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-Richaud-Degert (ERD)-type. Examples are provided as well as an explicit determination of all ERD-types \(d \equiv 1 \mod 8\) 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

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

The discriminant \(\Delta\) of \(K\) is \((w - \overline{w})^2 = 4d/\sigma^2\), and the absolute norm of \(\alpha\) is \(N(\alpha) = \alpha \overline{\alpha}\) where \(\overline{x}\) is the algebraic conjugate of \(x\). 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 \(a, b, c \in \mathbb{Z}, a > 0, c > 0, c | b, a \text{ and } ac | N(b + cw)\). 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 $i = 0, 1, \ldots d = P_{i+1}^2 + Q_i Q_{i+1}$, $P_{i+1} = a_i Q_i - P_i$ where $a_i = \lfloor (P_i + \sqrt{d})/Q_i \rfloor$ with $\lfloor \rfloor$ 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 $(b + w)/N(I) = \langle a, a_1, a_2, \ldots, a_k \rangle$ 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.,

$I_1 = [Q_0/\sigma, (P_0 + \sqrt{d})/\sigma] = I \sim I_2 = [Q_1/\sigma, (P_1 + \sqrt{d})/\sigma] \sim \ldots \sim$

$I_k = [Q_{k-1}/\sigma, (P_{k-1} + \sqrt{d})/\sigma]$.

Thus the $(P_i + \sqrt{d})/Q_i$ are complete quotients in the continued fraction expansion of $(b + w)/N(I)$ and the $Q_i/\sigma$'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, 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

\[
\begin{array}{c|c|c|c}
  i  & 0 & 1 & 2 \\
P_i & 0 & \ell & \ell \\
Q_i & 1 & r & 1 \\
a_i & \ell & 2\ell/r & 2\ell \\
\end{array}
\]

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

\[
\begin{array}{c|c|c|c|c}
  i  & 0 & 1 & 2 & | \text{if } r < \ell \} \\
P_i & \alpha & \ell - 1 & (r + 1)/2 & \{ \\
Q_i & 2 & (2\ell + r - 1)/2 & (2\ell - r + 1)/2 & \} \\
a_i & (\ell + \alpha - 1)/2 & 1 & \{ \\
\end{array}
\]

\[
\begin{array}{c|c|c|c|c|c}
  i  & 3 & 4 & \{ & \text{if } r < \ell \} & \{ \\
P_i & \{ & \ell - r & \ell - r & \} \\
& (r + 1)/2 & \ell - 1 & \} \\
Q_i & \{ & 2r & \} & \{ & \} \\
& (2\ell + r - 1)/2 & \} & \} \\
a_i & \{ & (\ell - r)/r & \} & \{ & \} \\
& 1 & \} & \} \\
\end{array}
\]

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

\[
\begin{array}{c|c|c|c|c}
  i  & 0 & 1 & 2 & 3 \\
P_i & 0 & \ell - 1 & r + \ell & r + \ell \\
Q_i & 1 & r + 2\ell - 1 & -r & \} \\
a_i & \ell - 1 & 1 & -2(\ell + r)/r & \} \\
\end{array}
\]

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

<table>
<thead>
<tr>
<th>( i )</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td>( P_i )</td>
<td>( \alpha )</td>
<td>( \ell - 1 )</td>
<td>( \ell + 2 )</td>
<td>( \ell + r )</td>
</tr>
<tr>
<td>( Q_i )</td>
<td>2</td>
<td>( (2\ell + r - 1)/2 )</td>
<td>( -2r )</td>
<td>:</td>
</tr>
<tr>
<td>( a_i )</td>
<td>( (\ell + \alpha - 1)/2 )</td>
<td>2</td>
<td>( -(\ell + r)/r )</td>
<td>:</td>
</tr>
</tbody>
</table>

**Case II.** \(| r | \) even.

**Case II(a).** \( |\sqrt{d}| = \ell \) (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

<table>
<thead>
<tr>
<th>( i )</th>
<th>0</th>
<th>1</th>
<th>2</th>
</tr>
</thead>
<tbody>
<tr>
<td>( P_i )</td>
<td>( \alpha )</td>
<td>( \ell )</td>
<td>( \ell )</td>
</tr>
<tr>
<td>( Q_i )</td>
<td>2</td>
<td>( r/2 )</td>
<td>:</td>
</tr>
<tr>
<td>( a_i )</td>
<td>( (\ell + \alpha)/2 )</td>
<td>( 4\ell/r )</td>
<td>:</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>( i )</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td>( P_i )</td>
<td>( \alpha )</td>
<td>( \ell - 2 )</td>
<td>( (r + 2\ell)/2 )</td>
<td>( (r + 2\ell)/2 )</td>
</tr>
<tr>
<td>( Q_i )</td>
<td>2</td>
<td>( (r + 4\ell - 4)/2 )</td>
<td>( -r/2 )</td>
<td>:</td>
</tr>
<tr>
<td>( a_i )</td>
<td>( (\ell + \alpha - 2)/2 )</td>
<td>1</td>
<td>( -2(2\ell + r)/r )</td>
<td>:</td>
</tr>
</tbody>
</table>

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 \( \varphi \sim 1 \) where \( \varphi \) 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 \( \Pi(a) \) holds Proposition 2.1 does not allow \( \wp \sim 1 \) since \( |r| \) is even. If \( \Pi(b) \) 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 \( \wp \neq 1 \) 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 \( \Pi(a) \) 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 \( \Pi(b) \) 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 that \( d - P_{i+1}^2 = Q_iQ_{i+1} \) 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. \( \Box \)

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

<table>
<thead>
<tr>
<th>( x )</th>
<th>122 - ( x^2 )</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>121 = 11^2</td>
</tr>
<tr>
<td>2</td>
<td>118 = 2 \cdot 59</td>
</tr>
<tr>
<td>3</td>
<td>113</td>
</tr>
<tr>
<td>4</td>
<td>106 = 2 \cdot 53</td>
</tr>
<tr>
<td>5</td>
<td>97</td>
</tr>
<tr>
<td>6</td>
<td>86 = 2 \cdot 43</td>
</tr>
<tr>
<td>7</td>
<td>73</td>
</tr>
<tr>
<td>8</td>
<td>58 = 2 \cdot 29</td>
</tr>
<tr>
<td>9</td>
<td>41</td>
</tr>
<tr>
<td>10</td>
<td>22 = 2 \cdot 11</td>
</tr>
<tr>
<td>11</td>
<td>1</td>
</tr>
</tbody>
</table>

**Remark 3.1.** Example 3.1 shows that when \( d = \ell^2 + 1 \equiv 2(\text{mod } 4) \), \( h(d) = 2 \) 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.** \( d \equiv 2, 3(\text{mod } 4) \). 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.** \( d \equiv 1(\text{mod } 4) \). 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 \( I \sim P \). \( \Box \)
The following examples illustrate remaining cases of Theorem 3.1.

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

\[
\begin{array}{ccc}
 i & 0 & 1 & 2 \\
P_i & 0 & 21 & 21 \\
Q_i & 1 & 6 & 1 \\
a_i & 21 & 7 & 42 \\
\end{array}
\]

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

\[
\begin{array}{ccc}
 i & 0 & 1 & 2 \\
P_i & 1 & 21 & 21 \\
Q_i & 2 & 3 & 2 \\
a_i & 11 & 14 & 22 \\
\end{array}
\]

and,

\[
\begin{array}{c|c|c}
 x & d - x^2 \\
\hline
1 & 446 = 2 \cdot 223 \\
2 & 443 \\
3 & 438 = 2 \cdot 3 \cdot 73 \\
4 & 431 \\
5 & 422 = 2 \cdot 211 \\
6 & 411 = 3 \cdot 137 \\
7 & 398 = 2 \cdot 199 \\
8 & 383 \\
9 & 366 = 2 \cdot 3 \cdot 61 \\
10 & 347 \\
11 & 326 = 2 \cdot 163 \\
12 & 303 = 3 \cdot 101 \\
13 & 278 = 2 \cdot 139 \\
14 & 251 \\
15 & 222 = 2 \cdot 111 \\
16 & 191 \\
17 & 158 = 2 \cdot 79 \\
18 & 128 = 3 \cdot 41 \\
19 & 86 = 2 \cdot 43 \\
20 & 47 \\
21 & 3 \cdot 7 \\
\end{array}
\]
Example 3.3. \((r < 0 \text{ even})\). Let \(d = 215 = 15^2 - 10\) with \(h(d) = 2\).

<table>
<thead>
<tr>
<th>(x)</th>
<th>(215 - x^2)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>214 = 2 \cdot 107</td>
</tr>
<tr>
<td>2</td>
<td>211</td>
</tr>
<tr>
<td>3</td>
<td>206 = 2 \cdot 103</td>
</tr>
<tr>
<td>4</td>
<td>199</td>
</tr>
<tr>
<td>5</td>
<td>190 = 2 \cdot 5 \cdot 19</td>
</tr>
<tr>
<td>6</td>
<td>179</td>
</tr>
<tr>
<td>7</td>
<td>166 = 2 \cdot 83</td>
</tr>
<tr>
<td>8</td>
<td>151</td>
</tr>
<tr>
<td>9</td>
<td>134 = 2 \cdot 67</td>
</tr>
<tr>
<td>10</td>
<td>115 = 5 \cdot 23</td>
</tr>
<tr>
<td>11</td>
<td>94 = 2 \cdot 47</td>
</tr>
<tr>
<td>12</td>
<td>71</td>
</tr>
<tr>
<td>13</td>
<td>46 = 2 \cdot 23</td>
</tr>
<tr>
<td>14</td>
<td>19</td>
</tr>
</tbody>
</table>

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

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

<table>
<thead>
<tr>
<th>(x)</th>
<th>(143 - x^2)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>142 = 2 \cdot 71</td>
</tr>
<tr>
<td>2</td>
<td>139</td>
</tr>
<tr>
<td>3</td>
<td>134 = 2 \cdot 67</td>
</tr>
<tr>
<td>4</td>
<td>127</td>
</tr>
<tr>
<td>5</td>
<td>118 = 2 \cdot 59</td>
</tr>
<tr>
<td>6</td>
<td>107</td>
</tr>
<tr>
<td>7</td>
<td>94 = 2 \cdot 47</td>
</tr>
<tr>
<td>8</td>
<td>79</td>
</tr>
<tr>
<td>9</td>
<td>62 = 2 \cdot 31</td>
</tr>
<tr>
<td>10</td>
<td>43</td>
</tr>
<tr>
<td>11</td>
<td>22 = 2 \cdot 11</td>
</tr>
</tbody>
</table>

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.
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 $\varphi = [2, w]$. It can be shown in a fashion similar to that used in the proof of Theorem 3.1 that $\varphi$ is not principal. However $\varphi^2 \sim 1$ 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 $\ell$ 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 $h(d) = 2$. \qed

**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 $\varphi^2$ primitive for $\varphi$ 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 $\varphi$ be an $O_K$-prime above $p$. If $\varphi$ is not inert then $N(\varphi^h) = \pm p^h = (x - dy^2)/\sigma^2$.

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

CLAIM 1. If \( y = 0 \) then \( p \) is ramified and \( h \) is even.

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

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 \( p^h \geq \left( \frac{(2t_\sigma)/\sigma - N(\varepsilon_d) - 1}{u_\sigma^2} \right) = B \) where the fundamental unit \( \varepsilon_d \) of \( K \) is given by \( \varepsilon_d = (t_d + u_d \sqrt{d})/\sigma \).

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 \( B = t_d/u_\sigma^2 = \ell/2 = \lfloor \omega \rfloor \). If \( r = 1 \) and \( \sigma = 1 \) then \( B = 2t_d/u_\sigma^2 = 2\ell = 2\lfloor \omega \rfloor \). If \( r = -1 \) then \( \sigma = 1 \) and \( N(\varepsilon_d) = 1 \) so \( B = (2t_\sigma - 2)/u_\sigma^2 = 2(\ell - 1) = 2\lfloor \omega \rfloor \). If \( r = 4 \) then \( \sigma = 2 \) and \( N(\varepsilon_d) = -1 \) so \( B = t_d/u_\sigma^2 = \ell/2 = \lfloor \sqrt{d} \rfloor/2 \). If \( r = -4 \) then \( \sigma = 2 \) and \( N(\varepsilon_d) = 1 \) so \( B = \ell - 2 \geq \lfloor \omega \rfloor \).

\[ \square \]

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

Applications.

(1) Let \( d = 4m^2 + 1 \). By Theorem 3.3 \( d \equiv 1 \) (mod 8) forces \( m \leq 2^{h(d)} \) whence

\[
\begin{align*}
    h(d) = 1 & \quad \text{if and only if} \quad d = 17 \ (m = 2), \\
    h(d) = 2 & \quad \text{if and only if} \quad d = 65 \ (m = 4), \\
    h(d) = 3 & \quad \text{if and only if} \quad d = 257 \ (m = 8), \\
    h(d) = 4 & \quad \text{if and only if} \quad d = 145 \ (m = 6).
\end{align*}
\]

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

(2) \( d \equiv 5 \) (mod 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.

(3) \( d \equiv 2 \) (mod 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 \( h(d) = 1 \).

(4) Finally note that if \( d \not\equiv 5 \) (mod 8) \( d = \ell^2 + r \) with \( |r| \in \{1, 4\} \) and \( h(d) \) is odd then \( 4^{h(d)} \geq d \).
References


