E. Dubois and C. Levesque
Nagoya Math. J.
Vol. 124 (1991), 157-180

# ON DETERMINING CERTAIN REAL QUADRATIC FIELDS WITH CLASS NUMBER ONE AND RELATING THIS PROPERTY TO CONTINUED FRACTIONS AND PRIMALITY PROPERTIES

EUGÈNE DUBOIS AND CLAUDE LEVESQUE

## § 1. Introduction and preliminary results

Thanks to K. Heegner [He], A. Baker [Ba] and H. Stark [S], we know that there are nine imaginary quadratic fields of class number one. Gauss conjectured that there are infinitely many real quadratic fields of class number one, but the conjecture is still open.

In a series of papers, R. A. Mollin [M1, M2, M3] studied the class number one problem for the so-called Richaud-Degert real quadratic fields $\mathbf{Q}(\sqrt{m})$, where the square-free integer $m$ is defined by

$$m = D^2 + d \text{ with } D \in \mathbf{N} = \{1, 2, \cdots\},\ d \in \mathbf{Z} = \{\cdots, -1, 0, 1, \cdots\},\ d \mid 4D\,.$$

R. A. Mollin and H. C. Williams [M-W], and independently S. Louboutin [Lo2], gave a list of all the Richaud-Degert quadratic fields with class number one. The first two authors showed that their list is complete, with possibly one more value, which is however ruled out if one assumes the general Riemann hypothesis (GRH). The last author assumed a certain version of GRH.

If $\mathbf{Q}(\sqrt{m})$ is a fixed real quadratic field such that $m$ is square-free $> 1$, then define the polynomial $f_m(x)$ by

$$f_m(x) := -x^2 + x + \frac{m-1}{4} \qquad \text{if } m \equiv 1 \pmod 4\,,$$

$$f_m(x) := -x^2 + m \qquad \text{if } m \not\equiv 1 \pmod 4\,.$$

Define also

$$\Delta := m, \quad \omega := (1 + \sqrt{m})/2 \qquad \text{if } m \equiv 1 \pmod 4\,,$$

$$\Delta := 4m, \quad \omega := \sqrt{m} \qquad \text{if } m \not\equiv 1 \pmod 4\,,$$

Received February 12, 1991.

and consider $\omega = [a_0, a_1, \cdots, a_i, \cdots]$, the continued fraction expansion of $\omega$. Here $\alpha_i := \dfrac{P_i + \sqrt{m}}{Q_i}$ where for each $i$,

$$P_i = a_{i-1}Q_{i-1} - P_{i-1}, \qquad Q_i = \frac{m - P_i^2}{Q_{i-1}},$$

with

$$(P_0, Q_0) := \begin{cases} (1, 2) & \text{if } m \equiv 1 \pmod 4, \\ (0, 1) & \text{if } m \not\equiv 1 \pmod 4, \end{cases}$$

and $a_i := \left[\dfrac{P_i + \sqrt{m}}{Q_i}\right]$, the greatest integer less than or equal to $\alpha_i$. Finally, by definition, let

$$E(m) := \left\{\frac{Q_i}{Q_0} : 1 \leq i \leq r\right\}$$

where $r$ is the length of the primitive period of $\omega$.

H. Lu gave in [Lu] a necessary and sufficient condition, involving the continued fraction expansion of $\omega$ and the number of solutions of certain Diophantine equations, under which the class number of a real quadratic field is one. This is precisely the purpose of this paper to apply his criterion to certain families of real quadratic fields previously discovered by L. Bernstein [Be1, Be2], C. Levesque and G. Rhin [Le-R] and C. Levesque [Le]. This will lead to certain criteria which must be satisfied to have class number one.

Let us state H. Lu's result which we plan to use extensively.

THEOREM 1.1 (Lu). *Let $m > 1$ be square-free and let $h(m)$ be the class number of the real quadratic field $\mathbf{Q}(\sqrt{m})$. Let $\lambda_1(m)$ and $\lambda_2(m)$ be the number of solutions of the two Diophantine equations*

$$x^2 + 4yz = \Delta \qquad \text{with integers } x, y, z \geq 0,$$
$$x^2 + 4y^2 = \Delta \qquad \text{with integers } x, y \geq 0,$$

*respectively. Let also $\omega = [a_0, \overline{a_1, \cdots, a_r}]$ be the development of $\omega$ as a simple continued fraction with primitive period length $r$ and let $c$ be defined as follows:*

*if $m \equiv 1 \pmod 4$, then $c := 0$ when $r$ is even with*
*$r = 2n$ and $a_n$ odd, and $c := 1$ otherwise;*

https://doi.org/10.1017/S0027763000003822 Published online by Cambridge University Press

*if* $m \not\equiv 1 \pmod 4$, *then* $c := 1$ *when* $r$ *is even with* $r = 2n$ *and* $a_n$ *odd, and* $c := 2$ *otherwise.*

*Then*

$$c + \sum_{i=1}^{r} a_i \leq \lambda_1(m) + \lambda_2(m) .$$

*Moreover*

$$h(m) = 1 \text{ if and only if } c + \sum_{i=1}^{r} a_i = \lambda_1(m) + \lambda_2(m) .$$

To use this criterion we remark that $\lambda_1(m) = \sum \tau(f_m(t))$ where $\tau(g)$ denotes the number of positive divisors of $g$ and where the sum is taken over all integers $t \geq P_0$, such that $f_m(t) > 0$, i.e., $P_0 \leq t < \omega$.

Lu's criterion is not the only elementary one which exists in the literature. There are others, some of which we would like to give the flavor of. Here is one of the first to be considered by different authors [Lo1].

THEOREM 1.2. *The class number of the real quadratic field* $\mathbf{Q}(\sqrt{m})$ *is one if and only if* $E(m)$ *contains the set*

$$\{p : p \text{ is prime, } p < \sqrt{\Delta}/2 \text{ and } \chi(p) \neq -1\} ,$$

*where* $\chi$ *is the character associated to* $\mathbf{Q}(\sqrt{m})$. *In other words,*

$$h(m) = 1 \Longleftrightarrow \text{all the non-inert primes smaller than } \sqrt{m}/Q_0 \text{ are in } E(m) .$$

*In practice, if* $h(m) = 1$ *and if a prime* $p$ *divides one of the* $Q_i/Q_0$, *then there exists an integer* $j$ *such that* $p = Q_j/Q_0$.

There is also what is called the real equivalent of the Frobenius-Rabinowitsch criterion [M-W]. Let us quote S. Louboutin's version [Lo2].

THEOREM 1.3. $h(m) = 1$ *if and only if for every integer* $v$ *such that* $0 \leq v < \sqrt{m}/Q_0$, *the prime divisors of* $f_m(v)$ *smaller than* $\sqrt{m}/Q_0$ *are in* $E(m)$.

Let us recall that the theorem of Frobenius-Rabinowitsch is characterizing class number one imaginary quadratic fields with the help of a primality property for the first values of a certain polynomial. In fact an equivalent way of stating Theorem 1.3 is the following one, in which one gets the full flavor of the Rabinowitsch-like criterion, in the sense that the class number one property is translated into the behaviour of the factorization over $\mathbf{Z}$ of $f_m(v)$.

THEOREM 1.4. *$h(m) = 1$ if and only if for every integer $v$ such that $0 \leq v < \sqrt{m}/Q_0$, the part of $f_m(v)$ free from the primes of $E(m)$ smaller than $\sqrt{m}/Q_0$ is 1 or is a prime greater than $\sqrt{m}/Q_0$.*

*Proof.* This follows from Theorem 1.3 if we note that $f_m(v) \leq (\sqrt{m}/Q_0)^2$.

Referring to Lu's theorem, we now want to give precisely which part of $\lambda_1(m) + \lambda_2(m)$ contributes exactly to $c + \sum_{i=1}^{r} a_i$. In fact, the very definition of the class number $h$ tells that $h(m)$ is equal to the number of non equivalent integral ideals of $\mathbf{Q}(\sqrt{m})$. According to Lemma 11 of [Lu], the number of integral ideals of $\mathbf{Q}(\sqrt{m})$ equivalent to $\mathfrak{A} = [1, \omega]$ is $c + \sum_{i=1}^{r} a_i$, where $\omega = [a_0, \overline{a_1, \cdots, a_r}]$ has primitive period length equal to $r$, so $c + \sum_{i=1}^{r} a_i$ is precisely the cardinal of all ideals $\mathfrak{A} = [Q, (P + \sqrt{\Delta})/2]$ such that $P^2 + 4QQ' = \Delta$ and such that $Q$ appears as $Q_i$.

It is now natural to define $\hat{\lambda}_1(m)$ and $\hat{\lambda}_2(m)$ to be the number of solutions of the two Diophantine equations of Theorem 1.1 with the assumption that $y, z \in \hat{E}(m)$, where

$$\hat{E}(m) := \{Q_i/Q_0 : 1 \leq i \leq r, Q_i < \sqrt{m}\} .$$

Therefore $c + \sum_{i=1}^{r} a_i$ is equal to $\hat{\lambda}_1(m)$, to which we add $\hat{\lambda}_2(m)$ to take into account the double contribution of the case $Q = Q'$.

When $m \not\equiv 1 \pmod 4$, $P^2 + 4QQ' = \Delta \Leftrightarrow QQ' = f_m(P/2)$. When $m \equiv 1 \pmod 4$, $P^2 + 4QQ' = \Delta \Leftrightarrow QQ' = f_m((P+1)/2)$. Moreover $f_m(t) \geq 0 \Leftrightarrow P_0 \leq t < \omega$.

Therefore, when we want to solve $P^2 + 4QQ' = \Delta$ with $Q$ equal to $Q_i$ for some $i$, we want to count how many times $f_m(t)$ $(P_0 \leq t < \omega)$ is equal to $QQ'$ with $Q$ equal to $Q_i$ for some $i$. It suggests to define

$$S(g) := \{b : b \mid g \text{ and either } b \in \hat{E}(m) \text{ or } g/b \in \hat{E}(m)\} ,$$

and to let $\hat{\tau}(g)$ be the cardinality of $S(g)$,

$$\hat{\tau}(g) := \sharp(S(g)) .$$

Note the analogy of $\hat{\tau}$ with the function $\tau : \tau(g)$ is the number of divisors of $g$, while $\hat{\tau}(g)$ is the number of divisors of $g$ having a certain property. We now see easily that $\hat{\lambda}_1(m) + \hat{\lambda}_2(m)$ is equal to the sum of all the $\hat{\tau}(f_m(t))$ ($t$ running from $P_0$ to $[\omega]$), to which sum we add $\hat{\lambda}_2(m)$.

In fact, we have proved the following.

THEOREM 1.5. *$c + \sum_{i=1}^{r} a_i = \hat{\lambda}_1(m) + \hat{\lambda}_2(m) = \hat{\lambda}_2(m) + \sum_{P_0 \leq t < \omega} \hat{\tau}(f_m(t))$, (the*

https://doi.org/10.1017/S0027763000003822 Published online by Cambridge University Press

*last sum being taken over all integers* $t \geq P_0$ *such that* $f_m(t) \geq 0$). *Moreover*

$$h(m) = 1 \Longleftrightarrow \lambda_1(m) = \hat{\lambda}_1(m) \quad \text{and} \quad \lambda_2(m) = \hat{\lambda}_2(m)\,.$$

In each of the next sections, the strategy will be the following. In a given parametric family of continued fractions, we will first determine $\hat{E}(m)$, then we will calculate explicitly $\hat{\lambda}_2(m) + \sum_{P_0 \leq t < \omega} \hat{\tau}(f_m(t))$, which quantity once equal to $\lambda_1(m) + \lambda_2(m)$ will provide certain primality conditions equivalent to the unicity of factorization in $Q(\sqrt{m})$.

## § 2. The case $m = (A^k + a)^2 + A$

Let $m$ be the square-free integer defined in [Be] as

$$m := (A^k + a)^2 + A \text{ with } A := 2a + 1;\ a, k \in \mathbf{N}\,.$$

Here $a$ even implies $m \equiv 2 \pmod 4$, and $a$ odd implies $m \equiv 3 \pmod 4$, whereupon $m \equiv a \pmod 2$. We shall always denote $\bar{a}$ the remainder (0 or 1) of the division of $a$ by 2. It follows from N. Nyberg [N] and L. Bernstein [Be1, Be2] that the primitive period length of the continued fraction expansion of $\sqrt{m}$ is $6k$. More precisely, $\sqrt{m} = [a_0, \overline{a_1, \cdots, a_{3k-1}, a_{3k}, a_{3k-1}, \cdots, a_1, 2a_0}]$ with

$$a_0 = A^k + a, \quad a_1 = 2A^{k-1}, \quad a_{3k-1} = 1, \quad a_{3k} = a_0 - 1, \quad a_{6k} = 2a_0\,,$$

and for $k \geq 2$, we have

$$a_{3s-1} = 1, \quad a_{3s} = A^s - 1, \quad a_{3s+1} = 2A^{k-s-1} - 1, \quad 1 \leq s \leq k-1\,,$$
$$Q_{3s-2} = A^s,\ Q_{3s-1} = 2A^k - 2A^{k-s} - A^s + 2a + 2,\ Q_{3s} = 2A^{k-s},\ 1 \leq s \leq k\,.$$

Since $a_{3k} \equiv a \pmod 2$, we have $c = 2 - \bar{a}$, so

$$c + \sum_{i=1}^{6k} a_i = 3A^k + 3a - 2k + 3 - \bar{a} + 6\sum_{i=1}^{k-1} A^i\,.$$

We can prove right away the following preliminary result.

THEOREM 2.1.

(i) *If* $a \equiv 1 \pmod 3$ *with* $a > 1$ *or if* $a \equiv 2 \pmod 3$ *with* $k$ *odd, then* $h(m) > 1$.

(ii) *If* $A$ *is not a prime, then* $h(m) > 1$.

*Proof.* (i) In the former case, we have $m \equiv 1 \pmod 3$ and $\chi(3) = 1$, so 3 is split. In the latter case, we have $m \equiv 0 \pmod 3$, so 3 is ramified. Since $a \neq 1$ we have $3 \notin E(m)$, whence the conclusion by Theorem 1.2.

https://doi.org/10.1017/S0027763000003822 Published online by Cambridge University Press

(ii) Let $A$ be a composite number divisible by the prime $q$. Then $m \equiv a^2 \pmod{q}$ and $\chi(q) = 1$, whence $q$ is a split prime not in $E(m)$. Theorem 1.2 applies again.

In the rest of this chapter, we plan to apply Theorem 1.5. Let us remark that the Diophantine equation $x'^2 + 4yz = 4m$ implies $x' = 2x$ and comes down to $x^2 + yz = m$. Therefore the number $\lambda_1(m)$ of solutions $x' \geq 0$, $y \geq 0$, $z \geq 0$ is equal to

$$\sum_{t=0}^{a_0} \tau(m - t^2) = \sum_{t=0}^{a_0} \tau(f_m(t)) .$$

We have the lower bound,

$$\sum_{t=0}^{a_0} \tau(f_m(t)) \geq \sum_{t=0}^{a_0} \hat{\tau}(f_m(t)) ,$$

and we plan to evaluate this last sum. We easily see that

$$\hat{E}(m) = \{1, 2, A^k, A^t, 2A^t : 1 \leq t \leq k - 1\} ,$$

though a few calculations are in order: for instance $Q_{3s-1} > a_0 = A^k + a$ for $1 \leq s \leq k$, $k \geq 2$. Therefore we want to count to factors of $f_m(s) = m - s^2$ of the following types:

(i) $1$ or $f_m(s)$,

(ii) $2$ or $\dfrac{f_m(s)}{2}$,

(iii) $A^t$ or $\dfrac{f_m(s)}{A^t}$, $(1 \leq t \leq k)$,

(iv) $2A^t$ or $\dfrac{f_m(s)}{2A^t}$, $(1 \leq t \leq k - 1)$.

We are therefore led to consider the following subsets of $\{0, 1, \cdots, a_0\}$:

$$S := \{a + 1, -a - 1 + A^k, a + A^k\}, \quad T := \{0, 1, \cdots, a_0\} \setminus S ,$$
$$G_t := \{a + 1 + uA^t : 1 \leq u \leq A^{k-t} - 1\},$$
$$G'_t := \{-a - 1 + uA^t : 1 \leq u \leq A^{k-t} - 1\}, \quad (1 \leq t \leq k - 1) .$$

As far as the elements of the above sets are concerned, we have:

$$m - (a + 1)^2 = A^k(A^k + 2a), \; m - (-a - 1 + A^k)^2 = 2A^{k+1}, \; m - a_0^2 = A ,$$
$$m - (a + 1 + uA^t)^2 = A^t g_t(u) ,$$
$$m - (-a - 1 + uA^t)^2 = A^t g'_t(u) ,$$

https://doi.org/10.1017/S0027763000003822 Published online by Cambridge University Press

with

$$g_t(u) := A^{2k-t} + 2aA^{k-t} - u^2A^t - 2u(a+1),$$
$$g'_t(u) := A^{2k-t} + 2aA^{k-t} - u^2A^t + 2u(a+1) = g_t(u) + 4u(a+1),$$
$$g_t(u) \equiv 0 \pmod 2 \iff u \equiv 1 \pmod 2 \iff g'_t(u) \equiv 0 \pmod 2.$$

When $s$ runs through $T$, we let $n_1$ be the number of divisors of $f_m(s)$ of type (i), and $n_2$, the number of divisors of type (ii); so when $s$ runs through $T$, there are $n_1 = 2\,\mathrm{card}(T)$ divisors of type (i) and $n_2 = \mathrm{card}(T) + 1 - \bar{a}$ divisors of type (ii) since

$$m - s^2 \equiv 0 \pmod 2 \iff s \equiv a \pmod 2.$$

Note also that for all $s \in T$, $2 \neq f_m(s)/2$, i.e., $4 \neq f_m(s) = m - s^2$, since $4 + s^2 \neq m = (A^k + a)^2 + A$.

When $s$ runs through $G_t \cup G'_t$ for a fixed $t$, we let $n_3(t)$ be the number of divisors of $f_m(s)$ of type (iii); we see that there are $n_3(t) = 2\,\mathrm{card}(G_t \cup G'_t)$ divisors of type (iii). Note here that for all $s \in G_t \cup G'_t$, $A^t$ is never equal to $f_m(s)/A^t$, since the contrary implies $g_t(s) = A^t$ or $g'_t(s) = A^t$; now $g_t(s) > A^t$ since $A^{2k-t} + 2aA^{k-t} > (1+u^2)A^t + 2u(a+1)$; in fact, this last inequality is true for $u = A^{k-t} - 1$, as is easily seen, so it is true for $1 \leq u \leq A^{k-t} - 1$; similarly, $g'_t(s) = g_t(u) + 4u(a+1) > A^t$. Now let $n_4(t)$ stand for the number of divisors of type (iv), so that there are $n_4(t) = \mathrm{card}(G_t) + \mathrm{card}(G'_t)$ divisors of type (iv), since they occur when $u \equiv 1 \pmod 2$; note again that for all $s \in G_t \cup G'_t$, $2A^t$ is never equal to $f_m(s)/(2A^t)$, since the contrary implies $g_t(u) = 4A^t$ or $g'_t(u) = 4A^t$; now $g_t(u) > 4A^t$ since the inequality $A^{2k-t} + 2aA^{k-t} > (4+u^2)A^t + 2u(a+1)$ holds true for $u = A^{k-t} - 2$, the greatest value of $u$ such that $u \equiv 1 \pmod 2$. Similarly $g'_t(u) > 4A^t$. Finally when $s$ runs through $S$, we let $n_5$ stand for the number of divisors of the four types, so that there are $n_5 = 2(k+1) + 2(k+2) + 2 = 4k + 8$ divisors of the four types.

Therefore we obtain for $k \geq 1$,

$$\begin{aligned}\sum_{s=0}^{o_0} \hat{\tau}(m - s^2) &= n_1 + n_2 + n_5 + \sum_{t=1}^{k-1} n_3(t) + n_4(t) \\ &= 3(A^k + a - 2) + (1 - \bar{a}) + 4k + 8 + 2\sum_{t=1}^{k-1} 3(A^{k-t} - 1) \\ &= 3A^k + 3a - 2k + 3 - \bar{a} + 6\sum_{t=0}^{k-1} A^t.\end{aligned}$$

In conclusion we have that $c + \sum_{i=1}^{6k} a_i$ is equal to $\sum_{t \geq 0} \tau(m - t^2)$ if

https://doi.org/10.1017/S0027763000003822 Published online by Cambridge University Press

and only if $\lambda_2(m) = 0$ and the only divisors of $m - t^2$ are those of either type (i), (ii), (iii) or (iv). We can now state the following theorem in which $m$ is defined at the beginning of the chapter, $g_t(u)$ and $g'_t(u)$ are as before, $P$ stands for the set of prime numbers and $2P := \{2p : p \in P\}$.

THEOREM 2.2. *$h(m) = 1 \Leftrightarrow$ the following conditions are satisfied:*

(1) $A \in P$, $A^k + 2a \in P$;

(2) $g'_t(u)$ *and* $g_t(u) \in P \cup 2P$ *for* $1 \leq t \leq k-1$, $1 \leq u \leq A^{k-t} - 1$ *and* $u \not\equiv 0 \pmod{A}$;

(3) $m - v^2 \in P \cup 2P$ *for* $0 \leq v \leq A^k + a - 1$, $v \not\equiv \pm (a+1) \pmod{A}$;

(4) $m$ *is not the sum of two squares.*

*Moreover, this last equivalence holds true for* $(k, a) \in \{(1,1), (1,3), (2,1), (2,2), (3,1)\}$, i.e., *for* $m \in \{19, 103, 107, 734, 787\}$ *and at most for one extra case* (*ruled out by* GRH).

*Proof.* It remains to prove the last assertion, i.e., to find all the pairs $(k, a)$ for which $h(m) = 1$. Like a few authors we will use the theorem of Tatuzawa [T] which states that with at most one possible exception

$$\frac{1}{2} > \delta > 0 \quad \text{and} \quad \Delta \geq \operatorname{Max}(e^{1/\delta}, e^{11.2}) \Longrightarrow L(1, \chi) > 0.655\,\delta \Delta^{-\delta}\,.$$

(By the way, J. Hoffstein [Ho] gives better bounds but the theorem of Tatuzawa is easier to use.) Recall that

$$h(m) = \sqrt{\Delta}\, L(1, \chi)/(2R)\,,$$

where $R$ is the regulator of $\mathbf{Q}(\sqrt{m})$, i.e., the logarithm of the absolute value of

$$\varepsilon = \left(\frac{A^k + a + \sqrt{m}}{A}\right)^{2k} \frac{(A^k + a + 1 + \sqrt{m})^2}{2}\,.$$

We need use an upper bound, $\varepsilon_u$, for $\varepsilon$ (hence for $R$) and a lower bound, $\Delta_l$, for $\Delta$. Since we have $A^k + a < \sqrt{m} < A^k + a + 1$, we deduce:

$$\Delta > \Delta_l := 4A^{2k} \quad \text{and} \quad \varepsilon < \varepsilon_u := 2^{2k+1} A^2 (A^{k-1} + 1)^{2k+2}\,.$$

By Tatuzawa's theorem with $\delta = 1/15$, we know that if $\Delta_l \geq 4A^{2k} > e^{15}$, then $h > 0.655 \Delta_l^{13/30}/(30 \log(\varepsilon_u))$. Now this last term is $> 1$ for $k \geq x$ and $a \geq y$ with $(x, y) = (1,625), (2,25), (3,8), (4,4), (5,3), (6,2), (9,1)$ respectively. We conclude that with one possible exception, $h > 1$ for the above con-

sidered values of $k$ and $a$ under consideration, since the lower bound $\Delta > e^{15}$ is secured in each case. To determine the candidates for the triviality of the class number among the remaining values left aside by the restrictions $k \geq x$ and $a \geq y$, one uses either Theorem 2.1 or the conditions (i) to (iv) of Theorem 2.2, or a table of class numbers. In the case $k = 1$ for instance, only ten values of a (namely 1, 3, 18, 69, 78, 99, 168, 309, 330) satisfy $2a + 1$, $4a + 1 \in P$ and $m \in P \cup 2P$. Hence the conclusion.

EXAMPLE. Let $k = 1$, i.e., $m = 9a^2 + 8a + 2$ with $a \in \mathbf{N}$ and $m$ square-free. Then $h(m) = 1 \Leftrightarrow a = 1$ or 3 (or one extra value ruled out by GRH) $\Leftrightarrow$ the following conditions hold:

(1) $2a + 1$ and $4a + 1 \in P$;

(2) $m - v^2 \in 2P$ for every $v$ with $0 \leq v \leq 3a - 1$, $v \equiv a \pmod 2$, $v \neq a$;

(3) $m - v^2 \in P$ for every $v$ with $0 \leq v \leq 3a - 1$, $v \not\equiv a \pmod 2$, $v \neq a + 1$;

(4) $m$ is not a sum of two squares.

## § 3. Other parametric families

In this chapter we shall deal with 15 other parametric families of real quadratic fields $\mathbf{Q}(\sqrt{m})$ for which it is always ASSUMED $m \not\equiv 1 \pmod 4$ and $m$ square-free. To save space we will refer to the original papers for the $a_i$'s and the $Q_i$'s. The letter $l$ is saved for the primitive length of the continued fraction expansion of $\sqrt{m}$, $c$ is defined in Lu's theorem and $\varepsilon$ will denote the fundamental unit of $\mathbf{Q}(\sqrt{m})$. The proofs follow the pattern of the last chapter, the integers $n_1$, $n_2$, $n_3$, $n_4$ and $n_5$ have a meaning similar to that of Chapter 2, and the details are left to the reader. Unless otherwise specified, $a, k \in \mathbf{N}$, $A := 2a + 1$, $E := 4a - 1$, $B := 2a - 1$.

**3.1.** Let us consider the case considered by N. Nyberg [N] and L. Bernstein [Be1, Be2]:

$$m := (A^k - a)^2 + A .$$

We have

$$m \equiv a \pmod 2, \quad l = 6k - 2 \quad \text{and}$$
$$\varepsilon = \left(\frac{A^k - a + \sqrt{m}}{A}\right)^{2k} \frac{(A^k - a - 1 + \sqrt{m})^2}{2} .$$

We easily find:

https://doi.org/10.1017/S0027763000003822 Published online by Cambridge University Press

$\hat{E}(m) = \{1, 2, A^k, A^t, 2A^t : 1 \leq t \leq k-1\}$, $c = 2 - \bar{a}$;

$S := \{a+1\} \cup \{-a-1+A^k, -a+A^k\}$, $T := \{0, 1, \cdots, A^k - a\} \setminus S$;

$G_t := \{a + 1 + uA^t; 1 \leq u \leq A^{k-t} - 1,\ u \neq A^{k-t} - 1 \text{ when } t = 1\}$,

$G_t' := \{-a - 1 + uA^t : 1 \leq u \leq A^{k-t} - 1\}$,

$g_t(u) := A^{2k-t} - 2aA^{k-t} - u^2A^t - 2u(a+1)$,

$g_t'(u) := g_t(u) + 4u(a+1)$, $(1 \leq t \leq k-1)$;

$n_1 = 2(A^k - a - 2)$ for $k \geq 2$, $n_1 = 2a$ for $k = 1$, $n_2 = A^k - a - 1 - \bar{a}$,

$n_3(t) = 4A^{k-t} - 4$ $(t > 1)$, $n_3(1) = 4A^{k-1} - 6$, $n_4(t) = 2A^{k-t} - 2$,

$n_5 = 4k + 6$ for $k \geq 2$, $n_5 = 6$ for $k = 1$;

$$\sum_{s=0}^{a_0} \hat{\tau}(m - s^2) = 3A^k - 3a - 2k - 1 - \bar{a} + 6\sum_{i=0}^{k-1} A^i = c + \sum_{i=1}^{l} a_i.$$

THEOREM 3.1.1.

(i) *If* $a \equiv 2 \pmod 3$ *with* $k$ *even or if* $a \equiv 1 \pmod 3$ *with* $a \geq 4$, *then* $h(m) > 1$.

(ii) *If* $A$ *is not prime, then* $h(m) > 1$.

*Proof.*

(i) In the former case, $m \equiv 0 \pmod 3$, 3 is ramified and $3 \notin E(m)$ as seen in [Be1], so $h(m) > 1$. In the latter case, $m \equiv 1 \pmod 3$, 3 is split and $3 \notin E(m)$, whence $h(m) > 1$.

(ii) As for Theorem 2.1 (ii).

THEOREM 3.1.2. $h(m) = 1 \Leftrightarrow$ *the following conditions are satisfied*:

(1) $A \in P$ *and for* $k > 1$, $A^k - 2a \in P$;

(2) $g_t(u)$ *and* $g_t'(u) \in P \cup 2P$ *for* $1 \leq t \leq k-1$, $1 \leq u \leq A^{k-t} - 1$ (*though* $u \neq A^{k-1} - 1$ *if* $g_1(u)$ *is considered*) *and* $u \not\equiv 0 \pmod A$;

(3) $m - v^2 \in P \cup 2P$ *for* $0 \leq v \leq A^k - a - 1$, $v \not\equiv \pm(a+1) \pmod A$;

(4) $m$ *is not the sum of two squares.*

*Moreover this last equivalence holds true for* $(k, a) \in \{(1,1), (1,2), (1,3), (1,5), (1,6), (1,11), (1,18), (2,1)\}$, i.e., *for* $m \in \{7, 14, 23, 47, 62, 67, 167, 398\}$ *and at most for one extra case* (*ruled out by* GRH).

*Proof.* We proceed as for Theorem 2.2. By [T] with $\delta = 1/15$ we have $h > 1$ for $k \geq x$ and $a \geq y$ with $(x, y) = (1, 900), (2, 25), (3, 8), (4, 4), (5, 3), (6, 2), (9, 1)$ respectively and we have only eight (or nine) cases for which $h(m) = 1$. For these eight values of $m$ the quadratic field is of Richaud-Degert type [M-W].

**3.2.** In [Be1, Be2], L. Bernstein dealt with the case

$$m := (A^k + a + 1)^2 - A\,,$$

for which we know

$$m \not\equiv a \pmod 2,\ l = 4k + 2 \quad \text{and}$$
$$\varepsilon = \left(\frac{A^k + a + 1 + \sqrt{m}}{A}\right)^{2k} \frac{(A^k + a + \sqrt{m})^2}{2}\,.$$

Here we get:

$\hat{E}(m) = \{1, 2, A^k, A^t, 2A^t : 1 \le t \le k - 1\}$, $c = 1 + \bar{a}$;
$S := \{a, -a + A^k, a + A^k\}$, $T := \{0, 1, \cdots, A^k + a\} \setminus S$;
$G_t := \{a + uA^t : 1 \le u \le A^{k-t} - 1\}$, $G_t' := \{-a + uA^t : 1 \le u \le A^{k-t} - 1\}$,
$g_t(u) := A^{2k-t} + 2(a + 1)A^{k-t} - u^2A^t - 2au$,
$g_t'(u) := g_t(u) + 4au$, $(1 \le t \le k - 1)$;
$n_1 = 2A^k + 2a - 4$, $n_2 = A^k + a - 3 + \bar{a}$, $n_5 = 6k + 8$,
$n_3(t) = 4(A^{k-t} - 1)$, $n_4(t) = 2(A^{k-t} - 1)$ $(1 \le t \le k - 1)$;
$$\sum_{s=0}^{a_0} \hat{\tau}(m - s^2) = 3A^k + 3a + 1 + \bar{a} + 6\sum_{i=0}^{k-1} A^i = c + \sum_{i=1}^{l} a_i.$$

THEOREM 3.2.1.

(i) *If* $a \not\equiv 2 \pmod 3$ *and* $a > 2$, *then* $h(m) > 1$.
(ii) *If* $A$ *is not prime, then* $h(m) > 1$.

*Proof.*

(i) If $a \equiv 1 \pmod 3$, then $m \equiv 1 \pmod 3$, 3 is split whence the conclusion since $3 \notin E(m)$ (as seen in [Be1]). If $a \equiv 0 \pmod 3$, then $m \equiv 0 \pmod 3$, i.e., 3 is ramified, whereupon $h(m) > 1$ since $3 \notin E(m)$.
(ii) As before.

THEOREM 3.2.2. $h(m) = 1 \Leftrightarrow$ *the following conditions are satisfied*:

(1) $A \in P$, $A^k + 2a + 2 \in P$;
(2) $g_t(u)$ *and* $g_t'(u) \in P \cup 2P$ *for* $1 \le t \le k - 1$, $1 \le u \le A^{k-t} - 1$, $u \not\equiv 0 \pmod A$;
(3) $m - v^2 \in P \cup 2P$ *for* $0 \le v \le A^k + a - 1$, $v \not\equiv \pm a \pmod A$;
(4) $m$ *is not the sum of two squares.*

*Moreover this last equivalence holds true for* $(k, a) \in \{(1, 1), (1, 2), (1, 5), (2, 1), (3, 1)\}$, i.e., *for* $m \in \{22, 59, 118, 278, 838\}$ *and at most for one extra case* (*ruled out by* GRH).

https://doi.org/10.1017/S0027763000003822 Published online by Cambridge University Press

*Proof.* As for Theorem 2.2. By [T] we have $h > 1$ for $k \geq x$ and $a \geq y$ with $(x, y) = (1, 355), (2, 25), (3, 8), (4, 4), (5, 3), (6, 2), (9, 1)$ respectively and we have only five (or six) cases for which $h(m) = 1$.

**3.3.** Let us now concentrate on the following family of L. Bernstein [Be1, Be2]:

$$m := (A^k - a - 1)^2 - A, \ a \geq 2, \ k \geq 2.$$

We have

$$m \not\equiv a \pmod 2, \quad l = 8k - 4 \quad \text{and}$$
$$\varepsilon = \left(\frac{A^k - a - 1 + \sqrt{m}}{A}\right)^{2k} \frac{(A^k - a + \sqrt{m})^2}{2}.$$

We easily find:

$$\hat{E}(m) = \{1, 2, A^t, 2A^t : 1 \leq t \leq k - 1\}, \quad c = 1 + \bar{a};$$
$$S := \{a\}, \quad T := \{0, 1, \cdots, A^k - a - 2\} \setminus S;$$
$$G_t := \{a + uA^t : 1 \leq u \leq A^{k-t} - 1, \ u \neq A^{k-1} - 1 \text{ when } t = 1\},$$
$$G'_t := \{-a + uA^t : 1 \leq u \leq A^{k-t} - 1\},$$
$$g_t(u) := A^{2k-t} - 2(a + 1)A^{k-t} - u^2A^t - 2ua,$$
$$g'_t(u) := g_t(u) + 4ua, \ (1 \leq t \leq k - 1);$$
$$n_1 = 2A^k - 2a - 4, \quad n_2 = A^k - a - 1 + \bar{a}, \quad n_5 = 2k + 2,$$
$$n_3(t) = 4A^{k-t} - 4 \text{ (except } n_3(1) = 4A^{k-1} - 6), \quad n_4(t) = 2A^{k-t} - 2$$
$$(1 \leq t \leq k - 1);$$
$$\sum_{s=0}^{a_0} \hat{\tau}(m - s^2) = 3A^k - 3a - 4k - 5 + \bar{a} + 6\sum_{i=0}^{k-1} A^i = c + \sum_{i=1}^{l} a_i.$$

THEOREM 3.3.1.

(i) *If* $a \equiv 1 \pmod 3$ *with* $a \geq 4$ (*and* $k \geq 2$), *then* $h(m) > 1$.

(ii) *If* $A$ *is not prime, then* $h(m) > 1$.

*Proof.*

(i) We have that $m \equiv 1 \pmod 3$ and 3 is split. By [Be1], $3 \notin E(m)$, whence the conclusion.

(ii) As before.

THEOREM 3.3.2. $h(m) = 1 \Leftrightarrow$ *the following conditions are satisfied*:

(1) $A \in P$, $A^k - 2a - 2 \in P$;

(2) $g_t(u)$ *and* $g'_t(u) \in P \cup 2P$ *for* $1 \leq t \leq k - 1$, $1 \leq u \leq A^{k-t} - 1$ (*though* $u \neq A^{k-1} - 1$ *if* $g_1(u)$ *is considered*) *and* $u \not\equiv 0 \pmod A$;

https://doi.org/10.1017/S0027763000003822 Published online by Cambridge University Press

(3) $m - v^2 \in P \cup 2P$ *for* $0 \leqq v \leqq A^k - a - 2$, $v \not\equiv \pm a \pmod{A}$;

(4) $m$ *is not the sum of two squares.*

*This last equivalence holds true for* $(k, a) \in \{(2, 1), (2, 2), (3, 1)\}$, *i.e., for* $m \in \{46, 479, 622\}$ *and at most for one extra case* (*ruled out by* GRH).

*Proof.* We proceed as for Theorem 2.2. By [T] we have $h(m) > 1$ for $k \geq x$ and $a \geq y$ with $(x, y) \in (2, 25), (3, 8), (4, 4), (5, 3), (6, 2), (9, 1)$ respectively and we have only three (or four) cases for which $h(m) = 1$.

*Remark.* The case where $k = 1$ and $m = (a - 1)^2 - 2$ is a Richaud-Degert case already considered by R. Mollin [M1] and S. Louboutin [Lo1]. Here $h(m) = 1 \Leftrightarrow m - v^2 \in P \cup 2P$ for $0 \leq v \leq a - 2 \Leftrightarrow m \in \{2, 7, 14, 23, 47, 62, 167, 398\}$ and at most for one extra value (ruled out by GRH).

**3.4.** Let us concentrate now on a parametric family considered by C. Levesque and G. Rhin [Le-R]:

$$m := (2aE^k + a)^2 - 2aE^k, \quad E := 4a - 1, \quad a \text{ odd and square-free.}$$

It is known that

$$l = 6k + 4 \quad \text{and} \quad \varepsilon = \left(\frac{4aE^k + 2a - 1 + 2\sqrt{m}}{E}\right)^{2k} \frac{(2aE^k + a + \sqrt{m})^2}{2a}.$$

Here we have:

$$\hat{E}(m) := \{1, 2a, E^t, 2aE^t : 1 \leq t \leq k\}, \quad m \equiv 3 \pmod 4, \quad c = 1;$$

$$S := \{a, -a + 2aE^k, a + (2a - 1)E^k\}, \quad T := \{0, 1, \cdots, 2aE^k + a - 1\} \setminus S;$$

$$G_t := \{a + uE^t : 1 \leq u \leq 2aE^{k-t} - 1\},$$

$$G'_t := \{-a + uE^t : 1 \leq u \leq 2aE^{k-t} - 1\},$$

$$g_t(u) := 4a^2E^{2k-t} + 4a^2E^{k-t} - 2aE^{k-t} - u^2E^t - 2ua,$$

$$g'_t(u) := g_t(u) + 4ua, \quad (1 \leq t \leq k);$$

$$g_t(u) \equiv 0 \pmod{2a} \Leftrightarrow u \equiv 0 \pmod{2a} \Leftrightarrow g'_t(u) \equiv 0 \pmod{2a}.$$

Let us look at the contribution of the elements of $\hat{E}(m)$ as divisors of $m - s^2$: when $s$ runs through $T$, there are $n_1 = 2$ card $(T) = 4aE^k - 2a - 6$ divisors of $m - s^2$ of the type (i) (i.e., of the form 1, $m - s^2$), and there are $n_2 = 2[(2aE^k + a - 1)/2a] = 2E^k$ divisors of the type (ii) (i.e., of the form $2a$, $(m - s^2)/(2a)$). When $s$ runs through $G_t \cup G'_t$, there are $n_3(t) = 2$ card $(G_t \cup G'_t) = 8aE^{k-t} - 4$ divisors of the type (iii) (i.e., of the form $E^t$, $(m - s^2)/E^t$) and there are $n_4(t) = 4[(2aE^{k-t} - 1)/(2a)] = 4E^{k-t} - 4$ divisors of the type (iv) (i.e., of the form $2aE^t$, $(m - s^2)/(2aE^t)$. The set $S$ contri-

https://doi.org/10.1017/S0027763000003822 Published online by Cambridge University Press

butes to $n_5 = 6k + 8$ divisors. So we obtain

$$\sum_{s=0}^{a_0} \hat{\tau}(m - s^2) = (4a + 2)E^k + 2a - 2k + (8a + 4)\sum_{i=0}^{k-1} E^i = c + \sum_{i=1}^{l} a_i .$$

THEOREM 3.4.1. *If* $a > 1$, *then* $h(m) > 1$.

*Proof.* For $q$, a prime dividing $a$, we have $q \mid m$, $q < \sqrt{m}$ and $q \notin E(m)$. (Another reason is that for $a > 1$, 2 is ramified and $2 \notin E(m)$.)

THEOREM 3.4.2. *Let* $a = 1$. *Then* $h(m) = 1 \Leftrightarrow$ *the following conditions are satisfied*:

(1) $2 \cdot 3^k + 1 \in P$;

(2) *for* $1 \leq t \leq k$, $1 \leq u \leq 2 \cdot 3^{k-t} - 1$ *and* $u \not\equiv 0 \pmod 3$, $g_t(u)$ *and* $g_t'(u) \in P \cup 2P$;

(3) $m - v^2 \in P \cup 2P$ *for* $0 \leq v \leq 2 \cdot 3^k$, $v \not\equiv \mp 1 \pmod 3$.

*Moreover this last equivalence holds true for* $k = 1$ $(m = 43)$ *and at most for one extra case (ruled out by* GRH).

*Proof.* As for Theorem 2.2, we use [T] to get $h > 1$ for $k \geq 9$; then we find $h = 1$ for one case (or two).

*Remark.* If we had stated Theorem 3.4.2 for arbitrary $a$, one of the conditions would read $g_t(u) \in P \cup 2P$, which clearly cannot always be fulfilled for $k \geq 2$ and $a \geq 2$, since $2a \mid g_t(2a)$.

**3.5.** We want to concentrate on this family:

$$m := (2aE^k - a)^2 + 2aE^k, \quad E := 4a - 1, \quad a \text{ odd and square-free.}$$

It was shown in [Le-R] that

$$l = 6k + 2 \quad \text{and} \quad \varepsilon = \left(\frac{4aE^k - 2a + 1 + 2\sqrt{m}}{E}\right)^{2k} \frac{(2aE^k - a + \sqrt{m})^2}{2a} .$$

Here we get

$$\hat{E}(m) := \{1, 2a, E^k, E^t, 2aE^t : 1 \leq t \leq k - 1\},\ m \equiv 3 \pmod 4,\ c = 1;$$
$$S := \{a, -a + 2aE^k, -a + (2a - 1)E^k\},\ T := \{0, 1, \cdots, 2aE^k - a\} \setminus S;$$
$$G_t := \{a + uE^t : 1 \leq u \leq 2aE^{k-t} - 1,\ u \neq 2a - 1 \text{ if } t = k\},$$
$$G_t' := \{-a + uE^t : 1 \leq u \leq 2aE^{k-t} - 1\},$$
$$g_t(u) := 4a^2E^{2k-t} - 4a^2E^{k-t} + 2aE^{k-t} - u^2E^t - 2ua,$$
$$g_t'(u) := g_t(u) + 4ua,\ (1 \leq t \leq k);$$
$$g_t(u) \equiv 0 \pmod{2a} \Leftrightarrow u \equiv 0 \pmod{2a} \Leftrightarrow g_t'(u) \equiv 0 \pmod{2a};$$

https://doi.org/10.1017/S0027763000003822 Published online by Cambridge University Press

$$n_1 = 4aE^k - 2a - 4, \quad n_2 = 2E^k, \quad n_5 = 6k + 6,$$
$$n_3(t) = 8aE^{k-t} - 4 \ (t > 1), \quad n_3(1) = 8a - 6, \quad n_4(t) = 4E^{k-t} - 4;$$
$$\sum_{s=1}^{a_0} \hat{\tau}(m - s^2) = (4a + 2)E^k - 2a - 2k + (8a + 4)\sum_{i=0}^{k-1} E^i = c + \sum_{i=1}^{l} a_i.$$

THEOREM 3.5.1. *If $a > 1$, then $h(m) > 1$.*

*Proof.* One proceeds as for Theorem 3.4.1.

THEOREM 3.5.2. *Let $a = 1$. Then $h(m) = 1 \Leftrightarrow$ the following conditions are satisfied*:

(1) $2 \cdot 3^k - 1 \in P$;

(2) *for* $1 \leq t \leq k$, $1 \leq u \leq 2 \cdot 3^{k-t} - 1$ *and* $u \equiv 0 \pmod 3$, $g_t(u)$ *and* $g_t'(u) \in P \cup 2P$;

(3) $m - v^2 \in P \cup 2P$ *for* $0 \leq v \leq 2 \cdot 3^k - 1$, $v \not\equiv \mp 1 \pmod 3$.

*This last equivalence holds true for $k \in \{1, 2\}$*, i.e., *for $m \in \{31, 307\}$, and at most for one extra case* (*ruled out by* GRH).

*Proof.* As for Theorem 2.2, we have $h(m) > 1$ if $k \geq 7$.

**3.6.** This section is devoted to this family:

$$m := (aE^k + a)^2 - aE^k, \quad E := 4a - 1, \quad a \text{ square-free} > 1.$$

It was proved in [Le-R] that

$$l = 6k + 4 \quad \text{and} \quad \varepsilon = \left(\frac{2aE^k + 2a - 1 + 2\sqrt{m}}{E}\right)^{2k} \frac{(aE^k + a + \sqrt{m})^2}{a}.$$

If $a \equiv 2 \pmod 4$ then $m \equiv 2 \pmod 4$. If $a \equiv 1 \pmod 4$ with $k$ even or if $a \equiv 3 \pmod 4$ with $k$ odd, then $m \equiv 3 \pmod 4$. Moreover

$$\hat{E}(m) := \{1, a, E^t, aE^t : 1 \leq t \leq k\}, \ c = 2;$$
$$S := \{a, -a + aE^k\}, \quad T := \{0, 1, \cdots, aE^k + a - 1\} \setminus S;$$
$$G_t := \{a + uE^t : 1 \leq u \leq aE^{k-t} - 1\},$$
$$G_t' := \{-a + uE^t : 1 \leq u \leq aE^{k-t} - 1\},$$
$$g_t(u) := a^2E^{2k-t} + 2a^2E^{k-t} - aE^{k-t} - u^2E^t - 2ua,$$
$$g_t'(u) := g_t(u) + 4ua, \quad (1 \leq t \leq k);$$
$$n_1 = 2aE^k + 2a - 6, \quad n_2 = 2aE^k, \quad n_5 = 6k + 8,$$
$$n_3(t) = 4aE^{k-t} - 4, \quad n_4(t) = 4E^{k-t} - 4, \quad (1 \leq t \leq k);$$
$$\sum_{s=0}^{a_0} \hat{\tau}(m - s^2) = (2a + 2)E^k + 2a - 2k + 2 + (4a + 4)\sum_{i=0}^{k-1} E^i = c + \sum_{i=1}^{l} a_i.$$

https://doi.org/10.1017/S0027763000003822 Published online by Cambridge University Press

THEOREM 3.6.1. *If* $a \neq 2$, *then* $h(m) > 1$.

*Proof.* If $a \neq 2$, then $2 \notin E(m)$ and 2 is ramified. Hence $h(m) > 1$.

THEOREM 3.6.2. *Let* $a = 2$. *Then* $h(m) = 1 \Leftrightarrow$ *the following conditions are satisfied*:

(1) $2 \cdot 7^k + 3 \in P$;

(2) $g_t(u)$ *and* $g'_t(u) \in P \cup 2P$ *for* $1 \leq t \leq k$, $1 \leq u \leq 2 \cdot 7^{k-t} - 1$ *and* $u \not\equiv 0 \pmod 7$;

(3) $m - v^2 \in P \cup 2P$ *for* $0 \leq v \leq 2 \cdot 7^k + 1$, $v \not\equiv 0 \pmod 7$;

(4) $m$ *is not the sum of two squares.*

*In fact, those conditions hold simultaneously for at most one value of* $k$ (*ruled out by* GRH).

*Proof.* By [T], we have $h > 1$ for $k \geq 7$. No $k \leq 6$ gives $h = 1$.

**3.7.** In this section we deal with the family [Le-R]:

$$m := (aE^k - a)^2 + aE^k, \quad E := 4a - 1, \quad a \text{ square-free} > 1.$$

We know that

$$l = 6k + 2 \quad \text{and} \quad \varepsilon = \left(\frac{2aE^k - 2a + 1 + 2\sqrt{m}}{E}\right)^{2k} \frac{(aE^k - a + \sqrt{m})^2}{a}.$$

If $a \equiv 2 \pmod 4$ then $m \equiv 2 \pmod 4$. If $a \equiv 1 \pmod 4$ with $k$ even or if $a \equiv 3 \pmod 4$ with $k$ odd, then $m \equiv 3 \pmod 4$. Moreover

$$\hat{E}(m) := \{1, a, E^k, E^t, aE^t : 1 \leq t \leq k - 1\}, \quad c = 2;$$
$$S := \{a, -a + aE^k\}, \quad T := \{0, 1, \cdots, aE^k - a\} \setminus S;$$
$$G_t := \{a + uE^t : 1 \leq u \leq aE^{k-t} - 1\},$$
$$G'_t := \{-a + uE^t : 1 \leq u \leq aE^{k-t} - 1\},$$
$$g_t(u) := a^2E^{2k-t} - 2a^2E^{k-t} + aE^{k-t} - u^2E^t - 2ua,$$
$$g'_t(u) := g_t(u) + 4ua, \quad (1 \leq t \leq k);$$
$$n_1 = 2aE^k - 2a - 2, \quad n_2 = 2E^k - 2, \quad n_5 = 6k + 6,$$
$$n_3(t) = 4aE^{k-t} - 4, \quad n_4(t) = 4E^{k-t} - 4;$$
$$\sum_{s=0}^{a_0} \hat{\tau}(m - s^2) = (2a + 2)E^k - 2a - 2k + (4a + 4) \sum_{i=1}^{k-1} E^i = c + \sum_{i=1}^{l} a_i.$$

THEOREM 3.7.1. *If* $a \neq 2$, *then* $h(m) > 1$.

*Proof.* If $a \neq 2$, $2 \notin E(m)$ and 2 is ramified. Hence $h(m) > 1$.

THEOREM 3.7.2. *Let* $a = 2$. *Then* $h(m) = 1 \Leftrightarrow$ *the following conditions*

https://doi.org/10.1017/S0027763000003822 Published online by Cambridge University Press

*are satisfied*:

(1) $2\cdot 7^k - 3 \in P$;

(2) $g(u)$ *and* $g_t'(u) \in P \cup 2P$ *for* $1 \leq t \leq k$, $1 \leq u \leq 2\cdot 7^{k-t} - 1$ *and* $u \not\equiv 0 \pmod 7$;

(3) $m - v^2 \in P \cup 2P$ *for* $0 \leq v \leq 2\cdot 7^k - 2$, $v \not\equiv 0 \pmod 7$;

(4) $m$ *is not the sum of two squares.*

*In fact, those conditions hold simultaneously for* $k = 1$, *i.e., for* $m = 158$, *and at most for one extra case (ruled out by* GRH).

*Proof.* By [T] we have $h > 1$ for $k \geq 5$.

**3.8.** Let us concentrate on this family considered by C. Levesque and G. Rhin [Le-R]:

$$m = (aF^k + a)^2 - F^k, \quad F := 4a^2 - 1 \quad \text{and} \quad k \text{ even}, \ m \equiv 3 \pmod 4.$$

It is known that

$$l = 3k + 2 \quad \text{and} \quad \varepsilon = \left(\frac{2a^2F^k + 2a^2 - 1 + 2a\sqrt{m}}{F}\right)^k (aF^k + a + \sqrt{m}).$$

We come up with:

$$\hat{E}(m) = \{1, F^t : 1 \leq t \leq k\}, \ c = 1;$$

$$S := \{a, -a + aF^k\}, \quad T := \{0, 1, \cdots, aF^k + a - 1\} \setminus S;$$

$$G_t := \{a + uF^t : 1 \leq u \leq aF^{k-t} - 1\},$$

$$G_t' := \{-a + uF^t : 1 \leq u \leq aF^{k-t} - 1\},$$

$$g_t(u) := a^2F^{2k-t} + 2a^2F^{k-t} - F^{k-t} - u^2F^t - 2ua,$$

$$g_t'(u) := g_t(u) + 4ua, \quad (1 \leq t \leq k);$$

$$n_1 = 2aF^k + 2a - 4, \quad n_5 = 3k + 4, \quad n_3(t) = 4aF^{k-t} - 4,$$

(no need of $n_2 = 0$, $n_4(t) = 0$);

$$\sum_{s=0}^{a_0} \hat{\tau}(m - s^2) = 2aF^k + 2a - k + 4a \sum_{i=0}^{k-1} F^i = c + \sum_{i=1}^{l} a_i.$$

THEOREM 3.8.1. $h(m) > 1$.

*Proof.* By Lu's theorem, to have $h = 1$ forces $F = (2a + 1)(2a - 1)$ to be prime, i.e., $a = 1$. Moreover it forces $a^2F^k + 2a^2 - 1 = 3^k + 1$ to be prime, which never happens. Another argument comes from the fact that 2 is ramified and $2 \notin E(m)$.

**3.9.** Another family of C. Levesque and G. Rhin [Le-R] for which $F := 4a^2 - 1$, is:

https://doi.org/10.1017/S0027763000003822 Published online by Cambridge University Press

$$m := (aF^k - a)^2 + F^k, \quad k \text{ odd}, \quad m \equiv 3 \pmod 4 .$$

It was proved that

$$l = 3k + 1 \quad \text{and} \quad \varepsilon = \left(\frac{2a^2F^k - 2a^2 + 1 + 2a\sqrt{m}}{F}\right)^k (aF^k - a + \sqrt{m}) .$$

We then find:

$$\hat{E}(m) = \{1, F^t : 1 \le t \le k - 1\}, \quad c = 1;$$
$$S := \{a, -a + aF^k\}, \quad T := \{0, 1, \cdots, aF^k - a\} \setminus S;$$
$$G_t := \{a + uF^t : 1 \le u \le aF^{k-t} - 1\},$$
$$G_t' := \{-a + uF^t : 1 \le u \le aF^{k-t} - 1\},$$
$$g_t(u) := a^2F^{2k-t} + 2a^2F^{k-t} + F^{k-t} - u^2F^t - 2ua,$$
$$g_t'(u) := g_t(u) + 4ua, \quad (1 \le t \le k);$$
$$n_1 = 2aF^k - 2a - 2, \quad n_5 = 3k + 3, \quad n_3(t) = 4aF^{k-t} - 4;$$
$$\sum_{s=0}^{a_0} \hat{\tau}(m - s^2) = 2aF^k - 2a - k + 1 + 4a \sum_{i=0}^{k-1} F^i = c + \sum_{i=1}^{l} a_i .$$

THEOREM 3.9.1. *If $m > 7$, then $h(m) > 1$.*

*Proof.* By Lu's theorem, to have $h = 1$ forces $F$ to be prime, i.e., $a = 1$. Moreover it forces $m - a^2 = a^2F^k - 2a^2 + 1 = 3^k - 1$ to be prime, which is possible only for $k = 1$. Note also that 2 is ramified and that $2 \notin E(m)$ for $(a, k) \neq (1, 1)$.

**3.10.** C. Levesque [Le] took $B = 2a - 1$ with $a > 1$ in the following parametric family:

$$m := (aB^k - a)^2 + 2aB^k, \quad a \text{ odd and square-free},$$

and proved that

$$l = 6k - 2 \quad \text{and} \quad \varepsilon = \left(\frac{aB^k - a + 1 + \sqrt{m}}{B}\right)^{2k} \frac{(aB^k - a + \sqrt{m})^2}{2a} .$$

Let us illustrate Theorem 1.5. Here we have (cf. Section 3.4 for the details of the argument):

$$\hat{E}(m) := \{1, 2a, B^k, B^t, 2aB^t : 1 \le t \le k - 1\}, \quad c = 2;$$
$$S := \{a, -a + aB^k, aB^k - a + 1\}, \quad T := \{0, 1, \cdots, aB^k - a + 1\} \setminus S;$$
$$G_t := \{a + uB^t : 1 \le u \le aB^{k-t} - 1, \ u \neq aB^{k-1} - 1 \text{ if } t = 1\},$$
$$G_t' := \{-a + uB^t : 1 \le u \le aB^{k-t} - 1\},$$

https://doi.org/10.1017/S0027763000003822 Published online by Cambridge University Press

$g_t(u) := a^2B^{2k-t} - 2a^2B^{k-t} + 2aB^{k-t} - u^2B^t - 2ua,$
$g'_t(u) = g_t(u) + 4ua, \quad (1 \le t \le k);$
$g_t(u) \equiv 0 \pmod{2a} \Leftrightarrow a \mid u$ with odd $u \Leftrightarrow g'_t(u) \equiv 0 \pmod{2a}$;
$n_1 = 2aB^k - 2a - 2, \quad n_2 = B^k - 1, \quad n_5 = 4k + 6, \quad n_3(1) = 4aB^{k-1} - 6,$
$n_3(t) = 4aB^{k-t} - 4 \ (2 \le t \le k), \quad n_4(t) = 2B^{k-t} - 2 \ (1 \le t \le k).$
$\sum_{s=0}^{a_0} \hat{\tau}(m - s^2) = (2a + 1)B^k - 2a - 2k + 1 + (4a + 2)\sum_{i=0}^{k-1} B^i.$

THEOREM 3.10.1. $h(m) > 1$.

*Proof.* By Lu's theorem, to have $h = 1$ forces $2a$ to be prime, a contradiction since $a > 1$. Another argument is that $2 \notin E(m)$ and $2 \mid 2a = Q_{3k-1}$.

**3.11.** The following family was also considered in [Le]:

$m := (aB^k + a)^2 - 2aB^k, \quad B = 2a - 1, \ a > 1$ odd and square-free.

It was proved that

$$l = 6k \quad \text{and} \quad \varepsilon = \left(\frac{aB^k + a - 1 + \sqrt{m}}{B}\right)^{2k} \frac{(aB^k + a + \sqrt{m})^2}{2a}.$$

As before, we will only illustrate Theorem 1.5. Here

$\hat{E}(m) := \{1, 2a, B^k, B^t, 2aB^t : 1 \le t \le k - 1\}, \ c = 2;$
$S := \{a, -a + aB^k, aB^k + a - 1\}, \quad T = \{0, 1, \cdots, aB^k + a - 1\} \setminus S;$
$G_t := \{a + uB^t : 1 \le u \le aB^{k-t} - 1\},$
$G'_t := \{-a + uB^t : 1 \le u \le aB^{k-t} - 1\},$
$g_t(u) := a^2B^{2k-t} + 2a^2B^{k-t} - 2aB^{k-t} - u^2B^t - 2ua,$
$g'_t(u) := g_t(u) + 4ua, \ (1 \le t \le k);$
$g_t(u) \equiv 0 \pmod{2a} \Leftrightarrow a \mid u$ with odd $u \Leftrightarrow g'_t(u) \equiv 0 \pmod{2a}$;
$\sum_{i=1}^{l} a_i = (2a + 1)B^k + 2a - 1 - 2k + 2(2a + 1)\sum_{i=0}^{k-1} B^i.$

As in Section 3.4, we find

$n_1 = 2aB^k + 2a - 6, \quad n_2 = B^k - 1, \quad n_3(t) = 4aB^{k-t} - 4,$
$n_4(t) = 2B^{k-t} - 2, \quad n_5 = 4k + 8,$
$\sum_{s=0}^{a_0} \hat{\tau}(m - s^2) = (2a + 1)B^k + 2a - 2k - 1 + (4a + 2)\sum_{i=0}^{k-1} B^i.$

THEOREM 3.11.1. $h(m) > 1$.

*Proof.* This follows from $2 \notin E(m)$, $2 | 2a = Q_{3k}$, or from Lu's theorem as before.

**3.12.** We take from [Le] the case:

$$m := (aA^k + a)^2 + 2aA^k, \ a \text{ odd and square-free,}$$

for which

$$l = 4k + 2 \quad \text{and} \quad \varepsilon = \left(\frac{aA^k + a - 1 + \sqrt{m}}{A}\right)^{2k} \frac{(aA^k + a + \sqrt{m})^2}{2a}.$$

To illustrate Theorem 1.5, one finds

$$\hat{E}(m) := \{1, 2a, A^k, A^t, 2aA^t : 1 \leq t \leq k - 1\}, \ c = 2;$$
$$S := \{a, -a + aA^k, a + aA^k\}, \quad T := \{0, 1, \cdots, aA^k + a\} \setminus S;$$
$$G_t := \{a + uA^t : 1 \leq u \leq aA^{k-t} - 1\},$$
$$G_t' := \{-a + uA^t : 1 \leq u \leq aA^{k-t} - 1\},$$
$$g_t := a^2A^{2k-t} + 2a^2A^{k-t} + 2aA^{k-t} - u^2A^t - 2au,$$
$$g_t'(u) := g_t(u) + 4au, \ (1 \leq t \leq k);$$
$$n_1 = 2aA^k + 2a - 4, \quad n_2 = A^k - 1, \quad n_5 = 6k + 8,$$
$$n_3(t) = 4aA^{k-t} - 4, \quad n_4(t) = 2A^{k-t} - 2;$$
$$c + \sum_{i=1}^{l} a_i = (2a + 1)A^k + 2a + 3 + 2(2a + 1)\sum_{t=0}^{k-1} A^t = \sum_{s=0}^{a_0} \hat{\tau}(m - s^2).$$

THEOREM 3.12.1. *If* $a > 1$, *then* $h(m) > 1$.

*Proof.* For $a > 1$, $2 | 2a = Q_{2k+1}$ and $2 \notin E(m)$.

When $a = 1$, the integer $m$ of this section is the same $m$ as in Section 3.2, whereupon we see from Theorem 3.2.2 that only $m = 22$, 118 and 838 have to be considered.

**3.13.** The next family is taken from [Le]:

$$m := (aA^k - a)^2 - 2aA^k, \ a \text{ odd and square-free (here } a > 1 \text{ if } k = 1).$$

It was proved that

$$l = 8k \text{ if } a \geq 3, \quad l = 8k - 4 \text{ if } a = 1 \quad \text{and} \quad k \geq 2,$$
$$\varepsilon = \left(\frac{aA^k - a - 1 + \sqrt{m}}{A}\right)^{2k} \frac{(aA^k - a + \sqrt{m})^2}{2a}.$$

To illustrate Theorem 1.5, one finds $c$, $\hat{E}(m)$ as in Section 3.12 and obtains

$S := \{a\}, \quad T = \{0, 1, \cdots, aA^k - a - 2\} \setminus S;$
$G_t := \{a + uA^t : 1 \leq u \leq aA^{k-t} - 1\},$
$G'_t = \{-a + uA^t : 1 \leq u \leq aA^{k-t} - 1\},$
$g_t := a^2A^{2k-t} - 2a(a+1)A^{k-t} - u^2A^t - 2au,$
$g'_t(u) := g_t(u) + 4au, \ (1 \leq t \leq k);$
$n_1 = 2aA^k - 2a - 4, \quad n_2 = A^k - 3, \quad n_5 = 2k + 2,$
$n_3(t) = 4aA^{k-t} - 4 \ (t > 1), \quad n_3(1) = 4aA^{k-1} - 6, \quad n_4(t) = 2A^{k-t} - 2;$

$$c + \sum_{i=1}^{l} a_i = c + (2a+1)A^k - 2a - 4k - 7 + 2(2a+1)\sum_{i=0}^{k-1} A^i$$
$$= \sum_{i=1}^{a_0} \hat{\tau}(m - s^2).$$

THEOREM 3.13.1. *If* $a > 1$, *then* $h(m) > 1$.

*Proof.* For $a > 1$, $2 \mid 2a = Q_{4k}$ and $2 \notin E(m)$.

When $a = 1$, the integer $m$ is the same as in Theorem 3.3.2, so only $m = 46$ and 622 have to be considered.

**3.14.** We now want to consider the case [Le]:

$$m := (2aF^k + a)^2 - aF^k, \quad F := 8a - 1, \ a \text{ square-free} > 1,$$

for which

$$l = 6k + 4 \quad \text{and} \quad \varepsilon = \left(\frac{8aF^k + 4a - 1 + 4\sqrt{m}}{F}\right)^{2k} \frac{(2aF^k + a + \sqrt{m})^2}{a}.$$

Here

$\hat{E}(m) := \{1, a, F^t, aF^t : 1 \leq t \leq k\}, \quad c = 2;$
$S := \{a, -a + 2aF^k\}, \quad T := \{0, 1, \cdots, 2aF^k + a - 1\} \setminus S,$
$G_t := \{a + uF^t : 1 \leq u \leq 2aF^{k-t} - 1\},$
$G'_t := \{-a + uF^t : 1 \leq u \leq 2aF^{k-t} - 1\},$
$g_t(u) := 4a^2F^{2k-t} + 4a^2F^{k-t} - aF^{k-t} - u^2F^t - 2ua,$
$g'_t(u) = g_t(u) + 4ua, \ (1 \leq t \leq k);$
$a \mid g_t(u) \Leftrightarrow a \mid u \Leftrightarrow a \mid g'_t(u);$
$n_1 = 4aF^k + 2a - 4, \quad n_2 = 4F^k - 2, \quad n_5 = 6k + 8,$
$n_3(t) = 8aF^{k-t} - 4, \quad n_4(t) = 8F^{k-t} - 4;$

$$\sum_{s=0}^{a_0} \hat{\tau}(m - s^2) = (4a+4)F^k + 2a - 2k + 2 + (8a+8)\sum_{i=0}^{k-1} F^i = c + \sum_{i=1}^{l} a_i.$$

https://doi.org/10.1017/S0027763000003822 Published online by Cambridge University Press

THEOREM 3.14.1. $h(m) > 1$.

*Proof.* If $a$ is odd, then $2 | Q_1 = 3aF^k + 2a - 1$ and $h(m) > 1$ since $2 \notin E(m)$. If $a$ is even with $a \neq 2$, then $2 | Q_{3k+2} = a$, and $2 \notin E(m)$, so $h(m) > 1$. If $a = 2$, $F = 15$ is not prime and as for Theorem 2.1 (ii) we have $h(m) > 1$.

**3.15.** Let us conclude with this family [Le]:

$$m := (2aF^k - a)^2 + aF^k, \quad F = 8a - 1, \quad a \text{ square-free} > 1,$$

for which

$$l = 6k + 2 \quad \text{and} \quad \varepsilon = \left(\frac{8aF^k + 4a + 1 + 4\sqrt{m}}{F}\right)^{2k} \frac{(2aF^k - a + \sqrt{m})^2}{a}.$$

Here we have that $c = 2$ and $\hat{E}(m)$, $S$, $G_t$, $G'_t$ are the same as in Section 3.14. This time,

$$T = \{0, 1, \cdots, 2aF^k - a\} \backslash S \text{ and}$$
$$g_t(u) := 4a^2F^{2k-t} - 4a^2F^{k-t} + aF^{k-t} - u^2F^t - 2ua, \; g'_t(u) := g_t(u) + 4ua;$$
$$n_1 = 4aF^k - 2a - 2, \quad n_2 = 4F^k - 4, \quad n_5 = 6k + 6,$$
$$n_3(t) = 8aF^{k-t} - 4, \quad n_4(t) = 8F^{k-t} - 4;$$
$$c + \sum_{i=1}^{l} a_i = c + 4(a + 1)F^k - 2a - 2k - 2 + 8(a + 1)\sum_{i=0}^{k-1} F^i$$
$$= \sum_{s=0}^{a_0} \hat{\tau}(m - s^2).$$

With the same proof as in 3.14 we have:

THEOREM 3.15.1. $h(m) > 1$.

In a forthcoming paper the families of continued fractions obtained by F. Halter-Koch [H-K] and by H. Williams will be investigated along the lines of this work.

**Acknowledgements.** It is a pleasure to thank R. A. Mollin for kindly making available his preprints, reprints and tables. The second author wishes to acknowledge the financial support of NSERC (Canada) and FCAR (Québec).

This work was initiated while the first author was at Université Laval on a sabbatical leave.

## References


[Ba] Baker, A., Linear forms in the logarithms of algebraic numbers, Mathematica, **13** (1966), 204–216.

[Be1] Bernstein, L., Fundamental units and cycles in the period of real quadratic number fields, I, Pacific J. Math., **63**, N°1, (1976), 37–61; J. Number Theory, **8** (1976), 446–491.

[Be2] ——, Fundamental units and cycles in the period of real quadratic number fields, II, Pacific J. Math., **63**, N°2, (1976), 63–78.

[H-K] Halter-Koch, F., Einige periodische Kettenbruchentwicklungen und Grundeinheiten quadratischer ordnungen, Abh. Math. Sem. Univ. Hamburg, **59** (1989), 157–169.

[He] Heegner, K., Diophantische Analysis und Modulfunktionen, Math. Z. **56** (1952), 227–253.

[Ho] Hoffstein, J., On the Siegel-Tatuzawa theorem, Acta Arith., **38** (1980), 167–174.

[Le] Levesque, C., Continued fraction expansions and fundamental units, J. Math. Phy. Sci., **22**, N°1, (1988), 11–44.

[Le-R] Levesque, C. and Rhin, G., A few classes of periodic continued fractions, Utilitas Mathematica, **30** (1986), 79–107.

[Lo1] Louboutin, S., Arithmétique des corps quadratiques réels et fractions continues, Thèse de doctorat, Univ. Paris 7, Juin 1987.

[Lo2] ——, Continued fractions and real quadratic fields, J. Number Theory, **30**, N°2, (1988), 167–176.

[Lu] Lu, H., On the class number of real quadratic fields, Scientia Sinica, **2** (1979), 118–130.

[M1] Mollin, R. A., 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., **105** (1987), 39–47.

[M2] ——, On prime valued polynomials and class numbers of real quadratic fields, Nagoya Math. J., **112** (1988).

[M3] ——, Class numbers of quadratic fields determined by solvability of diophantine equations, Math. Comp., **48**, N° 177 (1987), 233–242.

[M-W] Mollin, R. A. and Williams, H. C., Solution of the class number one problem for real quadratic fields of extended Richaud-Degert type (with one possible exception), from Number Theory, Proceedings (1990) edited by R. A. Mollin, published by W de G.

[N] Nyberg, M., Culminating and almost culminating continued fractions, Norsk. Mat. Tidsskr., **31** (1949), 95–99, (in Norwegian), MR A56–16.

[S] Stark, H. M., A complete determination of the complex quadratic fields of class number one, Michigan Math. J., **14** (1967), 1–27.

[T] Tatuzawa, T., On a theorem of Siegel, Japan J. Math., **21** (1951), 163–178.

[W] Williams, H. C., A note on the period length of the continued fraction expansion of certain $\sqrt{D}$, Utilitas Mathematica, **28** (1985), 201–209.



Eugène Dubois
*Département de Mathématiques*
*ISMRA & UNIVERSITE*
*14032 CAEN-FRANCE*

Claude Levesque
*Département de Mathématiques*
*Université LAVAL*
*QUEBEC*
*CANADA G1K 7P4*