25. Period Four and Real Quadratic Fields of Class Number One

By R. A. MOLLIN* and H. C. WILLIAMS**

(Communicated by Shokichi IYANAGA, M. J. A., April 12, 1989)

The purpose of this note is to provide criteria, in terms of prime-producing quadratic polynomials, for a real quadratic field $Q(\sqrt{d})$ to have class number $h(d)=1$, when the continued fraction expansion of $\omega$ is 4 (where $\omega=(1+\sqrt{d})/2$ if $d \equiv 1 \pmod{4}$ and $\omega=\sqrt{d}$ if $d \equiv 2, 3 \pmod{4}$). This continues the work of the first author in [4]–[11] and that of both authors in [12]–[18] in the quest for a general “Rabinowitsch-like” result for real quadratic field. Rabinowitch [19]–[20], proved that if $p$ is prime then $h(-p)=1$ and only if $x^2-x+(p+1)/4$ is prime for all integers $x$ with $1 \leq x \leq (p-7)/4$, $p > 7$. In [4] the first author found such a criterion for real quadratic fields of narrow Richaud-Degert (R-D)-type (see [1] and [21]). $Q(\sqrt{d})$ (or simply $d$) is said to be R-D type if $d=l^2+r$ with $4l \equiv 0 \pmod{r}$ and $-l \leq r \leq l$. If $|r| \in \{1, 4\}$ then $d$ is said to be of narrow R-D type. In [15]–[16] we found similar criteria for general R-D types. In fact in [18] we completed the task of actually determining all real quadratic fields of R-D type having class number one (with possibly only one more value remaining). However, our forging of intimate links between the class number one problem and prime-producing quadratic polynomials makes the existence of the potential additional value virtually impossible.

With the virtual solution of the class number one problem for real quadratic fields of R-D type the authors turned their attention to the general case. In [12] we found a Rabinowitsch criterion for $d \equiv 1 \pmod{4}$ where $\omega$ has period 3. Several examples of non-R-D types were provided as applications. The result in this paper is to find such a criterion when $\omega$ has period 4. Moreover for $d \equiv 5 \pmod{8}$ we determine all such $d$ with class number one (with possibly only one more value remaining).

**Theorem 1.** Let square-free $d \equiv 1 \pmod{4}$ and $\omega=\langle a, b, c, b, 2a-1 \rangle$ (the continued fraction expansion of period 4), $d=(2a-1)^4+4(c(fb-c)+f)$, and $2a-1=b^2cf-bc^2+c-2bf$ for some positive integers $a, b, c$ and $f$. Let, furthermore, $f(x)=-x^2-x+(d-1)/4$. Then $h(d)=1$ if and only if the following conditions (1)–(6) all hold.

1. $b(fb-c)+1$ is prime.
(2) \(c(fb-c)+f\) is prime.

(3) \(f_\alpha(x)/(b(fb-c)+1)\) is 1 or prime for all integers \(x\) with \(0 \leq x \leq a-1\) and \(x \equiv -2^{-1} \pmod{b(fb-c)+1}\).

(4) \(f_\alpha(x)/(c(fb-c)+f)\) is prime for all integers \(x\) with \(0 \leq x \leq a-1\) and \(x \equiv -2^{-1}(fb-c+1) \pmod{c(fb-c)+f}\).

(5) \(f_\alpha(x)/(c(fb-c)+f)\) is prime or 1 for all integers \(x\) with \(0 \leq x \leq a-1\) and \(x \equiv 2^{-1}(fb-c-1) \pmod{c(fb-c)+f}\).

(6) \(f_\alpha(x)\) is prime for all integers \(x\) with \(0 \leq x \leq a-1\) and \(x \equiv -2^{-1}(fb-c-1) \pmod{c(fb-c)+f}\), and \(x \equiv -2^{-1} \pmod{b(fb-c)+1}\).

Proof. The first statement of the theorem may be easily verified using the methods of Krutchik [2, Chapter 3–4]. To prove the rest of the theorem we invoke Lu [3, Theorem 2, p. 119] to get that \(h(d)=1\) if and only if \(2x+2b+c-1=\lambda(d)+\lambda_l(d)\) where \(\lambda(d)\) (respectively \(\lambda_l(d)\)) is the number of solutions of \(w^4+4vw=d\) (respectively \(w^4+4v^2=d\)) with positive integers \(u, v\) and \(w\). We note that if \(h(d)=1\) then \(\lambda_l(d)=0\) if \(d\) is not prime and \(\lambda_l(d)=1\) if \(d\) is prime. Thus we concentrate on \(\lambda_l(d)\).

Since \(w^4+4vw=d\) then \(u\) is odd, so we set \(u=2x+1\) to get that \(\frac{f_\alpha(x)}{x^2-x+(d-1)/4}=vw\) with \(0 \leq x \leq a-1\). We now investigate the number of divisors of \(f_\alpha(x)\).

In cases i–iv we assume that \(d\) is not prime. We will be able to deal with the \(d=\text{prime}\) case briefly at the end of the proof.

Case i. \(x \equiv -2^{-1} \pmod{b(fb-c)+1}\). (This means that \(f_\alpha(x)\equiv 0 \pmod{b(fb-c)+1}\). Thus, \(2x+2=1(b(fb-c)+1)\) for some positive integer \(l\). Since \(0 \leq x \leq a-1\) then \(1 \leq l \leq c\) and \(l\) must be odd. Since \(c\) is odd then there are \((c+1)/2\) such values of \(l\). We observe that \(f_\alpha(x) \equiv b(fb-c)+1\) and \(f_\alpha(x) \equiv (b(fb-c)+1)^l\). Therefore for all such values of \(l\), \(f_\alpha(x)\) has at least four divisors. Therefore the total number of divisors of \(f_\alpha(x)\) for such values of \(l\) is at least \(2c+2\).

Case ii. \(x \equiv -2^{-1}(fb-c+1) \pmod{c(fb-c)+f}\), which implies \(f_\alpha(x)\equiv 0 \pmod{c(fb-c)+f}\). Therefore, \(2x+1=c-2b+1(c(fb-c)+f)\) for some positive integer \(l\). Since \(0 \leq x \leq a-1\) then \(0 \leq l \leq b\). If \(b\) is odd then \(l\) must be odd so there are \((b+1)/2\) such values of \(l\). Since each such value of \(l\) yields at least four divisors then \(f_\alpha(x)\) has at least \(2b+2\) of them. If \(b\) is even, then \(l\) is even so there are \(b/2\) such values of \(l\), and in this case \(f_\alpha(x)\) has at least \(2b\) divisors.

There we must exercise caution because we have counted 4 divisors of \(f_\alpha(x)\) in both case i and case ii; namely when \(x=(fb+c-bc-c-c-1)/2\) then \(f_\alpha(x)=(b(fb-c)+1)(c(fb-c)+f)\).

Therefore we revise our count on the case ii divisors to \(2b\) for odd \(b\), and \(2b-2\) for even \(b\).

Case iii. \(x \equiv 2^{-1}(fb-c-1) \pmod{c(fb-c)+f}\) whence \(f_\alpha(x)\equiv 0 \pmod{c(fb-c)+f}\). Since \(0 \leq x \leq a-1\) then \(0 \leq l \leq b\). If \(b\) is odd, then \(l\) is odd and so there are \((b+1)/2\) such values of \(l\). Since \(f_\alpha(x)\) has at least four
divisors for all values of \( x \) except \( x=a-1 \), (in which case \( f_d(x)=c(fb-c+f) \)), in the range \( 0 \leq x \leq a-1 \), then there are at least \( 2b \) divisors. If \( b \) is even, then \( l \) is 0 or even and there \( (b/2)+1 \) such values of \( l \) yielding at least \( 2b+2 \) divisors.

Case iv. For the remaining \( a-(c+1)/2+b+1 \) values of \( x \), \( f_d(x) \) has at least \( 2(a-(c+1)(2+b+1))/2a-2b-c-3 \) divisors.

Hence from cases i–iv, \( f_d(x) \) has a total of at least \( 2a+2b+c-1 \) divisors if \( d \) is not prime. Thus \( \lambda_d(d) \geq 2a+2b+c-1 \). Moreover as noted at the outset \( \lambda_d(d)+\lambda_x(d)=2a+2b+c-1 \). Hence the minimum must be achieved; i.e., conditions (1)–(6) of the theorem must hold.

If \( d \) is prime, then the only difference in cases i–iii is that possibly \( f_d(x)=p^2 \) where

\[
p = c(fb-c)+f \quad \text{or} \quad p = b(fb-c)+1.
\]

However, since \( \lambda_d(d)=1 \) in this case, then \( d=p^2+(2x+1)^2 \) in at most one of the cases i–iii, and for this value of \( x \), \( f_d(x) \) has three divisors. Hence when \( d \) is prime the total number of divisors of \( f_d(x) \) is at least \( 2a+2b+c-2 \). Therefore, \( \lambda_d(d) \geq 2a+2b+c-2 \), and so again \( \lambda_d(d)+\lambda_x(d) \geq 2a+2b+c-1 \) and the minimum must be achieved. This completes the proof.

Corollary 1. If \( d \equiv 1 \pmod{8} \) and \( \omega \) has period 4 then \( h(d)=1 \) if and only if \( d=33 \).

Proof. Since \( d \equiv 1 \pmod{8} \) then \( c(fb-c)+f \) is even. Hence by Theorem 1-(2), \( c(fb-c)+f=2 \); whence, \( c=f=1 \) and \( b=2 \); i.e., \( h(d)=1 \) if and only if \( d=33 \).

Example of R-D types other than 33 satisfying Theorem 1 are 141, 213, 413, 573, 717, 1077, 1293 and 1757. Examples of non-R-D types satisfying Theorem 1 are 69, 133, 1897 and 3053. We conjecture that the above values represent all values, satisfying Theorem 1. However for \( d \equiv 1 \pmod{4} \) of period 4 only R-D types appear for \( h(d)=1 \) as we see in:

Theorem 2. If square-free \( d \equiv 1 \pmod{4} \) and \( \omega \) has period 4 then \( \omega=\langle a, b, c, b, 2a \rangle \), \( d=a^2-c^2+f(bc+1) \), and \( 2a=b^2cf+2fb-bee-c \) for positive integers \( a, b, c \) and \( f \). Thus, \( h(d)=1 \) if and only if \( d=(c+2)^2-2 \).

Proof. (1) Assume \( d \equiv 2 \pmod{4} \). By the result of Lu (op.cit.), \( h(d)=1 \) if and only if \( \lambda_d(d)=2a+2b+c+\theta \) where \( \theta=1 \) if \( c \) is odd, \( \theta=2 \) if \( c \) is even, and \( \lambda_d(d) \) is the number of solutions of \( w^2+4vw=4d \) in non-negative integers \( u, v \) and \( w \). Hence \( u=2x \) and we get: \( f_d(x)=d-x^2=vw \), with \( 0 \leq x \leq a \). We now examine the number of divisors of \( f_d(x) \).

Case i. \( a \) is odd and \( c \) is even. There are \((a+1)/2\) values of \( x \) for which \( f_d(x) \) is even, and so for these values \( f_d(x) \) has at least \( 2a+2 \) divisors. For the remaining \((a+1)/2\) values of \( x \) there are at least \( a+1 \) divisors of \( f_d(x) \). Hence \( \lambda_d(d) \geq 3a+3 \). Thus;

\[
2a+2b+c+\theta=2a+2b+c+2 \geq 3a+3; \quad \text{i.e.,} \quad 4b+3c \geq b^2cf+2f-be^2+2.
\]

Now, if \( f \geq 2 \) then \( 3c \geq b^2cf-be^2+2 \geq bc+2 \). Therefore \( b \leq 2 \). If \( b=2 \) then \( 3c \geq 4cf-2e^2+2 \), whence \( 2f-c=1 \). However, \( c \) is even, a contra-
diction. Hence $b=1$. Therefore $3c \geq c^2 - c^2 + 2$; whence, $f = c+1$ or $f = c+2$. If $f = c+2$ then $a = (3c + 4)/2$ which contradicts $2b + c \geq a + 2$. Thus, $f = c+1$ which implies $a = c+1$; whence $d = (c+1)^2 - 2$. It is a tedious check to show that $f = 1$ cannot hold.

Case ii. $a$ is odd and $c$ is odd. (Thus $\theta = 1$.) As in case i, $\lambda(d) \geq 3a + 3$. Thus $2a + 2b + c + 2 \geq 3a + 3$; i.e., $2b + c \geq a + 2$. Again it is a tedious check as in case i to show that $f \geq 2$ and that this forces $b = 1$ and $f = a = c+1$. However, $a$ is odd and $c$ is odd, a contradiction.

Case iii. $a$ is even and $c$ is odd. (Thus $\theta = 1$.) In this case there are $(a/2) + 1$ values of $x$ for which $f(x)$ is even, and $f(x)$ has at least $2a + 4$ divisors for these values. For the remaining $a/2$ values, $f(x)$ has at least $a$ divisors. Hence $\lambda(d) \geq 3a + 4$. Therefore $1 + 2a + 2b + c \geq 3a + 4$; i.e., $2b + c \geq a + 3$. Equivalently, $4b + 3c \geq bcf + 2fb - bc^2 + 6$. A tedious check as in case i shows $f \geq 2$ and that this forces $b = 1$ and $f = a = c+1$; whence, $d = (c+2)^2 - 2 \equiv 3$ (mod 4), a contradiction.

Case iv. $a$ even and $c$ even. This case is dispatched in a similar fashion to cases ii–iii.

(II) Assume $d \equiv 3$ (mod 4).

Since this situation is so similar to the above we merely point out the facts. The details are a straightforward check. When $a$ is even and $c$ is odd we can show that $d = (c+2)^2 - 2$ with $b = 1$ and $a = c+1 = f$.

In all of the remaining cases we get a contradiction. This proves the result.

Corollary 2. Suppose $d \equiv 1$ (mod 4) and $\omega$ has period 4. Then with possibly only one more value remaining, the following set contains all such $d$ with $h(d) = 1$:

\{7, 14, 23, 47, 62, 167, 398\}.

Proof. If $d = 5^2 - 2$ then $d$ is an example of an R-D type. In [18] the authors found all real quadratic fields of R-D type having class number one to be, with possibly only one more value remaining, in the following set:

\{2, 3, 6, 7, 11, 14, 17, 21, 23, 29, 33, 37, 38, 47, 53, 62, 77, 83, 101, 141, 167, 173, 197, 213, 227, 237, 293, 398, 413, 437, 453, 573, 677, 717, 1077, 1133, 1253, 1293, 1757\}.

A check of this set shows that the only ones of the form $5^2 - 2$ are those listed in the corollary.

References


