

Handwritten signature

Applications of a new class number two criterion for real quadratic fields

R.A. Mollin *

Abstract. The primary purpose of this paper is to provide a real quadratic field analogue of the well-known Hendy criterion for class number 2 of complex quadratic fields in terms of prime-producing quadratic polynomials. We do this for real quadratic fields of Extended-Richard-Degert (ERD)-type. Examples are provided as well as an explicit determination of all ERD-types $d \equiv 1 \pmod{8}$ with class number $h(d) = 2$. We also provide, for what are called narrow ERD-types, a general class number criterion which allows us to determine an algorithm for listing all $d = 4m^2 + 1$ of a given class number, (for even m). Finally, we provide a general condition on arbitrary square-free d for $h(d)$ to be less than or equal to 2 in terms of prime producing quadratic polynomials. This continues work in [3] - [13].

1 Notation and preliminaries

Throughout d will be a positive square-free integer. Let $[\alpha, \beta]$ be the module $\{\alpha x + \beta y : x, y \in \mathbb{Z}\}$. Note that the ring of integers \mathcal{O}_K of a quadratic field $K = \mathbb{Q}(\sqrt{d})$ is $[1, w]$ where

$$w = (\sigma - 1 + \sqrt{d})/\sigma \text{ with } \sigma = \begin{cases} 2, & \text{if } d \equiv 1 \pmod{4}, \\ 1, & \text{if } d \not\equiv 1 \pmod{4}. \end{cases}$$

The discriminant Δ of K is $(w - \bar{w})^2 = 4d/\sigma^2$, and the absolute norm of α is $N(\alpha) = \alpha\bar{\alpha}$ where $\bar{\alpha}$ is the algebraic conjugate of α . Details and proofs of the following remarks can be found in [14], (also see the elucidation in [13]).

Remark 1.1. If I is an ideal of \mathcal{O}_K (not contained in \mathbb{Z}), then $I = [a, b+cw]$ where $a, b, c \in \mathbb{Z}, a > 0, c > 0, c \mid b, c \mid a$ and $ac \mid N(b+cw)$. For a given I in \mathcal{O}_K a and c are unique and a is the least positive rational integer in I , denoted $L(I) = a$. Also let $ca = N(I) = \text{norm of } I$. If $I = (\alpha)$, principal, then $N(I) = |N(\alpha)|$. If $I \sim J$ then there is a $\gamma \in I$ such that $(\gamma)J = (L(J))I$. Here \sim denotes equivalence of ideals in the class group.

*The author gratefully acknowledges the financial support of N.S.E.R.C. Canada grant number A8484.

An ideal I is said to be *primitive* if $L(I) = N(I)$; i.e., $c = 1$. I is called a *reduced ideal* in \mathcal{O}_K if I is primitive and there does *not* exist a non-zero $\alpha \in I$ such that both $|\alpha| < L(I)$ and $|\bar{\alpha}| < L(I)$ hold.

Remark 1.2. If I is an ideal of \mathcal{O}_K then there is at least one *reduced* ideal J with $I \sim J$. If I is an ideal of \mathcal{O}_K then there is at least one *primitive* ideal J with $I \sim J$.

If I is a reduced ideal in \mathcal{O}_K then $L(I) < \sqrt{\Delta}$. If I is a primitive ideal in \mathcal{O}_K and $L(I) < \sqrt{\Delta}/2$ then I is reduced in \mathcal{O}_K .

Remark 1.3. Let $I = [N(I), b+w]$ be primitive then the expansion of $(b+w)/N(I)$ as a continued fraction proceeds as follows

$$(P_0, Q_0) = \begin{cases} (b, N(I)), & \text{if } d \not\equiv 1 \pmod{4}, \\ (2b+1, 2N(I)), & \text{if } d \equiv 1 \pmod{4}. \end{cases}$$

and, recursively for $i = 0, 1, \dots$ $d = P_{i+1}^2 + Q_i Q_{i+1}$, $P_{i+1} = a_i Q_i - P_i$ where $a_i = [(P_i + \sqrt{d})/Q_i]$ with $[\]$ being the greatest integer function.

Thus $1 \leq Q_i < 2\sqrt{d}$ and $1 \leq P_i < \sqrt{d}$ for $1 \leq i \leq k$. Let $a = a_0$ then $(b+w)/N(I) = \langle a, \overline{a_1, a_2, \dots, a_k} \rangle$ as a continued fraction of *period* length k .

Remark 1.4. Let $I = [N(I), b+w_0]$ be reduced then the expansion of $(b+w)/N(I)$ into a continued fraction yields *all* of the reduced ideals in \mathcal{O}_K equivalent to I ; i.e.,

$$I_1 = [Q_0/\sigma, (P_0 + \sqrt{d})/\sigma] = I \sim I_2 = [Q_1/\sigma, (P_1 + \sqrt{d})/\sigma] \sim \dots \sim I_k = [Q_{k-1}/\sigma, (P_{k-1} + \sqrt{d})/\sigma].$$

Thus the $(P_i + \sqrt{d})/Q_i$ are complete quotients in the continued fraction expansion of $(b+w)/N(I)$ and the Q_i/σ 's represent *norms* of all reduced ideals equivalent to I .

2 Reduced ideals, continued fractions and $h(d) = 2$

The development in Section 1 suggests the following generalization of [2] Proposition 2, p.169.

Proposition 2.1. Let $I = [N(I), b+w]$ be a reduced ideal in \mathcal{O}_K .

- (a) If J is also reduced and $I \sim J$ then $N(J) = Q_i/\sigma$ for some i with $1 \leq i \leq k$, where the Q_i 's appear in the continued fraction expansion of $(b+w)/N(I)$.
- (b) If J and \bar{J} are the only ideals of Norm $N(J)$, where J is reduced, and $N(J) = Q_i/\sigma$ for some i with $1 \leq i \leq k$ in the continued fraction expansion of $(b+w)/N(I)$ then either $J \sim I$ or $\bar{J} \sim I$.

Remark 2.1. To get Louboutin's result [ibid] we merely take I to be in the principal class in which case $N(I) = 1$ and $b = 0$; whence, if J and \bar{J} are the only ideals of norms $N(J)$ then $J \sim 1$ if and only if $N(J) = Q_i/\sigma$ for some i with $1 \leq i \leq k$ in the continued fraction expansion of w .

Now we would like to find criteria for $h(d) = 2$ in terms of the factorization of certain quadratic polynomials much in the same way as Hendy [1] accomplished the task for complex quadratic fields of class number 2. It turns out, that we can use Proposition 2.1 to explicitly do this for ERD types.

3 Quadratic polynomials, class number 2 and ERD types

In [1] Hendy provided necessary and sufficient conditions for $h(-d) = 2$ in terms of prime-producing quadratic polynomials. It is the goal of this section to provide such criteria for $h(d) = 2$ when d is of ERD-type; i.e., $d = \ell^2 + r$ where $4\ell \equiv 0 \pmod{r}$. Let

$$f_d(x) = \begin{cases} -x^2 + x + \frac{d-1}{4}, & \text{if } d \equiv 1 \pmod{4}, \\ -x^2 + d, & \text{if } d \equiv 2, 3 \pmod{4}. \end{cases}$$

Consider a reduced ideal $I = [N(I), -b + w]$ then we have $f_d(b) = -N(w - b)$. Thus the $f_d(x)$ is our canonical choice of a *norm-induced* polynomial which we will use to give an analogue of the aforementioned result of Hendy [1]. First we deal with the case where $d \equiv 2, 3 \pmod{4}$.

Theorem 3.1. *Let $d \not\equiv 1 \pmod{4}$, $d > 3$ be of ERD type $d = \ell^2 + r$ and assume that d cannot be written in the form $d = m^2 \pm 2$. Then $h(d) = 2$ if and only if (for $1 \leq x \leq \ell$) $d - x^2$ is*

- (i) *(for $|r|$ odd) prime, twice a prime, $|r|$ times a prime, $2|r|$ times a prime, or the product of two primes $(\ell + (r-1)/2)(\ell - (r-1)/2)$ which occurs at $|r+1|/2$, and $|r|$ is prime or 1.*
- (ii) *(for $|r|$ even) prime, twice a prime, $|r|/2$ times a prime or $|r|$ times a prime and $|r|/2$ is prime. Moreover, if $r < 0$ then additionally $(r+4\ell-4)/2$ times a prime where $(r+4\ell-4)$ is prime.*

Proof. First assume that $h(d) = 2$. Let

$$\alpha = \begin{cases} 1, & \text{if } d \equiv 3 \pmod{4}, \\ 0, & \text{if } d \equiv 2 \pmod{4}. \end{cases}$$

We will first calculate, for each case, the continued fraction expansion of both \sqrt{d} and $(\sqrt{d} + \alpha)/2$, and then analyze the factorization of $d - x^2$ for each case. Note that the ideal $J = [2, \alpha + \sqrt{d}]$ above 2 is not principal since $|r| \neq 2$ (where we invoke Proposition 2.1 and an examination of the continued fraction expansion of \sqrt{d} given below). Observe that $[\sqrt{d}] = \ell$ or $\ell - 1$. Thus we have

CASE I. $|r|$ odd.CASE I(A). $[\sqrt{d}] = \ell$, (whence $r > 0$). The continued fraction expansion of \sqrt{d} is then represented by

i	0	1	2
P_i	0	ℓ	ℓ
Q_i	1	r	1
a_i	ℓ	$2\ell/r$	2ℓ

That of $(\sqrt{d} + \alpha)/2$ is

i	0	1	2
P_i	α	$\ell - 1$	$(r + 1)/2$
Q_i	2	$(2\ell + r - 1)/2$	$(2\ell - r + 1)/2$
a_i	$(\ell + \alpha - 1)/2$	1	$\begin{cases} 1 & \text{if } r < \ell \\ 2 & \text{if } r = \ell \end{cases}$

i	3	4
P_i	$\begin{cases} \ell - r & \text{if } r < \ell \\ (r + 1)/2 & \text{if } r = \ell \end{cases}$	$\begin{cases} \ell - r & \text{if } r < \ell \\ \ell - 1 & \text{if } r = \ell \end{cases}$
Q_i	$\begin{cases} 2r & \text{if } r < \ell \\ (2\ell + r - 1)/2 & \text{if } r = \ell \end{cases}$	\vdots
a_i	$\begin{cases} (\ell - r)/r & \text{if } r < \ell \\ 1 & \text{if } r = \ell \end{cases}$	\vdots

CASE I(B). $[\sqrt{d}] = \ell - 1$, (whence $r < 0$), then for \sqrt{d}

i	0	1	2	3
P_i	0	$\ell - 1$	$r + \ell$	$r + \ell$
Q_i	1	$r + 2\ell - 1$	$-r$	\vdots
a_i	$\ell - 1$	1	$-2(\ell + r)/r$	\vdots

Observe that if $r = -1$ then the period length k is 2. The expansion for $(\sqrt{d} + \alpha)/2$ is

i	0	1	2	3
P_i	α	$\ell - 1$	$\ell + 2$	$\ell + r$
Q_i	2	$(2\ell + r - 1)/2$	$-2r$	\vdots
a_i	$(\ell + \alpha - 1)/2$	2	$-(\ell + r)/r$	\vdots

CASE II. $|r|$ even.

CASE II(A). $\lfloor \sqrt{d} \rfloor = \ell$ (whence $r > 0$). The expansion for \sqrt{d} in this case is the same as in I(a) whereas the expansion of $(\sqrt{d} + \alpha)/2$ is

i	0	1	2
P_i	α	ℓ	ℓ
Q_i	2	$r/2$	\vdots
a_i	$(\ell + \alpha)/2$	$4\ell/r$	\vdots

CASE II(B). $\lfloor \sqrt{d} \rfloor = \ell - 1$ (whence $r < 0$). The expansion of \sqrt{d} is the same as in I(b), while the expansion for $(\sqrt{d} + \alpha)/2$ is

i	0	1	2	3
P_i	α	$\ell - 2$	$(r + 2\ell)/2$	$(r + 2\ell)/2$
Q_i	2	$(r + 4\ell - 4)/2$	$-r/2$	\vdots
a_i	$(\ell + \alpha - 2)/2$	1	$-2(2\ell + r)/r$	\vdots

Now we examine $d - x^2$ for each case. Let p and q be odd primes dividing d such that $p < q$.

We first assume that $\wp \sim 1$ where \wp lies over p , then in Case I(a) $p = r$. If $q > \sqrt{d}$ then no other odd prime $s \neq p, q$ can divide $d - x^2$. The reason is that $s < \sqrt{d}$ in that case and so by Proposition 2.1, $s = (2\ell + r - 1)/2$ or $s = (2\ell - r + 1)/2$. In either instance we get $pqs > d - 1$. However, $d - 1 \geq d - x^2 > pqs$, a contradiction. We have shown that if $q > \sqrt{d}$ then $d - x^2$ is r times a prime or $2r$ times a prime, (since $d - x^2 \not\equiv 0 \pmod{4}$).

Now suppose that $q < \sqrt{d}$. Therefore by Proposition 2.1 we must have $q = (2\ell + r - 1)/2$ or $q = (2\ell - r + 1)/2$. In this case, if there is a third odd prime dividing d and $s > \sqrt{d}$ then we get a contradiction as above. If $s < \sqrt{d}$ then $p = r$, $q = (2\ell + r - 1)/2$ and $s = (2\ell - r + 1)/2$ (without loss of generality) by Proposition 2.1. However, we then get $pqs \geq d - 1$, a contradiction as above. We have shown, that if $q < \sqrt{d}$ then $d - x^2$ is r times a prime or $2r$ times a prime.

If I(b) holds then $p = -r$, (observing that $r + 2\ell - 1$ is even). As in I(a) above, if $q > \sqrt{d}$, then no other odd prime divides $d - x^2$, and the result follows. If $q < \sqrt{d}$ then $q = (2\ell + r - 1)/2$, whence no third odd prime divides $d - x^2$ and the result follows.

In the case where II(a) holds Proposition 2.1 does not allow $\wp \sim 1$ since $|r|$ is even. If II(b) holds then $p = r + 2\ell - 1$. Thus $q < \sqrt{d}$ is forced; whence, $q = -r/2$ or $q = (r + 4\ell - 4)/2$. As above there cannot be a third odd prime dividing $d - x^2$. Hence, we have shown in this case, that $d - x^2$ is $-r/2$ times a prime or $-r$ times a prime. This completes the case where $\wp \sim 1$ and two odd primes divide $d - x^2$.

Now assume $\wp \not\sim 1$ and two odd primes divide $d - x^2$. Therefore, by Proposition 2.1, if Case I(a) holds then $p = (2\ell + r - 1)/2$ or $p = (2\ell - r + 1)/2$. If $q > \sqrt{d}$ then $pq \geq d - 1$, a contradiction, unless $r = 1$ and $\ell = p$ in which case we are done. Therefore $q < \sqrt{d}$ so either $q = r$ or $q = (2\ell + r - 1)/2$ (when $p = (2\ell - r + 1)/2$), or $q = (2\ell - r + 1)/2$ (when $p = (2\ell + r - 1)/2$). As above no third odd prime can divide $d - x^2$. We have shown that $d - x^2$ is r times a prime, $2r$ times a prime or $(\ell + (r - 1)/2)(\ell - (r - 1)/2)$, a product of two primes at $x = (r + 1)/2$.

In Case I(b), $p = (2\ell + r - 1)/2$. Again $q > \sqrt{d}$ leads to a contradiction so $q < \sqrt{d}$; whence $q = -r$. For similar reasons to the previous cases no third odd prime can divide $d - x^2$. Thus, in this case $d - x^2$ is $-r$ times a prime or $-2r$ times a prime.

If Case II(a) holds then $p = r/2$. If $q < \sqrt{d}$ then Proposition 2.1 leads to $q = r/2$, a contradiction. Thus, $q > \sqrt{d}$ and no third odd prime can divide $d - x^2$. Therefore $d - x^2$ is $r/2$ times a prime or r times a prime. In Case II(b) we get $p = -r/2$ or $p = (r + 4\ell - 4)/2$. Again $q < \sqrt{d}$ is forced and no third odd prime can divide $d - x^2$. Thus $d - x^2$ is $-r/2$ times a prime or $-r$ times a prime.

This completes the case where two odd primes divide $d - x^2$. If only one odd prime divides $d - x^2$ then it is prime or twice a prime. Thus we have a complete analysis of the factorization of $d - x^2$.

It remains to show that $|r|/2$ and $(r + 4\ell - 4)/2$ are primes when $|r|$ is even, and $\ell + (r - 1)/2, \ell - (r - 1)/2$ and $|r|$ are primes (or $|r| = 1$) when $|r|$ is odd. The arguments for each of these is essentially the same so we only present the proof for $r > 0$ odd. If an odd prime p divides r then by Proposition 2.1, $p = r$, $p = (2\ell + r - 1)/2$ or $p = (2\ell - r + 1)/2$. However, in the latter two cases we get a contradiction.

Conversely, assume that (i) and (ii) hold. It suffices to show that a given reduced ideal $I = [N(I), b + w]$, either $I \sim 1$ or $I \sim J$.

CASE 1. $|r|$ is odd.

If $r > 0$ then from the above calculations for \sqrt{d} and $(\sqrt{d} + \alpha)/2$ we can get that $J \sim L$ or L' where L is a prime above $(2\ell + r - 1)/2$ and L' is a prime above $(2\ell - r + 1)/2$. If $r < 0$ then $J \sim L$. In either instance $R \sim 1$ where R is the prime over $|r|$.

We have
(b + w)/
holds so

$Q_i Q_{i+1}$
 $Q_i Q_{i+1}$
 $Q_i Q_{i+1}$
 $Q_i Q_{i+1}$
 $Q_i Q_{i+1}$

CASE 2.

Example

Remark
if and on
phenome

Proposi
prime fo

Proof. It
or $I \sim$
 $d - P_{i+1}^2$

CASE 1.
or p time

CASE 2.
 $f_d(x) =$
Thus by

We have that $d - P_{i+1}^2 = Q_i Q_{i+1}$ in the continued fraction expansion of $(b+w)/N(I)$. Since $1 \leq P_{i+1} < \sqrt{d}$ then $1 \leq P_{i+1} \leq \ell$. Then the hypothesis holds so that one of the following occurs

- $Q_i Q_{i+1}$ is prime, forcing $I \sim 1$.
- $Q_i Q_{i+1}$ is twice a prime, forcing either $I \sim 1$ or $I \sim J$.
- $Q_i Q_{i+1}$ is $|r|$ times a prime, forcing $I \sim R \sim 1$.
- $Q_i Q_{i+1}$ is $2|r|$ times a prime, forcing $I \sim 1$, $I \sim J$, or $I \sim JR \sim J$.
- $Q_i Q_{i+1}$ is $((2\ell + r - 1)/2)((2\ell - r + 1)/2)$, forcing $I \sim LL' \sim J^2 \sim 1$.

CASE 2. $|r|$ is even has essentially the same argument. □

Example 3.1. Let $d = 122 = 2 \cdot 61 = 11^2 + 1$ with $h(122) = 2$.

x	$122 - x^2$
1	121 = 11 ²
2	118 = 2 · 59
3	113
4	106 = 2 · 53
5	97
6	86 = 2 · 43
7	73
8	58 = 2 · 29
9	41
10	22 = 2 · 11
11	1

Remark 3.1. Example 3.1 shows that when $d = \ell^2 + 1 \equiv 2 \pmod{4}$, $h(d) = 2$ if and only if $d - x^2$ is a prime or twice a prime for all x with $1 \leq x \leq \ell$. This phenomenon has a generalization.

Proposition 3.1. Let p a fixed prime dividing d . If $f_d(x)$ is prime or p times a prime for all x with $1 \leq x \leq \omega$ then $h(d) \leq 2$.

Proof. It suffices to show that for a given reduced ideal $I = [N(I), b+w] \sim 1$ or $I \sim P$ where P is the ideal above p . Expand $(b+w)/N(I)$ and consider $d - P_{i+1}^2 = Q_i Q_{i+1}$ for $i \geq 1$.

CASE 1. $d \equiv 2, 3 \pmod{4}$. Since $P_{i+1} < \sqrt{d}$ then by hypothesis $Q_i Q_{i+1}$ is prime or p times a prime. Therefore $I \sim P$ or $I \sim 1$.

CASE 2. $d \equiv 1 \pmod{4}$. Since Q_i is even then we may set $P_{i+1} = 2x - 1$ to get $f_d(x) = -x^2 + x + (d-1)/4 = Q_i Q_{i+1}/4$ where $x = (P_{i+1} + 1)/2 < (\sqrt{d} + 1)/2 = \omega$. Thus by hypothesis $Q_i Q_{i+1}/4$ is prime or p times a prime; i.e., $I \sim 1$ or $I \sim P$. □

Example 3.3. ($r < 0$ even). Let $d = 215 = 15^2 - 10$ with $h(d) = 2$.

x	$215 - x^2$	
1	214	$= 2 \cdot 107$
2	211	
3	206	$= 2 \cdot 103$
4	199	
5	190	$= 2 \cdot 5 \cdot 19$
6	179	
7	166	$= 2 \cdot 83$
8	151	
9	134	$= 2 \cdot 67$
10	115	$= 5 \cdot 23$
11	94	$= 2 \cdot 47$
12	71	
13	46	$= 2 \cdot 23$
14	19	

Note that $(r + 4\ell - 4)/2 = 23$.

Example 3.4. ($r < 0$ odd). Let $d = 143 = 12^2 - 1$ with $h(d) = 2$.

x	$143 - x^2$	
1	142	$= 2 \cdot 71$
2	139	
3	134	$= 2 \cdot 67$
4	127	
5	118	$= 2 \cdot 59$
6	107	
7	94	$= 2 \cdot 47$
8	79	
9	62	$= 2 \cdot 31$
10	43	
11	22	$= 2 \cdot 11$

Remark 3.2. Theorem 3.1 characterizes $h(d) = 2$ for $d \equiv 2, 3 \pmod{4}$ of ERD types (except for the troublesome forms $d = \ell^2 \pm 2$) in terms of the factorization of $d - x^2$. To solve the problem for $d \equiv 1 \pmod{4}$ in terms of $-x^2 + x + (d - 1)/4$ remains open although Proposition 3.1 provides some evidence.

The following examples illustrate remaining cases of Theorem 3.1.

Example

Example 3.2. ($r > 0$ even). Let $d = 447 = 21^2 + 6$ with $h(d) = 2$. Thus for \sqrt{d}

i	0	1	2
P_i	0	21	21
Q_i	1	6	1
a_i	21	7	42

and for $(1 + \sqrt{d})/2$

i	0	1	2
P_i	1	21	21
Q_i	2	3	2
a_i	11	14	22

Note that

and,

Example

x	$d - x^2$
1	446 = 2 · 223
2	443
3	438 = 2 · 3 · 73
4	431
5	422 = 2 · 211
6	411 = 3 · 137
7	398 = 2 · 199
8	383
9	366 = 2 · 3 · 61
10	347
11	326 = 2 · 163
12	303 = 3 · 101
13	278 = 2 · 139
14	251
15	222 = 2 · 111
16	191
17	158 = 2 · 79
18	128 = 3 · 41
19	86 = 2 · 43
20	47
21	3 · 7

Remark
types (ε
of $d - x$
remains

We now explicitly determine all ERD types $d \equiv 1 \pmod{8}$ with $h(d) = 2$.

Theorem 3.2. *If $d \equiv 1 \pmod{8}$ and d is of ERD type then $h(d) = 2$ if and only if $d = 65$ or 105 .*

Proof. Let $h(d) = 2$ and $\wp = [2, w]$. It can be shown in a fashion similar to that used in the proof of Theorem 3.1 that \wp is not principal. However $\wp^2 \sim 1$ and, by Proposition 3.1 this forces $Q_i = 8$ for some i with $1 \leq i \leq k$, whenever $4 < \sqrt{d}/2$. Since $d \equiv 1 \pmod{8}$ then clearly $d = \ell^2 + r$ with ℓ even. Thus, by an analysis similar to that given in the proof of Theorem 3.1 we reduce to only two cases for the continued fraction expansion of w .

CASE 1. $[\sqrt{d}] = \ell = 2a$ with $\ell/2 \geq r \geq 1$. Hence $Q_1 = (2\ell + r - 1)/2$, $Q_2 = (2\ell - r + 1)/2$ and $Q_3 = 2r$ with $k = 6$ unless $r = 1$ in which case $k = 3$. If $Q_1/2 = 4$ then $2\ell + r = 17$ forcing $r = 1$ and $\ell = 8$, i.e., $d = 65$. If $Q_2/2 = 4$ then $2\ell - r = 15$ forcing $r = 5$ so $d = 105$ or $r = 1$ where $d = 65$. Clearly $Q_3/2 \neq 4$, so that completes this case.

CASE 2. $[\sqrt{d}] = \ell - 1 = 2a - 1$ with $-\ell/2 \leq r < -1$. Here $Q_1 = (2\ell + r - 1)/2$ and $Q_2 = -2r$ with $k = 4$. If $Q_1/2 = 4$ then $r = -1$ and $d = 80$, a contradiction. If $Q_2/2 = 4$ then r is even, a contradiction.

Hence if $d > 64$ then $h(d) = 2$ if and only if $d = 65$ or 105 . A quick check of $d < 64$ shows no d with d of ERD-type and $h(d) = 2$. \square

Remark 3.3. We may not employ the same technique as in Theorem 3.2 to investigate the $d \not\equiv 1 \pmod{4}$ of ERD type. The reason is that although $4 < \sqrt{d}$ may hold we do not have \wp^2 primitive for \wp above 2 so we may not employ Proposition 2.1.

Remark 3.4. The $d \equiv 5 \pmod{8}$ case has not been handled in terms of prime producing quadratic polynomial criteria for $h(d) = 2$ when d is of ERD type because there is no convenient prime in general to investigate, as there is with $p = 2$ in the $d \not\equiv 5 \pmod{8}$ case. Nevertheless, even in the latter case Theorem 3.1 shows that d 's of the form $\ell^2 \pm 2$ are problematic because in that case the ideals above 2 are principal, so we again do not have a convenient prime to investigate. Nevertheless restricting to $d = \ell^2 + r$ with $|r| \in \{1, 4\}$ does allow more to be said. Let $h = h(d)$ in what follows.

Theorem 3.3. *Let $d = \ell^2 + r$ with $|r| \in \{1, 4\}$. Then p is inert for all primes p with $p^h > \omega$ unless $h \equiv 0 \pmod{2}$ in which case p may be ramified.*

Proof. Let $p^h > \omega$ and let \wp be an \mathcal{O}_K -prime above p . If \wp is not inert then $N(\wp^h) = \pm p^h = (x - dy^2)/\sigma^2$.

The following shows that we may assume $y \neq 0$.

(4) Finally

a prime

Theorem

prime q

$d \equiv 2 \pmod{4}$

(3)

modulo

$d \equiv 5 \pmod{8}$

(2)

such $h(d)$

We may

producing

quadratic

polynomial

criteria

for

$h(d) = 2$

when

d is

of

ERD

type

because

there

is

no

convenient

prime

in

general

to

investigate,

as

there

is

that

case

the

ideals

above

2

are

principal,

so

we

again

do

not

have

a

convenient

prime

to

investigate.

Nevertheless

restricting

to

$d = \ell^2 + r$

- (4) Finally note that if $d \not\equiv 5 \pmod{8}$ $d = \ell^2 + r$ with $|r| \in \{1, 4\}$ and $h(d)$ is odd then $4h(d) \geq d$.
- (3) $d \equiv 2 \pmod{4}$ and $d = (2m + 1)^2 + 1$. Here we could take the least odd prime quadratic residue and get a bound as in (2). However, we may invoke Theorem 3.3, and get that $2m + 1$ is prime if $h(d) = 2$. Moreover, if there is a prime $p \mid m$ with $(2/p) = 1$ then $m = p$ if $h(d) = 1$.
- (2) $d \equiv 5 \pmod{8}$, $d = 4m^2 + 1$. Let p be the least prime quadratic residue modulo d then $d \leq 4p^{2h(d)} + 1$ by Theorem 3.3.

We may continue the use of Theorem 3.3 as an algorithm for finding all such $h(d)$.

- (1) Let $d = 4m^2 + 1$. By Theorem 3.3 $d \equiv 1 \pmod{8}$ forces $m \leq 2^{h(d)}$ whence
- $h(d) = 1$ if and only if $d = 17$ ($m = 2$),
 $h(d) = 2$ if and only if $d = 65$ ($m = 4$),
 $h(d) = 3$ if and only if $d = 257$ ($m = 8$),
 $h(d) = 4$ if and only if $d = 145$ ($m = 6$).

Applications.

Corollary 3.1. *If p splits then $h(d) \geq \log \omega / \log p$.*

It suffices now to check that this bound satisfies $B \geq \lfloor \omega \rfloor$.
 If $r = 1$ and $\sigma = 2$ then $N(\varepsilon_d) = -1$ so $B = t_d/u_d^2 = \ell/2 = \lfloor \omega \rfloor$. If $r = 1$ and $\sigma = 1$ then $B = 2t_d/u_d^2 = 2\ell = 2\lfloor \omega \rfloor$. If $r = -1$ then $\sigma = 1$ and $N(\varepsilon_d) = 1$ so $B = (2t_d - 2)/u_d^2 = 2(\ell - 1) = 2\lfloor \omega \rfloor$. If $r = 4$ then $\sigma = 2$ and $N(\varepsilon_d) = -1$ so $B = t_d/u_d^2 = \ell/2 = \lfloor \omega \rfloor$. If $r = -4$ then $\sigma = 2$ and $N(\varepsilon_d) = 1$ so $B = t_d/u_d^2 = \ell/2 = \lfloor \omega \rfloor$.
 □

CLAIM 2. If p splits in K then $p^h \geq \omega$.
 By [3] Lemma 1.1, p.40 since $\pm p^h \sigma^2 = x^2 - dy^2$ has a nontrivial solution (x, y) then $p^h \geq ((2td)/\sigma - N(\varepsilon_d) - 1)/u_d^2 = B$ where the fundamental unit ε_d of K is given by $\varepsilon_d = (t_d + u_d \sqrt{d})/\sigma$.

CLAIM 1. If $y = 0$ then p is ramified and h is even.
 We have $\wp^h = \left(\frac{\sigma}{x + y\sqrt{d}} \right)$. If $y = 0$ then $\frac{\sigma}{x + y\sqrt{d}} = \lambda$, a rational integer, and $\wp^h = \wp^h$, i.e., \wp^h is ambiguous. However the only non-trivial (primitive) ambiguous ideals are those whose ideal prime factors are ramified. (To see this set $\mathcal{A} = [N(\mathcal{A}), b + \overline{w}] = \underline{\mathcal{A}} = [N(\mathcal{A}), b + \overline{w}]$. Then $w - \overline{w} \in \mathcal{A}$ forcing $N(d) \mid N(w - \overline{w})$; i.e., primes dividing \mathcal{A} must ramify). Also $|N(\wp^h)| = p^h = \chi^2$, so h is even.

References

- [1] M.D. Hendy, *Prime Quadratics Associated With Complex Quadratic Fields of Class number Two*, Proc. Amer. Math. Soc. **43** (1974), 253–260.
- [2] S. Louboutin, *Continued Fraction and Real Quadratic Fields*, J. Number Theory **30** (1988), 167–176.
- [3] R.A. Mollin, *On the Insolubility of a Class of Diophantine Equations and the Non-triviality of the Class Numbers of Related Real Quadratic Fields of Richaud-Degert Type*, Nagoya Math. J. **105** (1987), 39–47.
- [4] R.A. Mollin, *Diophantine Equations and Class Numbers*, J. Number Theory **24** (1986), 7–19.
- [5] R.A. Mollin, *Necessary and Sufficient Conditions for the Class Number of a Real Quadratic Field to be One and a Conjecture of S. Chowla*, Proc. Amer. Math. Soc. **102** (1988), 17–21.
- [6] R.A. Mollin, *Class Number One Criteria for Real Quadratic Fields I*, Proc. Japan. Acad **63** Ser. A. (1987), 121–125.
- [7] R.A. Mollin, *Class Number One Criteria for Real Quadratic Fields II*, Proc. Japan. Acad **63** Ser. A. (1987), 162–164.
- [8] R.A. Mollin, *Class numbers and the Divisor Function* (to appear).
- [9] R.A. Mollin and H.C. Williams, *Continued Fractions of Period Five and Real Quadratic Fields of Class Number One*, Acta Arith. **LVI** (1990), 55–63.
- [10] R.A. Mollin and H.C. Williams, *Quadratic Non-Residues and Prime-Producing Polynomials*, Canad. Math. Bull. **32** (1989), 474–478.
- [11] R.A. Mollin and H.C. Williams, *Class Number One for Real Quadratic Fields, Continued Fractions and Reduced Ideals*, in “Number Theory and Applications”, Kluwer Academic Publishers (R.A. Mollin (ed.)) (NATO ASI, vol.C 265, 1989, 481–496.
- [12] R.A. Mollin and H.C. Williams, *Solution of the Class Number One Problem for Real Quadratic Fields of Extended Richaud-Degert type (with one possible exception)*, in “Number Theory” (R.A. Mollin (ed.)) Walter de Gruyter, Berlin, 1990, 417–425.
- [13] R.A. Mollin and H.C. Williams, *Computation of the Class Number of a Real Quadratic Field* (to appear: Advances in the Theory of Computing and Comp. Math.).
- [14] H.C. Williams and M.C. Wunderlich, *On the Parallel Generation of the Residues for the Continued Fraction Factoring Algorithm*, Math. Comp. **177** (1987), 405–423.