44. Class Number One Criteria for Real Quadratic Fields. II

By R. A. MOLLIN
Mathematics Department, University of Calgary,
Calgary, Alberta, Canada, T2N 1N4

(Communicated by Shokichi IYANAGA, M. J. A., May 12, 1987)

This paper continues the work begun in [6]. Therein we gave criteria for real quadratic fields of narrow Richaud-Degert (R-D) type to have class number one. This was a consequence of more general criteria given for real quadratic fields $Q(\sqrt{n})$ with $n\equiv 1 \pmod 4$.

Herein we will deal with positive square-free integers n of wide (R-D) type; i.e., $n=m^2+r$ where r divides $4m$ and $r\in(-m, m]$ with $|r|\neq 1, 4$. The first result generalizes results in [1], [3], [4], [9] and [11].

Theorem 1. *Let $n=l^2+r>7$ be of wide R-D type such that $n\not\equiv 1 \pmod 4$. If $h(n)=1$ then:*

(1) $|r|=2$.

(2) *p is inert in $Q(\sqrt{n})$ for all odd primes p dividing l.*

(3) *If $r=2$ then $l\equiv 0 \pmod 3$.*

(4) *If $r=-2$ then $l\not\equiv 0 \pmod 3$.*

Proof. Since $n\not\equiv 1 \pmod 4$ then 2 is ramified in $Q(\sqrt{n})$. Therefore, there are integers x and y such that $x^2-ny^2=\pm 2$. By [5, Theorem 1.1] $2\geq|r|$; where $|r|=2$ since $|r|\neq 1$ by hypothesis. This secures (1). If p is an odd prime dividing l such that p is not inert in $Q(\sqrt{n})$ then there are integers u and v such that $u^2-nv^2=\pm p$. By [5, Theorem 1.2] $n=7$ and $p=3$ are forced. This secures (2).

If 3 is not inert in $Q(\sqrt{n})$ then $x^2-ny^2=\pm 3$ for some integers x and y. Assume that $x>0$ and that $y>0$ is the *least* positive solution. Thus we may invoke [7, Theorem 108–108a, pp. 205–207] to get that if $x^2-ny^2=3$ then; for $x_1=(2l^2+r)/|r|$ and $y_1=2l/|r|$ (see [2] and [8]):

(i) $0\leq y\leq y_1\sqrt{3}/\sqrt{2(x_1+1)}$

and if $x^2-ny^2=-3$ then:

(ii) $0<y\leq y_1\sqrt{3}/\sqrt{2(x_1-1)}$.

A tedious check shows that $y=1$.

Therefore $x^2-n=\pm 3$; i.e., $x^2-l^2=r\pm 3$. An easy check shows that the only possible solutions to the latter equation occur when either $l=r=2$ or $l=3$, and $r=-2$. Thus, if $n>6$ when $r=2$, and $n>7$ when $r=-2$ then 3 is inert in $Q(\sqrt{n})$; whence $n\equiv 2 \pmod 3$. Therefore, $l\equiv 0 \pmod 3$ if $r=2$, and $l\not\equiv 0 \pmod 3$ if $r=-2$. This secures (3), (4) and the theorem. Q.E.D.

Remark 1. The converse of Theorem 1 is false. For example, if $n=12^2+2=146$ then Theorem 1 (1)–(3) are satisfied, but $h(n)=2$.

The following Table illustrates Theorem 1.

Table

l	r	n	$h(n)$
2	2	6	1
3	2	11	1
6	2	38	1
9	2	83	1
12	2	146	2
15	2	227	1
18	2	326	3
315	2	99227	18
3	-2	7	1
4	-2	14	1
5	-2	23	1
7	-2	47	1
8	-2	62	1
11	-2	119	2
13	-2	194	2
20	-2	398	1
316	-2	99854	21

All class numbers are taken from [10].

Theorem 2. *Let $n=l^2+r$ be of R-D type with $r\mid 2l$, and $n\equiv 1 \pmod 4$. If $h(n)=1$ then:*

(1) *If $n\equiv 1 \pmod 8$ then $n=33$.*

(2) *If $n\equiv 5 \pmod 8$ then $r<0$, $-r$ is a prime and p is inert in $Q(\sqrt{n})$ for all primes $p<|r|/4$.*

Proof. If $n\equiv 1 \pmod 8$ then 2 splits in $Q(\sqrt{n})$. Thus there are integers a and b such that $a^2-nb^2=\pm 8$.

By [5, Theorem 1.1] $|r|\le 8$. Also, using [7, Theorems 108–108a, pp. 205–207] we may achieve that $b=1$ by the same reasoning as in the proof of Theorem 1. Hence $a^2-l^2=r\pm 8$ where $|r|\le 8$. However, $n\equiv 1 \pmod 8$ and $|r|\ne 1, 4$. Therefore, $r\in\{-7, -3, 5\}$. An easy check of $a^2-l^2=r\pm 8$ for these values of r yields that the only solution is $l=6$ and $r=-3$; i.e., $n=33$.

Suppose that $n\equiv 5 \pmod 8$. If $|r|$ is not prime then there exists a prime p dividing $|r|$ such that $2<p<|r|$ and p is ramified in $Q(\sqrt{n})$. Therefore, there are integers c and d with $c^2-nd^2=\pm 4p$; whence $4p\ge |r|$ by [5, Theorem 1.1]. Hence, $|r|=2p$, $3p$ or $4p$. Either even case contradicts that $n\equiv 5 \pmod 8$. For the $|r|=3p$ case we note that it is well-known that if $h(n)=1$ then $n=s$ or pq where s, p and q are primes such that either $p=2$ and $q\equiv 3 \pmod 4$ or $p\equiv q\equiv 3 \pmod 4$, (e.g., see [5]). Thus $|r|=3p$ implies that n is a product of more than two primes. Hence $|r|$ is a prime. Moreover $|r|\equiv 3 \pmod 4$ and $(l^2+r)/|r|\equiv 3 \pmod 4$ is prime. If $r>0$ then $l^2\equiv 2r$

(mod 4) forcing r to be even, a contradiction. Thus $r<0$.

If $p<|r|/4$ is a prime which is not inert in $Q(\sqrt{n})$, then there are integers e and f such that $e^2-nf^2=\pm 4p$ with $|r|>4p$. This contradicts [5, Theorem 1.1]. This secures the theorem. Q.E.D.

Two examples which illustrate Theorem 2 (2) are $n=141=12^2-3$ and $n=1757=42^2-7$ for which $h(n)=1$.

Acknowledgement. The research in this paper was supported by both N.S.E.R.C. Canada Grant #A8484 and an I. W. Killam Award held at the University of Calgary in 1986.

References

[1] T. Azuhata: On the fundamental units and the class numbers of real quadratic fields. Nagoya Math. J., **95**, 123–135 (1984).
[2] G. Degert: Über die Bestimmung der Grundeinheit gewisser reell-quadratischer Zahlkörper. Abh. Math. Sem. Univ. Hamburg, **22**, 92–97 (1958).
[3] S. Louboutin: Critères des principalité et minoration des nombres de classes d'idéaux des corps quadratiques réels à l'aide de la théorie des fractions continues (preprint).
[4] R. A. Mollin: Diophantine equations and class numbers. J. Number Theory, **24**, 7–19 (1986).
[5] ——: 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 (to appear in Nagoya Math. J.).
[6] ——: Class number one criteria for real quadratic fields. I. Proc. Japan Acad., **63**A, 121–125 (1987).
[7] T. Nagell: Introduction to number theory. Chelsea, New York (1964).
[8] C. Richaud: Sur la résolution des équations $x^2-Ay^2=\pm 1$. Atti. Accad. Pontif. Nuovi Lincei, 177–182 (1866).
[9] R. Sasaki: Generalized Ono invariant and Rabinowich's theorem for real quadratic fields (preprint).
[10] H. Wada: A table of ideal class numbers of real quadratic fields. Kokyuroku in Math., **10**, Sophia University, Tokyo (1981).
[11] H. Yokoi: Class-number one problem for certain kinds of real quadratic fields. Nagoya University (1986) (preprint series #7).