the class number of related imaginary quadratic fields is divisible by a given integer.

**Introduction.** The primary aim of this paper is to investigate the relationship between solvability of diophantine equations and class numbers of quadratic fields. Most such investigations into real quadratic fields in the literature deal with Richaud-Degert (R-D)-type quadratic fields (see [4] and [14]); that is, those $Q(\sqrt{n})$ where $n$ is a square-free positive integer of the form $n = l^2 + r$ with integer $l > 0$, integer $r$ dividing $4l$ and $-l < r \leqslant l$. The seminal paper in this regard is by Ankeny, Chowla, and Hasse [1]. However, many authors have studied such fields and considered generalizations thereof. Among them are: Azuhata [2], Kutsuna [8], Lang [9], Takeuchi [15], Yokoi [16]–[18], and the author [10]–[13]. In Section 1 we investigate a larger class of real quadratic fields than the (R-D)-types. We obtain conditions for the solvability of certain diophantine equations and use the result to determine nontriviality of the class numbers of these real quadratic fields. Moreover, we obtain as immediate consequences many of the above results in the literature.

The connection between solvability of certain diophantine equations and the divisibility of the class number of imaginary quadratic fields by a given integer has been given much attention. Among such inquiries are: Cowles [3], Hongwen [7], Gross and Rohrlich [5], and the author [11] and [13]. In the second section we obtain sufficient conditions for a quadratic field (real or imaginary) to have the exponent of its class group divisible by a given integer $t$. This result is most readily applied to imaginary quadratic fields upon which we focus. We provide sufficient conditions (in elementary arithmetic terms) for the exponent of the class group of certain

imaginary quadratic fields to be divisible by $t$. Furthermore, results from the literature cited above are obtained as immediate consequences.

Finally, in both sections we provide tables of examples to illustrate the above results.

**1. Real Quadratic Fields and Diophantine Equations.** First we need three preliminary lemmas. Before proceeding with these results we comment on notation and definitions which are used therein.

Let $n$ be a square-free positive integer and let $t$ be any positive integer. If $(u, v)$ is an integer solution of the diophantine equation $x^2 - ny^2 = \pm 4t$, then we say that $(u, v)$ is a *trivial solution* when $t = m^2$ and $m$ divides both $u$ and $v$. Otherwise, $(u, v)$ is called *nontrivial*. Finally, in what follows, $N$ denotes the norm from $Q(\sqrt{n})$ to $Q$.

The first lemma is a generalized Davenport-Ankeny-Hasse result which we proved in [12].

**LEMMA 1.1.** *Let $n$ be a square-free positive integer and let $t$ be any positive integer. Suppose that $(A + B\sqrt{n})/\sigma$ is the fundamental unit of $Q(\sqrt{n})$, where $\sigma = 2$ if $n \equiv 1$ (mod 4) and $\sigma = 1$ otherwise, and let $N((A + B\sqrt{n})/\sigma) = \delta$. If there is a nontrivial solution to the diophantine equation $x^2 - ny^2 = \pm \sigma^2 t$, then*

$$t \geq ((2A/\sigma) - \delta - 1)/B^2.$$

The next result is a generalized Richaud-Degert result proved in [8, Theorem 1, p. 580]. In what follows $\mathrm{sgn}(r) = r/|r|$ for an integer $r$.

**LEMMA 1.2.** *Let $n$ be a square-free positive integer and let $v$ be the least positive integer such that $v^2 n = l^2 + r$ with integer $r \in (-l, l]$ and $4l \equiv 0$ (mod $r$). Then the fundamental unit $\varepsilon_n$ of $Q(\sqrt{n})$ is of the following form:*
   (i) $\varepsilon_n = l + v\sqrt{n}$ *and* $N(\varepsilon_n) = -\mathrm{sgn}(r)$ *for* $|r| = 1$ *(except for $(n, v) = (5, 1)$).*
   (ii) $\varepsilon_n = (l + v\sqrt{n})/2$ *and* $N(\varepsilon_n) = -\mathrm{sgn}(r)$ *for* $|r| = 4$.
   (iii) $\varepsilon_n = [(2l^2 + r) + 2lv\sqrt{n}]/|r|$ *and* $N(\varepsilon_n) = 1$ *for* $|r| \neq 1$ *or* 4.

The final lemma generalizes [12, Theorem 1.1].

**LEMMA 1.3.** *Let $n$ be a square-free positive integer, $t$ any positive integer, and $v$ the least positive integer such that $v^2 n = l^2 + r$ with integer $r \in (-l, l]$ and $4l \equiv 0$ (mod $r$). If $x^2 - ny^2 = \pm \sigma^2 t$ has a nontrivial solution in integers $(x, y)$, where $\sigma = 2$ if $n \equiv 1$ (mod 4) and $\sigma = 1$ otherwise, then*
   (i) *If $r = 1$ and $(n, v) \neq (5, 1)$ then $t\sigma^2 v^2 \geq 2l$.*
   (ii) *If $r = -1$ then $tv^2 \geq 2(l - 1)$.*
   (iii) *If $r = 4$ then $tv^2 \geq l$.*
   (iv) *If $r = -4$ then $tv^2 \geq l - 2$.*
   (v) *If $|r| \neq 1$ or 4 then $t\sigma^2 v^2 \geq |r|$.*

*Proof.* Let $\delta$ be as defined in Lemma 1.1.
   (i) If $r = 1$ then $\delta = -1$. If $l$ is even then $\sigma = 2$, and if $(n, v) \neq (5, 1)$ then $A = 2l$ and $B = 2v$, by Lemma 1.2. Therefore, from Lemma 1.1 we have: $t \geq l/2v^2$; that is, $\sigma^2 v^2 t \geq 2l$. If $l$ is odd then by Lemma 1.2, $\sigma = 1$, $A = l$ and $B = v$, provided $(n, v) \neq (5, 1)$. Therefore, by Lemma 1.1: $t \geq 2l/v^2$; that is, $tv^2 \geq 2l$.

(ii) If $r = -1$ then $\sigma = \delta = 1$. By Lemma 1.2, $A = l$ and $B = v$. Therefore, by Lemma 1.1: $t \geqslant (2l - 2)/v^2$; that is, $tv^2 \geqslant 2(l - 1)$.

(iii)–(iv) If $|r| = 4$ then $\sigma = 2$, $\delta = -\text{sgn}(r)$, $A = l$ and $B = v$ by Lemma 1.2. Therefore, by Lemma 1.1: If $r = 4$ then $\delta = -1$ and $t \geqslant ((2l/2)/v^2)$; that is, $tv^2 \geqslant l$. If $r = -4$ then $\delta = 1$ and $t \geqslant ((2l/2) - 2)/v^2$; that is, $v^2 t \geqslant l - 2$.

(v) If $|r| \neq 1$ or 4 then $\delta = 1$, $A = \sigma(2l^2 + r)/|r|$, and $B = 2lv\sigma/|r|$ by Lemma 1.2. Thus from Lemma 1.1: $t \geqslant ((2\sigma(2l^2 + r)/\sigma|r|) - 2)/((4l^2v^2\sigma^2)/r^2)$. Thus: $t \geqslant (2l^2|r| + r|r| - r^2)/(2\sigma^2l^2v^2)$. If $r > 0$ then $t \geqslant r/v^2\sigma^2$; that is, $t\sigma^2v^2 \geqslant |r|$. If $r < 0$ then $t \geqslant -(l^2r + r^2)/l^2v^2\sigma^2$; that is, $t\sigma^2v^2 \geqslant -(l^2r + r^2)/l^2$. Now, if $t\sigma^2v^2 < -r - 1$ then $-r - 1 \geqslant -(l^2r + r^2)/l^2$ whence $l^2 < r^2$, contradicting the hypothesis. Hence $t\sigma^2v^2 \geqslant -r = |r|$. $\square$

Lemma 1.3 has, as immediate consequences, several results in the literature. Among these are: Ankeny, Chowla, and Hasse [1, Lemma, p. 218] and S. D. Lang [9, Lemma, p. 70].

Now we are in a position to prove the first main result which generalizes [12, Theorem 1.2].

THEOREM 1.1. *Let $n > 5$ be a square-free integer and let $v$ be the least positive integer such that $v^2n = l^2 + r$ with integer $r \in (-l, l]$ and $4l \equiv 0 \pmod{r}$ and let the following conditions be satisfied:*

(i) *$l = st$ where $s > 0$ and $t > 1$ are integers with g.c.d. $(t, r) = 1$.*

(ii) *$r$ divides $4s$ with $-2s < r \leqslant 2s$.*

(iii) *If $n \equiv 1 \pmod{4}$ then $|r| = 1$ or 4.*

(iv) *If $r = 1$ and $l$ is even then $s > 2v^2$.*

(v) *If $r = 1$ and $l$ is odd then $2s > v^2$.*

(vi) *If $r = -1$ then $tv^2 < 2(l - 1)$.*

(vii) *If $r = 4$ then $s > v^2$.*

(viii) *If $r = -4$ then $t(s - v^2) > 2$.*

(ix) *If $|r| \neq 1$ or 4 and $v > 1$ then $t > |r|$.*

*Furthermore, let $\sigma = 2$ if $n \equiv 1 \pmod{4}$ and $\sigma = 1$ otherwise. If $x^2 - ny^2 = \pm\sigma^2t$ has a nontrivial integer solution $(x, y)$, and if $(x, y) = (u_0, v_0)$ is the minimal solution (that is, $u_0 \geqslant 0$ and $v_0 > 0$ is smallest), then $|r| \notin \{1, 4\}$ and either:*

(a) *$v_0 \leqslant v^2$ and if $v_0 = v$ then $v > 1$ or*

(b) *$v_0(2 - |r|) \geqslant v^2(1 - |r|)$ if $|r| \neq 2$ and $v_0 > 1$ and*

(c) *$v > 1$ if $r = 2$ and*

(d) *either $v > 1$ or both $v_0 = 1$ and if $r = -2$ then $l = 3$.*

*In particular, if $v = 1$ then $x^2 - ny^2 = \pm\sigma^2t$ has a nontrivial solution if and only if $n = 7$ and $t = 3$; that is, $x^2 - 7y^2 = -3$ (in fact: $l = 3$, $r = -2$, $u_0 = 2$ and $v_0 = 1$).*

*Proof.* Hypotheses (iv)–(viii) imply, by Lemma 1.3(i)–(iv), that when $|r| \in \{1, 4\}$ then $x^2 - ny^2 = \pm\sigma^2t$ cannot have an integer solution. Henceforth we assume $|r| \notin \{1, 4\}$, which implies by hypothesis (iii) that $\sigma = 1$. We now prove the result by contradiction. Thus we assume

$$(1) \qquad\qquad v_0 > v^2 \quad \text{or} \quad v_0 = v = 1$$

and

$$(2) \qquad\qquad v_0(2 - |r|) < v^2(1 - |r|) \quad \text{if } |r| \neq 2 \text{ and } v_0 > 1$$

or

(3)                                  $v = 1$   if $r = 2$,

or

(4)                 $v = 1$ and either $v_0 \geqslant 2$ or $l \neq 3$   if $r = -2$.

We have $\pm tv^2 = (u_0v)^2 - (l^2 + r)v_0^2$. For the sake of convenience, we let $w = \pm tv^2$. Let $a = |u_0v - lv_0| > 0$ and $b = u_0v + lv_0 > 0$ whence $w + rv_0^2 = (u_0v - lv_0)(u_0v + lv_0)$. Set $\alpha = 1$ if $w > -rv^2$ and $\alpha = -1$ otherwise, whence $(a - 1)(b + \alpha) = ab + a\alpha - b - \alpha \geqslant 0$; that is, $ab - \alpha \geqslant b - a\alpha$. Therefore, by hypothesis (i),

$$
\begin{aligned}
0 \leqslant |w|(s - 1) = lv^2 - |w| &= \left(\left((b - \alpha a)/2v_0\right)v^2\right) - ab + \alpha rv_0^2 \\
&= \left((b - \alpha a)v^2 - 2v_0ab + 2\alpha rv_0^3\right)/2v_0 \\
&\leqslant \left((ab - \alpha)v^2 - 2v_0ab + 2\alpha rv_0^3\right)/2v_0 \\
&= -\left(\alpha\left(v^2 - 2rv_0^3\right) + ab\left(2v_0 - v^2\right)\right)/2v_0,
\end{aligned}
$$

which by (1) is less than zero if $r\alpha < 0$. Thus we assume henceforth that $r\alpha > 0$. Furthermore, from the above inequality we get

(5)                          $ab \leqslant -\alpha\left(v^2 - 2rv_0^3\right)/\left(2v_0 - v^2\right).$

Let $A = (2l^2 + r)/|r|$ and $B = 2lv/|r|$ whence $A + B\sqrt{n}$ is the fundamental unit of $Q(\sqrt{n})$ by Lemma 1.2(iii). It is straightforward to check (using the methodology of [12, Lemma 1.1] for example) that $(u_0A - nv_0B, u_0B - v_0A)$ is a nontrivial solution of $x^2 - ny^2 = w$. Therefore, by the minimality of $v_0$ we get

$$
|u_0B - v_0A| = \left|\left(2u_0lv - v_0(2l^2 + r)\right)/|r|\right| \geqslant v_0,
$$

whence either

(6)                          $2l(u_0v - v_0l) \geqslant v_0(r + |r|)$

or

(7)                          $2l(u_0v - v_0l) \leqslant v_0(r - |r|).$

*Case* I: $\alpha = -1$ *and* $r < 0$. If (6) holds then $u_0v \geqslant v_0l$. Thus,

$$
-rv_0^2 > w = (u_0v)^2 - (l^2 + r)v_0^2 \geqslant (v_0l)^2 - (l^2 + r)v_0^2 = -rv_0^2,
$$

a contradiction.

Thus (7) holds; that is, $u_0lv \leqslant v_0(l^2 + r)$. Thus,

$$
l^2w = l^2(u_0v)^2 - l^2(l^2 + r)v_0^2 \leqslant (l^2 + r)^2v_0^2 - l^2(l^2 + r)v_0^2 = r(l^2 + r)v_0^2,
$$

whence

(8)                                  $l^2w \leqslant r(l^2 + r)v_0^2.$

If $w > 0$ then by (8) we have $0 < l^2w \leqslant r(l^2 + r)v_0^2 < 0$, a contradiction. Therefore, we assume for the remainder of Case I that $w < 0$.

Assume $v_0 \geqslant -w$. Therefore, from (8),

$$
l^2v_0 \geqslant -l^2w \geqslant -r(l^2 + r)v_0^2,
$$

whence

$$
r^2v_0^2 \geqslant -l^2(1 + rv_0)v_0.
$$

Thus,

$$r^2 v_0^2 v^4 \geqslant -(lv^2)(1 + rv_0)v_0 \geqslant -w^2(1 + rv_0)v_0,$$

whence

$$w^2 \leqslant -\left[(r^2 v_0^2 v^4)/(1 + rv_0)v_0\right] < v^4(1 - r),$$

contradicting hypothesis (ix), if $v > 1$, and Lemma 1.3(v), if $v = 1$.

Now assume $v_0 v^2(-r - 1) \geqslant -w > v_0$. (Observe that, by Theorem 1.1(v), either $v_0 > 1$ or $v > 1$.) Therefore, from (8) we have

$$l^2 v^2 v_0(-r - 1) \geqslant -l^2 w \geqslant -r(l^2 + r)v_0^2,$$

whence

$$r^2 v_0^2 \geqslant l^2\left(v^2 v_0(r + 1) - rv_0^2\right).$$

Therefore,

$$r^2 v_0^2 v^4 \geqslant (lv^2)^2\left(v^2 v_0(r + 1) - rv_0^2\right) \geqslant w^2\left(v^2 v_0(r + 1) - rv_0^2\right).$$

It follows from (1) that $v^2 v_0(r + 1) - rv_0^2 > 0$. Therefore,

$$w^2 \leqslant r^2 v_0 v^4/\left(v^2(r + 1) - rv_0\right).$$

Hence by (1), $w^2 < r^2 v^4$, contradicting hypothesis (ix), if $v > 1$, and Lemma 1.3(v), if $v = 1$.

Now assume $-w > v_0 v^2(-r - 1)$. From (5) we have

$$ab \leqslant \left(v^2 - 2rv_0^3\right)/\left(2v_0 - v^2\right),$$

whence

$$-w = ab + rv_0^2 \leqslant \left[\left(v^2 - 2rv_0^3\right)/\left(2v_0 - v^2\right)\right] + rv_0^2$$
$$= v^2\left(1 - rv_0^2\right)/\left(2v_0 - v^2\right).$$

Thus,

$$(9) \quad -w \leqslant v_0 v^2(-r - 1) + \left(v_0^2(r + 2)v^2 - v_0(r + 1)v^4 + v^2\right)/\left(2v_0 - v^2\right).$$

If $v_0 > 1$ and $r \neq -2$ then by (2), $v_0(r + 2) < (r + 1)v^2$, whence by (1),

$$v_0^2(r + 2)v^2 - v_0(r + 1)v^4 + v^2 < v^2 < v_0 < 2v_0 - v^2.$$

Therefore, from (9) we may conclude

$$v_0 v^2(-r - 1) < -w < v_0 v^2(-r - 1) + 1,$$

a contradiction. Hence $v_0 = 1$ or $r = -2$.

If $v_0 = 1$ then by (1), $v = 1$. If $r \neq -2$ then from (9), $-r - 1 < -w \leqslant -r + 1$. By hypothesis (i), $-w \neq -r$, whence $-w = t = -r + 1$. Therefore $u_0^2 - n = r - 1$; that is, $u_0^2 - l^2 = 2r - 1$. Recall that $u_0 + l = b > 0$ and $l - u_0 = a > 0$. Thus $-r = (ab - 1)/2$ and $s = (a + b)/(ab + 1)$. By hypothesis (ii), $(4s/(-r))$ must be an integer; that is, $8(a + b)/((ab)^2 - 1)$ is an integer. In particular, we must have $8(a + b) \geqslant (ab)^2 - 1$. Since $b > a$ then $16b > 8(a + b) \geqslant (ab)^2 - 1$; that is, $1 > b(a^2 b - 16)$, whence $a = 1$ and $b \leqslant 16$, since $a$ and $b$ are odd. Therefore $b \in S = \{3, 5, 7, 9, 11, 13, 15\}$. It is easy to check that $8(a + b)/((ab)^2 - 1)$ is an integer for only $b = 3, 5$ or $9$ of $S$. If $b = 9$ then $r = -4$, a contradiction. If $b = 5$ then $r = -2$, contradicting our assumption. If $b = 3$ then $r = -1$, a contradiction.

Now if $v_0 = 1$ and $r = -2$ then $v = 1$ and $l \neq 3$ by (4). By (9), $1 < -w \leqslant 3$. Therefore, by hypothesis (i), $t = 3$, whence $u_0^2 - l^2 = -5$, forcing $l = 3$, a contradiction. Hence $v_0 \geqslant 2$ and $r = -2$. Therefore, by (4), $v = 1$. By (9),

$$v_0 < -w \leqslant (2v_0 + 1)/(2v_0 - 1) < 2,$$

a contradiction.

*Case* II: $\alpha = 1$ *and* $r > 0$. If (7) holds then $u_0 v \leqslant v_0 l$. Therefore,

$$-rv^2 < w = (u_0 v)^2 - (l^2 + r)v_0^2 \leqslant (v_0 l)^2 - (l^2 + r)v_0^2 = -rv_0^2,$$

a contradiction. Hence (6) holds; that is, $u_0 v l \geqslant v_0(l^2 + r)$. Thus,

$$l^2 w = (l u_0 v)^2 - l^2(l^2 + r)v_0^2 \geqslant v_0^2(l^2 + r^2) - l^2(l^2 + r)v_0^2$$

$$= r(l^2 + r)v_0^2.$$

Hence,

(10)                             $$l^2 w \geqslant r(l^2 + r)v_0^2.$$

If $w < 0$ then $0 > l^2 w \geqslant r(l^2 + r)v_0^2 > 0$, a contradiction. Henceforth, $w > 0$. From (5),

$$ab \leqslant (2rv_0^3 - v^2)/(2v_0 - v^2).$$

Thus,

$$w = ab - rv_0^2 \leqslant \left[(2rv_0^3 - v^2)/(2v_0 - v^2)\right] - rv_0^2$$

$$= v^2(rv_0^2 - 1)/(2v_0 - v^2)$$

$$= v^2(r - 1)v_0 + (v_0^2(2 - r)v^2 + v_0(r - 1)v^4 - v^2)/(2v_0 - v^2).$$

By (1)–(3),

$$(v_0^2(2 - r)v^2 + v_0(r - 1)v^4 - v^2)/(2v_0 - v^2) < 1.$$

If $w > v^2(r - 1)v_0$ then $v^2(r - 1)v_0 < w < v^2(r - 1)v_0 + 1$, a contradiction. Hence, $0 < w < v^2(r - 1)v_0$; that is, $v_0 > w/(r - 1)v^2 > 0$. Thus from (10),

$$l^2 w \geqslant r(l^2 + r)v_0^2 > (r(l^2 + r)v_0 w)/(r - 1)v^2 > (l^2 + r)w,$$

where the last inequality follows from (1). However, $r > 0$, so we have a contradiction. $\square$

An immediate consequence of Theorem 1.1 is Yokoi [16, Theorem 2, p. 153].

We now apply Theorem 1.1 to the determination of nontrivial class numbers of real quadratic fields. The following result generalizes [12, Theorem 2.1].

THEOREM 1.2. *Let $n > 7$ be a square-free integer and let $v$ be the least positive integer such that $v^2 n = l^2 + r$, where either $v = 1$ and $r \in (-l, l]$, $4l \equiv 0 \pmod{r}$ and $n \not\equiv 1 \pmod 4$, or $|r| = 1, 4$. Let $q$ be a prime dividing $l$ such that: if $r = 1$ and $l$ is even then $l > 2qv^2$; if $r = 1$ and $l$ is odd then $2l > v^2 q$; if $r = -1$ then $qv^2 < 2(l - 1)$; if $r = 4$ then $l > qv^2$; and if $r = -4$ then $l > 2 + qv^2$. Then $h(n) > 1$ if any of the following conditions hold*:

(i) g.c.d.$(q, r) = 1$, $q > 2$ *and* $(r/q) = 1$, *where $(\ /\ )$ denotes the Legendre symbol*.

(ii) $q = 2$ *and* $r \neq 1$ *is odd.*

(iii) $q = 2$, $r = 1$ *and* $l \equiv 0 \pmod 4$.

(iv) $q$ *divides* $r$ *and* $|r| > q$.

(v) $|r| = q > 2$.

*Proof.* If $v = 1$ then the result is [12, Theorem 2.1]. If $v \neq 1$ then $|r| = 1$ or $4$ by hypothesis. Suppose $h(n) = 1$. Therefore, there exist integers $(x, y)$ such that:

(a) In cases (i) and (iii), $x^2 - ny^2 = \pm \sigma^2 q$, where $\sigma = 2$ if $n \equiv 1 \pmod 4$ and $\sigma = 1$ otherwise, since $q$ splits in $Q(\sqrt{n})$.

(b) In case (ii) with $r = -1$, $x^2 - ny^2 = \pm 2$, since 2 ramifies in $Q(\sqrt{n})$.

(a)–(b) contradict Theorem 1.1. □

The following table provides an application of Theorem 1.2. The entries are all of the integers less than 100 available by this method. Note that of the 22 integers $n$ less than 100 with $h(n) > 1$ we miss only four by this method, namely 55, 66, 70, and 91.

TABLE 1.1

| $v$ | $l$ | $r$ | $n$ | $h(n)$ |
|---|---|---|---|---|
| 1 | 3 | 1 | 10 | 2 |
| 1 | 4 | −1 | 15 | 2 |
| 1 | 5 | 1 | 26 | 2 |
| 1 | 5 | 5 | 30 | 2 |
| 1 | 6 | −2 | 34 | 2 |
| 1 | 6 | −1 | 35 | 2 |
| 1 | 6 | 3 | 39 | 2 |
| 1 | 6 | 6 | 42 | 2 |
| 1 | 7 | 2 | 51 | 2 |
| 13 | 99 | 1 | 58 | 2 |
| 1 | 8 | 1 | 65 | 2 |
| 5 | 43 | 1 | 74 | 2 |
| 1 | 9 | −3 | 78 | 2 |
| 1 | 9 | −2 | 79 | 3 |
| 1 | 9 | 1 | 82 | 4 |
| 1 | 9 | 4 | 85 | 2 |
| 1 | 9 | 6 | 87 | 2 |
| 1 | 10 | −5 | 95 | 2 |

**2. Imaginary Quadratic Fields and Diophantine Equations.** The first main result actually holds for *real or* imaginary quadratic fields. However, the theorem is more readily applied to imaginary quadratic fields as its corollary illustrates. Moreover, the following generalizes [11, Theorems 2.1 and 2.2]. In what follows, $\mathscr{C}_K$ denotes the class group of $K = Q(\sqrt{n})$. Moreover, by a *primitive element* $(x + y\sqrt{n}) \in \mathscr{O}_K$, the ring of integers of $K$, we mean that g.c.d.$(\sigma x, \sigma y) = \sigma$, where $\sigma = 2$ if $n \equiv 1 \pmod 4$ and $\sigma = 1$ otherwise. Finally, for a prime $p$ and an integer $m$, $p^a = |m|_p$ denotes the fact that $p^a$ divides $m$ but $p^{a+1}$ does not.

THEOREM 2.1. *Let $n$ be a square-free integer and let $m > 1$, $t > 1$ be integers such that*

(i) $\pm m^t$ *is the norm of a primitive element from* $K = Q(\sqrt{n})$;

(ii) $\pm m^c$ is not the norm of a primitive element from $K$ for all $c$ properly dividing $t$, and

(iii) if $t = |m|_2 = 2$ then $n \equiv 1 \pmod 8$.

Then $t$ divides the exponent of $\mathscr{C}_K$.

*Proof.* By (i) there are relatively prime integers $x_0$ and $y_0$ such that $x_0^2 - ny_0^2 = \pm \sigma^2 m^t$, where $\sigma = 2$ if $n \equiv 1 \pmod 4$ and $\sigma = 1$ otherwise. Let $m = p_1^{a_1} \cdots p_r^{a_r}$, where the $p_i$'s are distinct rational primes and the $a_i$'s are positive integers. We claim that $p_i \mathscr{O}_K = \mathscr{P}_i \mathscr{Q}_i$ for distinct $\mathscr{O}_K$-primes $\mathscr{P}_i$ and $\mathscr{Q}_i$ with $i \in \{1, \ldots, r\}$. If $p_i > 2$, then $(n/p_i) = (ny_0^2/p_i) = (x_0^2 - \sigma^2 m^t/p_i) = (x_0^2/p_i) = 1$. If $p_i = 2$, then by hypothesis (iii), $n \equiv 1 \pmod 8$, and the claim follows.

Note that if $z_1 = [x_0 + y_0\sqrt{n}]/\sigma$ and $z_2 = [x_0 - y_0\sqrt{n}]/\sigma$, then

$$(m)^t = (z_1)(z_2) = [\mathscr{P}_1^{a_1}\mathscr{Q}_1^{a_1}]^t \cdots [\mathscr{P}_s^{a_s}\mathscr{Q}_s^{a_s}]^t.$$

Now, if $\mathscr{P}_i$ divides both $z_1$ and $z_2$, then $z_1 + z_2 = x_0$ and $(z_1 - z_2)^2 = y_0^2 n$ are in $\mathscr{P}_i$. However, g.c.d.$(x_0, n) = 1$, since $t > 1$ and $n$ is square-free. Moreover, g.c.d.$(x_0, y_0) = 1$, whence $1 \in \mathscr{P}_i$, a contradiction. Hence, for a suitable choice of $\mathscr{R}_i = \mathscr{P}_i$ or $\mathscr{Q}_i$ we have $([x + y\sqrt{n}]/\sigma) = (\mathscr{R}_1^{a_1} \cdots \mathscr{R}_s^{a_s})^t = \mathscr{A}^t$, say. Let $g = $ g.c.d.$(t, h(n))$. Then there are integers $u$ and $v$ such that $tu + h(n)v = g$. Hence $\mathscr{A}^g = \mathscr{A}^{tu + h(n)v} = (\mathscr{A}^t)^u (\mathscr{A}^{h(n)})^v$ is principal. Therefore, $\mathscr{A}^g$ yields a primitive element of which $\pm m^g$ must be a norm. By (ii), $g = t$; that is, $\mathscr{A}$ is an element of order $t$ in $\mathscr{C}_K$, so $t$ divides the exponent of $\mathscr{C}_K$.  □

An immediate consequence of Theorem 2.1 is Cowles [3, Theorem, p. 113].

The following is an application of Theorem 2.1 to imaginary quadratic fields and generalizes [11, Corollaries 2.4 and 2.6].

COROLLARY 2.1. *Let $n$ be a square-free negative integer and $m > 1$, $t > 1$ any integers such that $m^t$ is the norm of a primitive element of $Q(\sqrt{n})$. Let $x_0^2 - ny_0^2 = \sigma^2 m^t$ (with $\sigma = 2$ if $n \equiv 1 \pmod 4$ and $\sigma = 1$ otherwise) be a solution such that the following conditions are satisfied:*

(1) $x_0^2 \leqslant \sigma^2 m^{t-1}(m - 1)$.

(2) $y_0 \leqslant b$ *for all positive integers $b$ which satisfy $nb^2 = a^2 - 4m^c$ for some $c$ properly dividing $t$ and some integer $a > 0$ relatively prime to $b$.*

(3) *If $t = |m|_2 = 2$ then $n \equiv 1 \pmod 8$.*

*Then $t$ divides the exponent of $C_K$.*

*Proof.* Suppose there is a proper divisor $c$ of $t$ and relatively prime integers $a$ and $b$ such that $4m^c = a^2 - nb^2$. Therefore, $4m^c > -nb^2 = -(x_0^2 - 4m^t)b^2/y_0^2$, whence

$$(y_0^2/b^2 m^{t-c-1}) + (x_0^2/4m^{t-1}) > m.$$

However, $(x_0^2/4m^{t-1}) \leqslant (x_0^2/m^{t-1}\sigma^2) \leqslant m - 1$ and $y_0^2/b^2 \leqslant 1$ by (2), whence $y_0^2/b_0^2 m^{t-c-1} \leqslant 1/m^{t-c-1} \leqslant 1$. Therefore,

$$1 + (m - 1) \geqslant (y_0^2/b^2 m^{t-c-1}) + (x_0^2/\sigma^2 m^{t-1}) > m,$$

a contradiction.  □

Immediate consequences of Corollary 2.1 are Gross and Rohrlich [5, Theorem 5.3, p. 222] and Hongwen [7, Theorem 6, p. 1277]. Both of the above dealt only with the case $x_0 = y_0 = 1$.

The following table illustrates Corollary 2.1 by providing 15 examples of certain values available by this method. Note that for $y_0 = 1$, condition (2) of Corollary 2.1 is vacuous, and in fact for small values of $y_0$ the result is easy to apply. Few values of $n$ are unavailable by this method.

TABLE 2.1

| $x$ | $y$ | $m$ | $t$ | $\sigma$ | $-n$ | $h(n)$ |
|-----|-----|-----|-----|----------|------|--------|
| 3 | 2 | 7 | 2 | 1 | 10 | 2 |
| 5 | 2 | 3 | 4 | 1 | 14 | 4 |
| 1 | 1 | 2 | 2 | 2 | 15 | 2 |
| 2 | 1 | 5 | 2 | 1 | 21 | 4 |
| 9 | 2 | 13 | 2 | 1 | 22 | 2 |
| 29 | 1 | 6 | 3 | 2 | 23 | 3 |
| 1 | 1 | 2 | 3 | 2 | 31 | 3 |
| 8 | 2 | 14 | 2 | 1 | 33 | 4 |
| 1 | 1 | 3 | 2 | 2 | 35 | 2 |
| 9 | 1 | 2 | 5 | 2 | 47 | 5 |
| 2 | 1 | 3 | 4 | 1 | 77 | 8 |
| 7 | 1 | 2 | 5 | 2 | 79 | 5 |
| 13 | 1 | 8 | 2 | 2 | 87 | 6 |
| 3 | 1 | 5 | 2 | 2 | 91 | 2 |
| 7 | 1 | 6 | 2 | 2 | 95 | 8 |

All values in the above table are taken from "Groupe des classes des corps quadratiques imaginaires $Q(\sqrt{-a})$, $a < 10,000$" by Bernard Oriat of Faculté des Sciences de Besançon.

Department of Mathematics and Statistics
University of Calgary
Calgary, Alberta, Canada T2N 1N4

1. N. C. ANKENY, S. CHOWLA & H. HASSE, "On the class number of the maximal real subfield of a cyclotomic field," *J. Reine Angew. Math.*, v. 217, 1965, pp. 217–220.

2. T. AZUHATA, "On the fundamental units and the class numbers of real quadratic fields," *Nagoya Math. J.*, v. 95, 1984, pp. 125–135.

3. M. J. COWLES, "On the divisibility of the class number of imaginary quadratic fields," *J. Number Theory*, v. 12, 1980, pp. 113–115.

4. G. DEGERT, "Über die Bestimmung der Grundeinheit gewisser reell-quadratischer Zahlkörper," *Abh. Math. Sem. Univ. Hamburg*, v. 22, 1958, pp. 92–97.

5. B. H. GROSS & D. E. ROHRLICH, "Some results on the Mordell-Weil group of the Jacobian of the Fermat curve," *Invent. Math.*, v. 44, 1978, pp. 201–224.

6. H. HASSE, "Über mehrklassige aber eingeschlechtige reell-quadratische Zahlkörper," *Elem. Math.*, v. 20, 1965, pp. 49–59.

7. LU HONGWEN, "The continued fractions, class number and the others," *Sci. Sinica Ser. A*, v. 26, 1983, pp. 1275–1284.

8. M. KUTSUNA, "On the fundamental units of real quadratic fields," *Proc. Japan Acad. Sci.*, v. 50, 1974, pp. 580–583.

9. S. D. LANG, "Note on the class number of the maximal real subfield of a cyclotomic field," *J. Reine Angew. Math.*, v. 290, 1977, pp. 70–72.

10. R. A. MOLLIN, "Lower bounds for class numbers of real quadratic fields," *Proc. Amer. Math. Soc.*, v. 96, 1986, pp. 545–550.

11. R. A. MOLLIN, "Diophantine equations and class numbers," *J. Number Theory*, v. 24, 1986, pp. 7–19.

12. R. A. MOLLIN, "On the insolubility of a class of diophantine equations and the nontriviality of the class numbers of related real quadratic fields of Richaud-Degert type," *Nagoya Math. J.* (To appear.)

13. R. A. MOLLIN, "On class numbers of quadratic extensions of algebraic number fields," *Proc. Japan Acad. Ser. A Math. Sci.*, v. 62, 1986, pp. 33–36.

14. C. RICHAUD, "Sur la résolution des équations $x^2 - Ay^2 = \pm 1$," *Atti Accad. Pontif. Nuovi Lincei*, 1866, pp. 177–182.

15. H. TAKEUCHI, "On the class-number of the maximal real subfield of a cyclotomic field," *Canad. J. Math.*, v. 33, 1981, pp. 55–58.

16. H. YOKOI, "On the diophantine equation $x^2 - py^2 = \pm 4q$ and the class number of real subfields of a cyclotomic field," *Nagoya Math. J.*, v. 91, 1983, pp. 151–161.

17. H. YOKOI, "On real quadratic fields containing units with norm −1," *Nagoya Math. J.*, v. 33, 1968, pp. 139–152.

18. H. YOKOI, "On the fundamental unit of real quadratic fields with norm 1," *J. Number Theory*, v. 2, 1970, pp. 106–115.