Can. J. Math., Vol. XLII, No. 2, 1990, pp. 315–341

PRIME PRODUCING QUADRATIC POLYNOMIALS AND CLASS-NUMBERS OF REAL QUADRATIC FIELDS

STÉPHANE LOUBOUTIN

1. Introduction. Frobenius-Rabinowitsch's theorem provides us with a necessary and sufficient condition for the class-number of a complex quadratic field with negative discriminant D to be one in terms of the primality of the values taken by the quadratic polynomial

$$f_1(k) = k^2 + k + \frac{1-D}{4}$$

with discriminant D on consecutive integers (See [**1**], [**7**]). M. D. Hendy extended Frobenius-Rabinowitsch's result to a necessary and sufficient condition for the class-number of a complex quadratic field with discriminant D to be two in terms of the primality of the values taken by the quadratic polynomials

$$f_2(k) = 2k^2 - \frac{D}{8} \quad \text{or} \quad f_2(k) = 2k^2 + 2k + \frac{4-D}{8},$$

and

$$f_p(k) = pk^2 + pk + \frac{p^2 - D}{4p}$$

with discriminant D (see [**2**], [**7**]).

R. A. Mollin and H. C. Williams [**9**] proved that if we transpose Frobenius-Rabinowitsch's result to the real quadratic case, we get a characterization for the class-number of certain real quadratic fields to be one. Then, in [**10**] they conjectured some transpositions of Hendy's results to the real quadratic case: they noticed that if some quadratic polynomials with positive discriminant D take only prime values on some consecutive integers, then the class-number of the real quadratic field $\mathbf{Q}(\sqrt{D})$ equals one and the field is of Richaud-Degert type. It may be relevant to remind the reader that, whenever d is a positive square free integer, the real quadratic field $\mathbf{Q}(\sqrt{d})$ is of Richaud-Degert type if d can write: $d = m^2 + r$ with $-m < r \leqq m$ or $r = \pm 4m/3$, and with r dividing $4m$. It was proved by Louboutin [**4**] and independently by Mollin-Williams (using different techniques) in [**9**]–[**10**] that under the assumption of the extended Riemann's hypothesis there are 43 real quadratic fields of Richaud-Degert type with class-number one (See [**4**]): d = 2, 3, 5, 6, 7, 11, 13, 14, 17, 21, 23, 29, 33, 37, 38, 47, 53, 62, 69, 77, 83, 93, 101, 141, 167, 173, 197,

Received April 30, 1989.

https://doi.org/10.4153/CJM-1990-018-3 Published online by Cambridge University Press

213, 227, 237, 293, 398, 413, 437, 453, 573, 677, 717, 1077, 1133, 1253, 1293 and 1757. Moreover, in [**11**] Mollin and Williams were able to remove the extended Riemann's hypothesis assumption and proved that there exists at most one more such field. (See [**11**].) Thus, in our Theorems 2, 3, 5, 8, 5, 9 and 10 the known values are the only possible ones under the assumption of the extended Riemann's hypothesis. Moreover, without this assumption there exists at most one more value of d which satisfies one of these theorems.

We first give Theorem 2 that collects together results from [**9**] and [**10**] under a single proof and therefore simplifies the proofs. We will then prove in Theorems 2, 5, 9 and 10 that whenever one of the polynomials $f_1(k)$, $f_2(k)$ or $f_p(k)$ with positive discriminant D is prime valued on consecutive integers, then the real quadratic field with discriminant D is essentially a principal field of Richaud-Degert type. Conversely, we will strive to characterize in Theorems 2, 2′ and 5 the principal real quadratic fields of Richaud-Degert type in such terms. However, we will not be able to achieve this task in the case involving the polynomial $f_p(k)$ (see Section 4). We will give in Conjecture 2 a precise statement of what is still to be proved to get this missing characterization.

Notations. p, q are odd prime integers. Whenever $d > 1$ is a square free positive integer, D, $\mathbf{R}$, χ, $\mathcal{H}$ and $h(d)$ are the discriminant, ring of algebraic integers, character, ideal class-group and class-number of the real quadratic field $\mathbf{Q}(\sqrt{d})$. B is a Minkowski's upper bound, i.e., such that the ideal class-group is generated by the non-inert prime ideals with norm p, $p \leqq B$. It is well known that we can take $B = \frac{1}{2}\sqrt{D}$ in the real quadratic case. Whenever $\mathbf{I}$ is an ideal, we write $\mathbf{I}'$ its conjugate. A primitive integral ideal $\mathbf{I}$ with norm $N = N(\mathbf{I})$ of a quadratic field can be written as a Z-module:

$$\mathbf{I} = \mathbf{Z}N + \mathbf{Z}\,\frac{b+\sqrt{D}}{2} = \left(N, \frac{b+\sqrt{D}}{2}\right)_{\mathbf{Z}},$$

with b uniquely determined modulo $2N$. Furthermore, such a $\mathbf{Z}$-module is an ideal if and only if N divides $(b^2 - D)/4$. The real quadratic surd

$$x_0(\mathbf{I}) = \frac{b+\sqrt{D}}{2N}$$

is called the quadratic irrationality attached to the ideal $\mathbf{I}$. We then define $x_i(\mathbf{I})$ as the i-th complete quotient of the continued fractional expansion of $x_0(\mathbf{I})$, and write $x_0'(\mathbf{I})$ the conjugate in the field of this irrationality. Hence,

$$x_0(\mathbf{I}) - x_0'(\mathbf{I}) = \frac{\sqrt{D}}{N}\,.$$

The primitive ideal $\mathbf{I}$ is said to be invariant or ramified if $\mathbf{I} = \mathbf{I}'$, i.e., if $\mathbf{I}$ is a primitive ideal product of prime ramified ideals. Moreover, we will make use

https://doi.org/10.4153/CJM-1990-018-3 Published online by Cambridge University Press

of the theory of cycles of reduced ideals, as delineated in Louboutin [**5**], [**6**]. We will mainly use the fact that two integral ideals are equivalent in the ideal class group if and only if the periods of the continued fractions of their attached quadratic irrationalities are equal, a circular permutation apart.

2. Cases involving the polynomial $k^2 + k + (1 - d)/4$.

LEMMA 1. *$d \not\equiv 1$ [8], $d > 5$. $d = m^2 \pm 2$ or there exists a prime p such that $3 \leqq p \leqq \sqrt{d}$ and $\chi(p) \neq -1$.*

Proof. We can write $d = m^2 + r$ with $-m < r \leqq m$ (thus $|r| < \sqrt{d}$). If p is an odd prime dividing r, then $d \equiv m^2[p]$ and $\chi(p) \neq -1$ and we have the result. If $r = \pm 2^n$, $n \geqq 0$, by using $d \equiv 5$ [8] or $d \equiv 2, 3$ [4], one easily gets: $d = m^2 \pm 1$, $d = m^2 \pm 2$ or $d = m^2 \pm 4$. If $d = m^2 + 1$ or $m^2 + 4$, then $\chi(p) \neq -1$ and $3 \leqq p \leqq \sqrt{d}$ whenever p divides m. If $d = m^2 - 1$ or $d = m^2 - 4$, then $\chi(p) \neq -1$ and $3 \leqq p \leqq \sqrt{d}$ whenever p divides $m - 1$ or $m - 2$.

THEOREM 2. *Let $d \equiv 5$ [8], $d > 5$. The four following assertions are equivalent:*

1) *$f(k) = -k^2 - k + (d-1)/4$ is prime or equal to one for $1 \leqq k \leqq (\sqrt{d} - 1)/2$.*

2) *d is square free, $d = p^2 + 4$, $(p+2)^2 - 4$ or $4p^2 + 1$ and $\chi(q) = -1, 2 \leqq q \leqq \sqrt{d}$ and $q \neq p$.*

3) *d is square free, $d = m^2 + 4$, $m^2 - 4$ or $4m^2 + 1$ and $h(d) = 1$.*

4) *$(d/q) = -1, 2 \leqq q < \frac{1}{2}\sqrt{d-1}$ (q prime).*

Known values: $d = 13, 21, 29, 37, 53, 77, 101, 173, 197, 293, 437$ and 677.

Proof. 1) ⇒ 2)

$$f(k) = \frac{d - (2k+1)^2}{4}.$$

Since $d \equiv 5$ [8], d is not a perfect square. The $f(k)$'s,

$$1 \leqq k \leqq \frac{\sqrt{d} - 1}{2}$$

are hence odd integers.

If d is not square free, there exists q odd with $q \geqq 3$ and q^2 dividing d. Then

$$1 \leqq \frac{q-1}{2} \leqq \frac{\sqrt{d} - 1}{2}$$

and q^2 divides $f((q-1)/2)$ which consequently is not prime. Hence d is square free.

Let p be a prime such that $3 \leqq p \leqq \sqrt{d}$ and $\chi(p) \neq -1$ (Lemma 1). Let $\mathbf{P}$ be a prime ideal over (p). We have

$$\mathbf{P} = \left(p, \frac{2b + 1 + \sqrt{d}}{2}\right)_{\mathbf{Z}} \quad \text{with } 1 \leqq b \leqq p.$$

https://doi.org/10.4153/CJM-1990-018-3 Published online by Cambridge University Press

The conjugate ideal $\mathbf{P}'$ then writes

$$\mathbf{P}' = \left(p, \frac{2b'+1+\sqrt{d}}{2}\right)_{\mathbf{Z}}$$

and we can take $b' = p-1-b$ or $b' = 2p-1-b$. Hence either b or b', let us take b, satisfies

$$1 \leqq b \leqq \frac{p-1}{2} \quad \text{or} \quad b = p-1.$$

Since $\mathbf{P}$ is an ideal, p divides

$$\frac{(2b+1)^2-d}{4} = f(b).$$

α) Let us assume $2 \leqq b \leqq (p-3)/2$. Then $f(b)$ is prime and

$$p = f(b) \geqq f\left(\frac{p-3}{2}\right) = \frac{d-(p-2)^2}{4}.$$

Hence $p^2 \leqq d \leqq p^2+4$. Since $d \equiv 5$ [8], we have $d = p^2+4$.

β) Let us assume $b = (p-1)/2$. Then

$$p = f(b) = \frac{d-p^2}{4} \quad \text{and} \quad d = p(p+4) = (p+2)^2-4.$$

γ) Let us assume $b = p-1$ and

$$p \leqq \frac{\sqrt{d}-1}{2}.$$

Then

$$p = f(p-1) = \frac{d-(2p+1)^2}{4} \quad \text{and} \quad d = 4p^2+1.$$

δ) Let us assume

$$b = p-1 \quad \text{and} \quad p > \frac{1+\sqrt{d}}{2}.$$

Then p divides $f(p-1)$ and hence $d = 4pn+1$. But then

$$n < \frac{\sqrt{d}-1}{2},$$

https://doi.org/10.4153/CJM-1990-018-3 Published online by Cambridge University Press

hence $p+1-n>2$ and $f(n)=n(p+1-n)$ is not prime. This case cannot occur.

Since d uniquely writes $d=m^2+r$ with $-m<r\leqq m$, whenever $d=m^2+4$, m^2-4 or $4m^2+1$, $d\neq 5$, d writes in only one of these three forms. Hence $\chi(q)=-1$, $3\leqq q\leqq\sqrt{d}$ and $q\neq p$.

2) ⇒ 3) If $d=p^2+4$, $p(p+4)$ or $4p^2+1$ then

$$\frac{p+2+\sqrt{d}}{2},\quad \frac{p+\sqrt{d}}{2}\quad\text{and}\quad\frac{2p+1+\sqrt{d}}{2}$$

have norm $\pm p$. Thus the prime ideals over (p) are principal. Since $\sqrt{D}=\sqrt{d}$ is a Minkowski's upper bound and since $\chi(2)=-1$, we have $h(d)=1$.

3) ⇒ 4) follows from Louboutin [**5**], Theorem 3.

4) ⇒ 1) Whenever

$$2\leqq k\leqq\frac{1+\sqrt{d}}{2}$$

we have

$$1\leqq f(k)<\frac{d-1}{4}.$$

If $f(k)$ is neither prime nor equal to one, there exists a prime p dividing $f(k)$ such that

$$3\leqq p<\frac{\sqrt{d-1}}{2}.$$

Since $f(k)\equiv(2k-1)^2$ $[p]$, we get $\chi(p)\neq -1$.

We will later on show in Theorem 4 that the right bounds for k, i.e., those suggested by the fact that $\frac{1}{2}\sqrt{d}$ is a Minkowski's upper bound, are

$$0\leqq k\leqq\tfrac{1}{4}\sqrt{d}-\tfrac{1}{2}.$$

Whenever $d=4m^2+1$, $f(0)=m^2$ is not prime. Nevertheless we have:

THEOREM 2′. *Let $d\equiv 5$ [8], $d>5$. The four following assertions are equivalent:*

1) *$f(k)=-k^2-k+(d-1)/4$ is prime or equal to one for $0\leqq k\leqq\frac{1}{4}\sqrt{d}-\frac{1}{2}$.*

2) *d is square free, $d=p^2+4$ or $d=(p+2)^2-4$ with p prime and $\chi(q)=-1$, $2\leqq q\leqq\frac{1}{2}\sqrt{d}$.*

3) *d is square free, $d=m^2\pm 4$ and $h(d)=1$.*

4) *$(d/q)=-1$, $2\leqq q<\frac{1}{2}\sqrt{d}$ (q prime).*

Proof. Since there exists a prime q such that

$$\tfrac{1}{2}\sqrt{d-1}\leqq q\leqq\tfrac{1}{2}\sqrt{d}$$

https://doi.org/10.4153/CJM-1990-018-3 Published online by Cambridge University Press

if and only if $d = 4q^2 + 1$, and since $\frac{1}{2}\sqrt{d}$ is a Minkowski's upper bound, here again we have 2) $\Rightarrow$ 3) $\Rightarrow$ 4) $\Rightarrow$ 1).

1) $\Rightarrow$ 2) remains to be proved. If q^2 divides d, since $d \equiv 5$ [8] is not a perfect square, we have

$$5q^2 \leqq d \quad \text{and} \quad 2 \leqq \frac{q+1}{2} \leqq \tfrac{1}{4}\sqrt{d} + \tfrac{1}{2},$$

and q^2 divides $f((q+1)/2)$ which consequently is not prime. Hence d is square free.

Let us suppose that there exists a prime p such that

$$3 \leqq p \leqq \tfrac{1}{2}\sqrt{d} \quad \text{and} \quad \chi(p) \neq -1.$$

Now we can take b such that

$$0 \leqq b \leqq \frac{p-1}{2}$$

(since we can take $0 \leqq b \leqq p-1$). Hence, we are in case α) or β) in the proof of Theorem 2), 1) $\Rightarrow$ 2), and $d = p^2 + 4$ or $p(p+4)$. In these two cases we have $p > \frac{1}{2}\sqrt{d}$, hence $\chi(q) = -1, 3 \leqq q \leqq \frac{1}{2}\sqrt{d}$. According to the previous theorem, we have $d = p^2 + 4$ or $d = p(p+4)$ (since $\chi(p) = +1$ whenever $d = 4p^2 + 1$).

After having given as small of a bound as possible such that whenever the $f(k)$'s are prime or equal to one whenever k is nonnegative and less than this bound then the field is principal and of Richaud-Degert type, we now show that, inversely, whenever the field is one of those principal fields considered above we can give the optimal upper bound k_0 such that $f(k)$ is prime or equal to one whenever $0 \leqq k < k_0$, and such that $f(k_0)$ is neither prime nor equal to one.

THEOREM 3. *Let $d > 5$, $d \equiv 5$ [8] be square free and*

$$f_1(k) = k^2 + k + \frac{1-d}{4}.$$

1) *If $d = m^2 + 4$ then $h(d) = 1$ if and only if $|f_1(k)|$ is prime or equal to one whenever*

$$0 \leqq k \leqq \frac{3m-5}{2}.$$

Note that

$$f_1\left(\frac{3m-3}{2}\right) = m(2m-3)$$

is not prime. Known values: $d =$ 13, 29, 53, 173 and 293.

https://doi.org/10.4153/CJM-1990-018-3 Published online by Cambridge University Press

2) *If* $d = m^2 - 4$ *then* $h(d) = 1$ *if and only if* $|f_1(k)|$ *is prime or equal to one whenever*

$$0 \leqq k \leqq \frac{3m-9}{2}.$$

Note that

$$f_1\left(\frac{3m-7}{2}\right) = (m-2)(2m-5)$$

is not prime. Known values: $d = 21, 77$ *and* 437.

3) *If* $d = 4m^2 + 1$ *then* $h(d) = 1$ *if and only if* $|f_1(k)|$ *is prime or equal to one whenever* $1 \leqq k \leqq 2m - 2$. *Note that*

$$f_1(2m-1) = m(3m-2)$$

is not prime. Known values: $d = 37, 101, 197$ *and* 677.

Proof. According to previous theorems these conditions of primality are sufficient to state $h(d) = 1$. Conversely, let us suppose that $h(d) = 1$ and prove that the $|f_1(k)|$'s are prime or equal to one.

Case 3. Whenever $1 \leqq k \leqq 2m - 2$ we have $|f_1(k)| < d$. If one of the $|f_1(k)|$'s is neither prime nor equal to one, there exists a prime p dividing $|f_1(k)|$ such that $3 \leqq p \leqq \sqrt{d}$ and $\chi(p) \neq -1$. Thus, $p = m$ (Theorem 2). Since m divides $f_1(k) = k^2 + k + m^2$ if and only if $k \equiv m - 1, m$ $[m]$ and since $|f_1(m-1)| = |f_1(m)| = m$ is prime, we obtain what we wanted.

Cases 1), 2). These are more tricky to prove, since now $|f_1(k)|$ can be greater than d. For example, let us prove the first case. We first notice that, according to Theorem 2, m is prime and $\chi(p) \neq -1$, $3 \leqq p \leqq \sqrt{d}$, $p \neq m$. Let p be a prime such that $p < 2m - 3$ and $\chi(p) \neq -1$. For one of the prime ideals $\mathbf{P}$ above (p) we have:

$$\mathbf{P} = \left(p, \frac{2k+1+\sqrt{d}}{2}\right)_{\mathbf{Z}}$$

with

$$0 \leqq k \leqq \frac{p-1}{2} < m - 2 \quad \text{and } p/|f_1(k)|.$$

Thus $|f_1(k)| < d$. Since $\chi(q) \neq -1$ whenever q divides any $|f_1(k)|$, if $|f_1(k)|$ is not prime then m divides $|f_1(k)|$ and

$$k \equiv \frac{m-3}{2}, \frac{m+1}{2} \,[m].$$

https://doi.org/10.4153/CJM-1990-018-3 Published online by Cambridge University Press

Since

$$\left|f_1\left(\frac{m-3}{2}\right)\right| = \left|f_1\left(\frac{m+1}{2}\right)\right| = m$$

is prime, $|f_1(k)|$ is prime and thus $p = |f_1(k)|$, whenever $p < 2m-3$. One easily gets the successive minima of $|f_1(k)|$, $k \geqq 0$, as 1, m, $2m-3$

$$\left(\text{whenever } k = m,\ \frac{m-3}{2} \quad \text{or} \quad \frac{m+1}{2},\ \frac{m-5}{2}\right).$$

Hence $\chi(p) = -1$, $3 \leqq p < 2m-3$ and $p \neq m$. Let

$$k_0 = \frac{3m-3}{2},$$

we have $|f_1(k_0)| = m(2m-3)$ which is not prime and $|f_1(k)| < m(2m-3)$ whenever $0 \leqq k \leqq k_0 - 1$. If p divides $|f_1(k)|$ then $\chi(p) \neq -1$ and thus $p = m$. Hence, if any $|f_1(k)|$ is not prime, then m divides it. We have just seen that in this case

$$k = \frac{m-3}{2} \quad \text{or} \quad \frac{m+1}{2}$$

and $|f_1(k)| = m$ is prime.

3. Cases involving the polynomials $2k^2 - (d/2)$ and $2k^2 + 2k + (1-d)/2$. Let δ be a square free positive integer dividing D, the discriminant of our real quadratic field. There exists only one ramified ideal (i.e., an ideal which is a product of prime ramified ideals) with norm δ, we will write it $\mathbf{I}_\delta$ and call it the ideal over δ. We have:

$$\mathbf{I}_\delta = \left(\delta,\ \frac{\epsilon\delta + \sqrt{D}}{2}\right)_{\mathbf{Z}}$$

with $\epsilon = 0$ whenever $d \equiv 2$ [4] or $d \equiv 3$ [4] and δ odd, and $\epsilon = 1$ otherwise. The polynomial

$$f_\delta(X) = \delta X^2 + \epsilon\delta X + \frac{\epsilon\delta - (D/\delta)}{4} = \frac{\delta^2(2X+\epsilon)^2 - D}{4\delta}$$

is a quadratic polynomial with integral coefficients and discriminant D. It is odd valued only on $\mathbf{Z}$ only in the three following cases:

$$d = D \equiv 5\ [8] \text{ and } \delta \text{ odd:} \quad f_\delta(X) = \delta X^2 + \delta X + \frac{\delta - (d/\delta)}{4} \quad (\epsilon = 1)$$

$$d \equiv 3\ [4] \text{ and } \delta \text{ even:} \quad f_\delta(X) = \delta X^2 + \delta X + \frac{\delta - (D/\delta)}{4} \quad (\epsilon = 1)$$

$$d \equiv 2\ [4] \text{ and } \delta \text{ even:} \quad f_\delta(X) = \delta X^2 - \frac{d}{\delta} \quad (\epsilon = 0).$$

https://doi.org/10.4153/CJM-1990-018-3 Published online by Cambridge University Press

THEOREM 4. *If the* $|f_\delta(k)|$*'s* $0 \leqq k \leqq (B-1)/2$ *are prime or equal to* 1 *and if* $\mathbf{I}$ *is a primitive ideal with norm* N *such that* $1 < N \leqq B$ *and* G.C.D.$(N, \delta) = 1$, *then* N *is prime and*

$$N \in \left\{ |f_\delta(k)|;\ 0 \leqq k \leqq \frac{B-1}{2} \right\}$$

and $\mathbf{I}$ *is equivalent in the ideal class-group to the ramified ideal* $\mathbf{I}_\delta$.

Moreover, if B *is a Minkowski's upper bound, the ideal class group of the quadratic field is generated by the prime ramified ideals with norm dividing* δ.

Proof. $\mathbf{II}_\delta$ is primitive and writes:

$$\mathbf{II}_\delta = \left(N\delta,\ \frac{n + \sqrt{D}}{2} \right)_{\mathbf{Z}}.$$

Since $\mathbf{II}_\delta$ is included in $\mathbf{I}_\delta$,

$$\frac{n+\sqrt{D}}{2} \in \mathbf{I}_\delta.$$

Thus we can write

$$n = 2k\delta + \epsilon\delta \quad \text{and} \quad \mathbf{II}_\delta = \left(N\delta,\ \frac{(2k+\epsilon)\delta + \sqrt{D}}{2} \right)_{\mathbf{Z}}.$$

$\mathbf{II}_\delta$ being an ideal with norm $N\delta$, $N\delta$ divides

$$\frac{((2k+\epsilon)\delta)^2 - D}{4}$$

and N divides $f_\delta(k)$.

$$\mathbf{I}'\mathbf{I}_\delta = \mathbf{I}'\mathbf{I}'_\delta = \left(N\delta,\ \frac{(2k'+\epsilon)\delta + \sqrt{D}}{2} \right)_{\mathbf{Z}} \quad \text{with } k' = -k - \epsilon.$$

Since k and k' are only determined modulo N, we can suppose that $0 \leqq k \leqq N-1$ holds and we can take $k' = N - \epsilon - k$. Hence, for either k or k' (let us take k)

$$0 \leqq k \leqq \frac{N-1}{2}$$

holds. If $1 < N \leqq B$, then N divides $f_\delta(k)$ which is prime, hence $N = |f_\delta(k)|$. Thus, the principal ideal

$$\left(\frac{(2k+\epsilon)\delta + \sqrt{D}}{2} \right)$$

is included in $\mathbf{II}_\delta$ and with norm $N\delta$, as $\mathbf{II}_\delta$. Hence, $\mathbf{II}_\delta$ is principal and $\mathbf{I}$ is equivalent in the class-group to $\mathbf{I}'_\delta = \mathbf{I}_\delta$.

Remark. Let us suppose $d = D \equiv 5$ [8] and let $\mathbf{I}$ be a primitive ideal with norm N such that $N \leqq B+2$ and G.C.D.$(N, D) = 1$. Then, under the hypothesis of Theorem 4, we have

$$N \in \left\{ |f_\delta(k)|;\ 0 \leqq k \leqq \frac{B-1}{2} \right\}.$$

In fact, in the proof of Theorem 4, we can suppose that for either k or k' (let us take k)

$$0 \leqq k \leqq \frac{N-3}{2}$$

holds. Otherwise,

$$k = \frac{N-1}{2} \quad \text{and } N \text{ divides} \quad \frac{(\delta N)^2 - D}{4},$$

hence divides D. We will need this improvement in Theorem 10.

Theorem 5 below is a proof of conjecture 3.1 of [**12**].

THEOREM 5. *Let $d \equiv 2, 3$ [4], $d > 0$. The three following assertions are equivalent:*

1) *$|f_2(k)|$ is prime or equals one for*

$$0 \leqq k \leqq \frac{\sqrt{d}-1}{2}.$$

2) *d is square free, $d = m^2 \pm 2$ and $\chi(q) = -1$, $3 \leqq q \leqq \sqrt{d}$, or $d = p^2 + 1$ or $p(p+2)$ and $\chi(q) = -1$, $3 \leqq q \leqq \sqrt{d}$ and $q \neq p$.*

3) *d is square free with $d = m^2 \pm 2$ and $h(d) = 1$, or d is square free with $d = m^2 \pm 1$ and $h(d) = 2$.*

Known values: $h(d) = 1$ and $d = m^2 \pm 2 = 2$, 3, 6, 7, 11, 14, 23, 38, 47, 62, 83, 167, 227 and 398. $h(d) = 2$ and $d = m^2 \pm 1 = 10$, 15, 26, 35, 122, 143 and 362.

Proof. This is similar to that of Theorem 2.

1) $\Rightarrow$ 2) Let p be a prime such that $3 \leqq p \leqq \sqrt{d}$ and $\chi(p) \neq -1$. If there does not exist such a prime, then $d = n^2 \pm 2$ and $\chi(p) \neq -1$, $3 \leqq p \leqq \sqrt{d}$ (Lemma 1). Otherwise, there exists a prime ideal $\mathbf{P}$ over (p) such that

$$\mathbf{I}_2\mathbf{P} = \left(2p, \frac{2k+\epsilon+\sqrt{d}}{2}\right)_{\mathbf{Z}} \quad \text{with } 0 \leqq k \leqq \frac{p-1}{2}.$$

https://doi.org/10.4153/CJM-1990-018-3 Published online by Cambridge University Press

Since p divides $|f_2(k)|, p = |f_2(k)|$. Moreover, we have $0 \leqq 2k+\epsilon \leqq 2k+1 \leqq \sqrt{d}$, hence $|f_2(k)| = -f_2(k)$.

α) Let us assume

$$0 \leqq k \leqq \frac{p-3}{2}.$$

Then

$$p = -f_2(k) \geqq \frac{d-(p-2)^2}{2}.$$

Hence $p^2 \leqq d \leqq p^2 - 2p + 4$. This case cannot occur.

β) Let us assume

$$k = \frac{p-1}{2}.$$

Then

$$p = -f_2(k) = \frac{d-(p-1+\epsilon)^2}{2},$$

hence $d = p(p+2)$ whenever $\epsilon = 0$, and $d = p^2 + 1$ whenever $\epsilon = 1$. Moreover, as in Theorem 2, we have $\chi(q) = -1$, $3 \leqq q \leqq \sqrt{d}$ and $q \neq p$.

2) $\Rightarrow$ 1) Whenever

$$0 \leqq k \leqq \frac{\sqrt{d}-1}{2},$$

we have

$$|f_2(k)| \leqq \frac{d}{2} < d.$$

If q is a prime dividing $|f_2(k)|$, then $\chi(q) \neq -1$. Hence $|f_2(k)|$ is prime or equal to one whenever $d = m^2 \pm 2$. If $d = p(p+2)$ or $d = p^2 + 1$, p divides $|f_2(k)|$,

$$0 \leqq k \leqq \frac{p-1}{2}$$

if and only if

$$k = \frac{p-1}{2}.$$

In both cases

$$\left| f_2\left(\frac{p-1}{2}\right) \right| = p$$

is prime. Hence, $|f_2(k)|$ is prime or equal to one whenever

$$0 \leqq k \leqq \frac{\sqrt{d}-1}{2}.$$

2) $\Rightarrow$ 3) In the case of $d = m^2 \pm 2$, the algebraic integer $m+\sqrt{d}$ is with norm ± 2. The prime ramified ideal $\mathbf{I}_2$ over (2) is thus principal, and $h(d) = 1$. In the cases of $d = p(p+2)$ or $d = p^2+1$, since $\chi(q) = -1$, $3 \leqq q \leqq \sqrt{d}$ and $q \neq p$, the ideal class-group is generated by any prime ideal $\mathbf{P}$ above (p). Moreover, the algebraic integers $p+1+\sqrt{d}$ or $p+\sqrt{d}$ being with norms $\pm 2p$, $\mathbf{P}$ is equivalent to $\mathbf{I}_2$ and $h(d) \leqq 2$. Whenever $d = p^2+1$, the fundamental unit $\epsilon_0 = p+\sqrt{d}$ is with norm -1. By genus theory, we have $h(d) \geqq 2$ and $h(d) = 2$.

3) $\Rightarrow$ 2) Whenever $d = m^2 \pm 2$, this follows from [**5**], Theorem 3. Whenever $d = m^2 \pm 1$, with the notations of Louboutin [**6**] and by calculating the continued fractions expansion of $\omega_0 = \sqrt{d}$ and $x_0(\mathbf{I}_2)$, one can easily get $E(D) = \{1, 2, m\}$ whenever $d = m^2+1$, and $E(D) = \{1, 2, m-2, 2(m-2)\}$ whenever $d = m^2-1$. Hence, by [**6**], Theorem 3 we get the result.

PROPOSITION 6. *Let* $\mathbf{I}$ *be a primitive integral ideal:* $x_2(\mathbf{I})$ *is reduced if and only if* $-x_1'(\mathbf{I}) > 0$. *Moreover, if* $\mathbf{I}$ *is a primitive integral ideal with norm* N *less than* $\sqrt{D}$, *then* $x_2(\mathbf{I})$ *is reduced.*

Proof. See Williams-Wunderlich "On the parallel generation of the residues for the continued fraction factoring algorithm"; Math. of Comp. *177* (1987), 405–423.

Remarks. If $\mathbf{I}$ is a primitive integral ideal, $x_1(\mathbf{I})$ is reduced if and only if $x_0(\mathbf{I})$ can be taken reduced.

Even though this bound $\sqrt{D}$ cannot help us to give a different proof of Theorem 3, it will yet be used to prove Theorem 8 below.

COROLLARY 7. *Let* $d = m^2+1 \equiv 2$ [4] *be a square free integer,* $\mathbf{P}$ *a non inert prime ideal with norm* p *such that* $p \leqq \sqrt{D}$. *Then,* $\mathbf{P}$ *is not principal and* $\mathbf{P}$ *is equivalent in the ideal class-group to the prime ideal* $\mathbf{I}_2$ *over* (2) *if and only if* $p = 2$ *or* $p = m$.

THEOREM 8. *Let* $d \equiv 2, 3$ [4], $d > 2$ *be a square free integer. Let us consider the two polynomials*

$$f_2(k) = 2k^2 - \frac{d}{2}$$

whenever

$$d \equiv 2\,[4], \quad \textit{and} \quad f_2(k) = 2k^2 + 2k + \frac{1-d}{2}$$

https://doi.org/10.4153/CJM-1990-018-3 Published online by Cambridge University Press

whenever $d \equiv 3$ [4]. *We have:*

d	$h(d)$	*upper bound*	*known values*
$m^2 - 2 \equiv 2\,[4]$	1	$\dfrac{3m-6}{2}$	14, 62 *and* 398
$m^2 + 2 \equiv 2\,[4]$	1	$\dfrac{3m-2}{2}$	3, 6 *and* 38
$m^2 - 2 \equiv 3\,[4]$	1	$\dfrac{3m-7}{2}$	7, 23, 47 *and* 167
$m^2 + 2 \equiv 3\,[4]$	1	$\dfrac{3m-3}{2}$	11, 83 *and* 227
$m^2 + 1 \equiv 2\,[4]$	2	$\dfrac{3m-3}{2}$	10, 26, 122 *and* 362
$m^2 - 1 \equiv 3\,[4]$	2	$\dfrac{3m-6}{2}$	15, 35 *and* 143

For instance, the fifth line of this chart reads: whenever $d = m^2 + 1 \equiv 2$ [4] *is a square free integer,* $h(d) = 2$ *if and only if* $|f_2(k)|$ *is prime or equal to one whenever*

$$0 \leqq k \leqq \frac{3m-3}{2}.$$

The only known such values are: $d =$ 10, 26, 122 *and* 362. *Moreover, as in Theorem* 3, *these upper bounds are optimal.*

Proof. According to Theorem 5, these conditions of primality are sufficient to state the results on $h(d)$. Conversely, let us for example prove the fifth case. Let $d = m^2 + 1 \equiv 2$ [4] with $h(d) = 2$ and let

$$k_0 = \frac{3m-1}{2}.$$

We have $|f_2(k_0)| = m(4m-3) < D$. If $|f_2(k)|$, $0 \leqq k \leqq k_0 - 1$ is neither prime nor equal to one, there exists a prime p dividing $|f_2(k)|$ such that $p < \sqrt{D}$. Since $\chi(p) \neq -1$, by the previous corollary, $p = m$. m prime divides $|f_2(k)|$ if and only if

$$k \equiv \frac{m-1}{2} \quad \text{or} \quad \frac{m+1}{2}\ [m].$$

$$\left| f_2\left(\frac{m-1}{2}\right) \right| = \left| f_2\left(\frac{m+1}{2}\right) \right| = m$$

being prime, we have

$$k \geqq \frac{3m-1}{2}$$

when $|f_2(k)|$ is neither prime nor equal to one.

4. Cases involving the polynomial $pk^2 + pk + (p-q)/4$**.** Let $\mathbf{Q}(\sqrt{d})$, $d = m^2 + r > 0$ square free, be a real quadratic field of Richaud-Degert type with class-number one.

In the case of $d \equiv 1$ [8], since the ideal (2) splits completely, Louboutin [**5**], Proposition 2 gives us 2 as a Q_i/Q_0's and we readily get $d = 17$ or 33 by calculating the continued fractional expansion of

$$\omega_0 = \frac{1+\sqrt{d}}{2}$$

according to the parity of m and the sign of r (See [**4**].)

In the case of $d \equiv 2$, 3 [4], we similarly get $d = m^2 \pm 2$ (the ideal (2) being ramified, 2 is also a Q_i/Q_0's).

In the case of $d \equiv 5$ [8], if the fundamental unit is with norm -1, then $d = m^2 + 4$ or $d = 4m^2 + 1$.

In these three cases, the previous theorems give us a characterization of the principality of the field in terms of the primality of the values taken by some quadratic polynomials.

In the case of $d \equiv 5$ [8], if the fundamental unit is with norm $+1$, then $d = pq$ with $p < q$ odd prime integers such that $p \equiv q \equiv 3$ [4] (by genus theory). Moreover, since the field is of Richaud-Degert type, we have $d = p^2s^2 \pm 4p$ or $d = 4p^2s^2 \pm p$, i.e., $q = ps^2 \pm 4$ or $q = 4ps^2 \pm 1$. If $d = p^2 \pm 4p$ (i.e., $s = 1$), then $d = m^2 - 4$ with $m = p + 2$ or $p - 2$ and Theorem 2 gives us such a characterization.

By searching on a pocket programmable calculator the d's with $d = pq \equiv 5$ [8], $p \equiv q \equiv 3$ [4], and such that the $|f_p(k)|$'s are prime or equal to one whenever

$$0 \leqq k \leqq \tfrac{1}{4}\sqrt{d} - \tfrac{1}{2},$$

we get the three values $d = 21$, 77 and 437 that can write $d = m^2 - 4$, as well as the fourteen values of the following chart (when k_0 is such that the $|f_p(k)|$'s are prime or equal to one whenever $0 \leqq k \leqq k_0 - 1$, and $|f_p(k_0)|$ is neither prime, nor equal to one; i.e., $k_0 - 1$ is the optimal upper bound of our set of consecutive integers). We can notice that these 17 fields are the known principal fields of Richaud-Degert type with $d = pq$.

$d = p^2s^2 + 4\epsilon p$	p	s	ϵ	k_0	$d = 4p^2s^2 + \epsilon p$	p	s	ϵ	k_0
69	3	3	-1	4	141	3	2	-1	3
93	3	3	$+1$	6	573	3	4	-1	7
213	3	5	-1	9	1293	3	6	-1	11
237	3	5	$+1$	11	1757	7	3	-1	16
413	7	3	-1	12					
453	3	7	$+1$	16					
717	3	9	-1	19					
1077	3	11	-1	24					
1133	11	3	$+1$	22					
1253	7	5	$+1$	27					

One can check that

$$k_0 = \operatorname{Inf}\left\{x; x = \left|\frac{p(2k-1)^2 - q}{4}\right| - k, \quad x \geqq 0,\ k \geqq 0\right\}.$$

k_0 defined in such terms is equal to

$$\frac{(2p-1)(s-1)}{2} + \epsilon$$

whenever $d = p^2s^2 + 4\epsilon p$ (with $\epsilon = \pm 1$) and is equal to

$$(p-1)s - \frac{p-\epsilon}{4}$$

whenever $d = 4p^2s^2 + \epsilon p$ (even though it seems that there exists no such field with $d = 4p^2s^2 + p$).

We are thus entitled to emphasize the two following conjectures, the first one being introduced by Mollin-Williams [**10**].

CONJECTURE 1. *Let $d = pq \equiv 5$ [8] and $p \equiv q \equiv 3$ [4]. The two following assertions are equivalent:*

1) $|f_p(k)| = |pk^2 + pk + (p-q)/4|$ *is prime or equal to one whenever* $0 \leqq k \leqq \frac{1}{4}\sqrt{d} - \frac{1}{2}$.

2) $d = p^2s^2 \pm 4p$ *or* $d = 4p^2s^2 \pm p$ *and* $h(d) = 1$.

CONJECTURE 2. *$d = pq \equiv 5$ [8], $p < q$. Let us consider the polynomial*

$$f_p(k) = pk^2 + pk + \frac{p-q}{4}.$$

We have, with $s > 1$ in the last two lines:

d	$h(d)$	*upper bound*	*known values*
$4p^2s^2+p$	1	$(p-1)s-\frac{p+3}{4}$	*none*
$4p^2s^2-p$	1	$(p-1)s-\frac{p+5}{4}$	141, 573, 1293 *and* 1757
p^2s^2+4p	1	$\frac{(2p-1)(s-1)}{2}$	93, 237, 453, 1133 *and* 1253
p^2s^2-4p	1	$\frac{(2p-1)(s-1)}{2}-2$	69, 213, 413, 717 *and* 1077

This chart reads like that of Theorem 8.

Remark. These upper bounds would be optimal since we have the two non-trivial factorizations:

$$f_p(k_0) = \left(k_0 + \frac{s-1}{2}\right)\left(p\left(k_0 - \frac{s-3}{2}\right) - 1\right)$$

$$\text{whenever } d = p^2s^2 + 4\epsilon p.$$

$$f_p(k_0) = (k_0 + s)(p(k_0 - s + 1) - 1) \quad \text{whenever } d = 4p^2s^2 + \epsilon p.$$

Theorem 9 below is our first step in the study of these conjectures. Together with Theorem 10, it shows the effect of the choice of the upper bound (of our set of consecutive integers on which $f_p(X)$ is prime valued) on the wideness of the family of fields characterized in such terms.

THEOREM 9. *$d = pq \equiv 5$ [8], $p < q$. If*

$$|f_p(k)| = \left|pk^2 + pk + \frac{p-q}{4}\right|$$

is prime or equal to one whenever $0 \leqq k \leqq \frac{1}{2}\sqrt{d} - \frac{1}{2}$, then $h(d) = 1$ and $d = p^2s^2 \pm 4p$. Hence $p \equiv q \equiv 3$ [4]. The only known such values are: $d = 21$, 69, 77, 93, 213, 237, 413, 437, 453, 717, 1077, 1133 and 1253.

This result is our first step towards Mollin-Williams' conjecture following their Theorem 6 in [**8**].

Proof. We first show a better statement: let $d \equiv 5$ [8] and δ dividing d with $1 < \delta < d$. If $|f_\delta(k)|$ is prime or equal to one whenever $0 \leqq k \leqq \frac{1}{2}\sqrt{d} - \frac{1}{2}$, then $d = \delta^2s^2 \pm 4\delta$.

Let

$$y = \frac{1}{\delta}\sqrt{d}.$$

If there exists k such that

$$0 \leqq k \leqq \tfrac{1}{2}\sqrt{d} - \tfrac{1}{2}$$

and such that

$$|f_\delta(k)| \leqq \tfrac{1}{4}\sqrt{d},$$

then

$$(2k+1)^2 \leqq y^2 + y \leqq \left(y + \tfrac{1}{2}\right)^2.$$

Thus,

$$k \leqq \tfrac{1}{2}y - \tfrac{1}{2} \leqq \tfrac{1}{6}\sqrt{d} - \tfrac{1}{2}.$$

Let $s = |f_\delta(k)|$. If $s \neq 1$, s is prime and

$$f_\delta(k+s) = f_\delta(k) + s \cdot f_\delta'(k) + \frac{s^2}{2} f_\delta''(k),$$

i.e.,

$$f_\delta(k+s) = \pm s + \delta s(s + 2k + 1) \quad (*).$$

Since

$$0 \leqq k + s \leqq \tfrac{1}{4}\sqrt{d} - \tfrac{1}{2} + \tfrac{1}{4}\sqrt{d} \leqq \tfrac{1}{2}\sqrt{d} - \tfrac{1}{2}$$

and since s divides $f_\delta(k+s)$ because of (*), we have $|f_\delta(k+s)| = s$. But it is in contradiction with (*). Hence,

$$|f_\delta(k)| = 1 \quad \text{and} \quad d = \delta^2(2k+1)^2 \pm 4\delta.$$

Let us now suppose that

$$|f_\delta(k)| > \tfrac{1}{4}\sqrt{d},$$

whenever

$$0 \leqq k \leqq \tfrac{1}{2}\sqrt{d} - \tfrac{1}{2}.$$

Since $|f_\delta(k)| \leqq \frac{1}{2}\sqrt{d}$ if and only if $y^2 - 2y \leqq (2k+1)^2 \leqq y^2 + 2y$, there exists k such that

$$0 \leqq k \leqq \tfrac{1}{2}y \leqq \tfrac{1}{4}\sqrt{d}$$

https://doi.org/10.4153/CJM-1990-018-3 Published online by Cambridge University Press

and such that

$$\tfrac{1}{4}\sqrt{d} < |f_\delta(k)| \leqq \tfrac{1}{2}\sqrt{d}.$$

In fact, whenever $y \leqq 1+\sqrt{2}$ we can take $k = 0$, and whenever $y > 1+\sqrt{2}$, we can take k such that $0 < x_1 \leqq k \leqq x_2$, when

$$x_1 = \frac{\sqrt{y^2-2y}-1}{2} \quad \text{and} \quad x_2 = \frac{\sqrt{y^2+2y}-1}{2},$$

since $x_2 - x_1 > 1$. Since

$$x_2 \leqq \tfrac{1}{2}y \leqq \tfrac{1}{4}\sqrt{d},$$

we have

$$0 \leqq k \leqq \tfrac{1}{4}\sqrt{d}.$$

Now,

$$k \leqq \tfrac{1}{4}\sqrt{d} < s \leqq \tfrac{1}{2}\sqrt{d},$$

with $s = |f_\delta(k)|$ a prime integer. Hence $k' = s - k - 1$ is such that

$$0 \leqq k' \leqq \tfrac{1}{2}\sqrt{d} - \tfrac{1}{2}$$

and thus, $|f_\delta(k')|$ is prime or equal to one. Since

$$f_\delta(k') = f_\delta(s-k-1) = f_\delta(k-s) = f_\delta(k) - s \cdot f_\delta'(k) + \frac{s^2}{2} f_\delta''(k),$$

we have

$$f_\delta(k') = \pm s + \delta s(s-(2k+1)) \quad (^{**}).$$

Hence s divides $|f_\delta(k')|$ and $s = |f_\delta(k')|$. Now (**) implies $s = 2k+1$. Thus

$$4s = \left|\delta s^2 - \frac{d}{\delta}\right| \quad \text{and} \quad d = \delta^2 s^2 + 4\epsilon s\delta \quad \text{with } \epsilon = \pm 1.$$

Now,

$$\left| f_\delta\left(\frac{3s-1}{2}\right)\right| = s(2\delta s - \epsilon)$$

is not prime, while

$$\frac{3s-1}{2} \leqq \tfrac{1}{2}\sqrt{d}-\tfrac{1}{2}$$

if $\epsilon = +1$, or if $\epsilon = -1$ and $\delta > 3$. Whenever $\epsilon = -1$ and $\delta = 3$, we have

$$\frac{3s-5}{2} \leqq \tfrac{1}{2}\sqrt{d}-\tfrac{1}{2}$$

and

$$\left|f_3\left(\frac{3s-5}{2}\right)\right| = 6s^2-17s+12 = (2s-3)(3s-4)$$

is not prime, this case cannot occur.

Whenever $\delta = p$, we thus get $d = p^2s^2 \pm 4p$. Since $(ps+\sqrt{d})/2$ is with norm $\pm p$, the ramified ideal $\mathbf{I}_p$ above (p) is principal. By Theorem 4, $h(d) = 1$. Hence $p \equiv q \equiv 3$ [4].

We now want to settle such a result with an upper bound lower than $\frac{1}{2}\sqrt{d}-\frac{1}{2}$ in order to get the 17 known real quadratic fields of Richaud-Degert type with $d = pq$ and $h(d) = 1$. On the other hand, we do not want this upper bound to be too small thus running the risk of obtaining more than those fields. Hence, we take this upper bound as great as Conjecture 2 enables us to choose it.

Whenever $d = 4p^2s^2 - p$ with $p = 3$, the greatest integer less than or equal to $\frac{1}{3}\sqrt{d}-\frac{1}{2}$ is equal to $2s-1$, while $|f_p(2s-1)|$ is neither prime nor equal to one (remark following Conjecture 2). So, $|f_p(k)|$ is prime or equal to one whenever $0 \leqq k \leqq \frac{1}{3}\sqrt{d}-\frac{1}{2}$ cannot hold. However, the greatest integer less than or equal to $\frac{1}{3}\sqrt{d}-1$ is equal to $2s-2$. That is why we will take $\frac{1}{3}\sqrt{d}-1$ as upper bound in Theorem 10 below.

THEOREM 10. *$d = pq \equiv 5$ [8], $p < q$ and $p \equiv q \equiv 3$ [4]. If*

$$|f_p(k)| = \left|pk^2+pk+\frac{p-q}{4}\right|$$

is prime or equal to one whenever $0 \leqq k \leqq \frac{1}{3}\sqrt{d}-1$, then $h(d) = 1$ and $d = p^2s^2 \pm 4p$, or $d = 4p^2s^2 \pm p$, or

$$d = p\,\frac{p(3b+4)^2+4}{9} \quad \textit{with } p \equiv -1\,[12].$$

The only known such values are: $d = 21, 69, 77, 93, 141, 213, 237, 413, 437, 453, 573, 717, 1077, 1133, 1253, 1293$ and 1757. They all write $d = p^2s^2 \pm 4p$, or $d = 4p^2s^2 \pm p$.

https://doi.org/10.4153/CJM-1990-018-3 Published online by Cambridge University Press

Remark. We are now in a position to discuss Mollin-Williams' Conjecture 1. Let k_0 be the infimum introduced just before Conjecture 1. We have:

d	k_0	$f_p(k_0)$	known values with $h(d) = 1$
$p\,\dfrac{p(3b+2)^2+4}{9}$	$\dfrac{3pb+p+1}{9} - \dfrac{b+1}{2}$	$\left(k_0 + \dfrac{b+1}{2}\right)\left(p\left(k_0 - \dfrac{b-1}{2}\right) - 1\right)$	$(p, b, d) = (11, 1, 341)$
$p\,\dfrac{p(3b+4)^2+4}{9}$	$\dfrac{3pb+5p-1}{9} - \dfrac{b+3}{2}$	$\left(k_0 + \dfrac{b+3}{2}\right)\left(p\left(k_0 - \dfrac{b+1}{2}\right) - 1\right)$	none

This value k_0 agrees with the optimal upper bound in the only known case $h(d) = 1$. If this value k_0 were the optimal upper bound, it would imply that Conjecture 1 based on numerical evidences cannot be proved by algebraic means only. Though Mollin-Williams' conjecture so happens to hold empirically, we must however notice that, algebraically speaking, this conjecture is not satisfactory. Indeed Theorem 10 presents us with a more restrictive hypothesis, yet not implying such a narrow conclusion as the field being of Richaud-Degert type. There could have existed fields

$$\text{the non empty family of fields } \mathbf{Q}(\sqrt{d}),$$
$$d = p\,\frac{p(3b+2)^2+4}{9} \quad \text{and} \quad h(d) = 1$$

such that the hypothesis of Conjecture 1 would have held

$$\left(\text{since } \frac{3pb+p+1}{9} - \frac{b+1}{2} \text{ can be greater than } \tfrac{1}{4}\sqrt{d} - \tfrac{1}{2}\right)$$

whereas its conclusion would not. If such fields do not exist, it is just because, under the Riemann's hypothesis, this family is reduced to one field: $d = 341$

$$\left(\text{for which we have } \frac{3pb+p+1}{9} - \frac{b+1}{2} > \tfrac{1}{4}\sqrt{d} - \tfrac{1}{2}\right).$$

Hence, if Conjecture 1 holds numerically, it is thanks to nothing but the work of chance, and there is no hope to ever settling it by algebraic means.

In order to settle Theorem 10, we will show that the primality of the $f_p(k)$'s implies that there exists a few primitive integral ideals with small norm. Lemma 11 below then gives us the field as being essentially a field of Richaud-Degert type.

LEMMA 11. *d a square free positive integer such that the fundamental unit of the real quadratic field $\mathbf{Q}(\sqrt{d})$ is with norm $+1$. Let us suppose that the cycle of principal reduced ideals contains at most four non invariant ideals with norm less than $\frac{2}{3}\sqrt{D}$, at most two non invariant ideals with norm less than $\sqrt{D/5}$ and does not contain any non invariant ideal with norm less than $\frac{1}{3}\sqrt{D}$, then the field is of Richaud-Degert type or*

$$D = M\frac{M(3b+2)^2+4}{9} \quad \textit{or} \quad M\frac{M(3b+4)^2+4}{9}, \qquad M \equiv -1\,[3].$$

Proof. Let

$$\mathbf{R}_0 = \mathbf{R} = \left(1, \frac{m+\sqrt{D}}{2}\right)_{\mathbf{Z}}$$

be the ring of algebraic integers of the field, let

$$x_0(\mathbf{R}) = \frac{m+\sqrt{D}}{2} = [\overline{a, n_1, n_2, \dots, n_k, b, n_k, \dots, n_2, n_1}]$$

be the continued fractional expansion of the real quadratic reduced surd attached to $\mathbf{R}$ (with even length $L = 2k+2$, since the fundamental unit is with norm $+1$) and let $\mathbf{R}_k$ be the k-th ideal with norm N_k of the cycle of principal reduced ideals. By Louboutin [**6**], Proposition 7, $\mathbf{R}_0$ and $\mathbf{R}_{k+1}$ are the only reduced invariant principal ideals. Since

$$x_0(\mathbf{R}_k) < x_0(\mathbf{R}_k) - x_0'(\mathbf{R}_k) = \frac{\sqrt{D}}{N_k} < 3,$$

we have $n_k \leqq 2$, for n_k is the greatest integer less than or equal to $x_0(\mathbf{R}_k)$.

We first show that at most one of the n_i's equals 2. Let us suppose $n_i = n_j = 2$ and $i < j$. Since $n_{i+1} = 1$ or 2,

$$x_i(\mathbf{R}) = [2, 2, \alpha] > [2, 2, 1] = \tfrac{7}{3} > \sqrt{5},$$

or

$$x_i(\mathbf{R}) = [2, 1, \alpha] > [2, 1, 1] = \tfrac{5}{2} > \sqrt{5},$$

hence $N_i < \sqrt{D/5}$. Moreover, since $n_{j-1} = 1$ or 2, $x_j(\mathbf{R}) = [\overline{2, \dots, 2}]$ which implies

$$x_j(\mathbf{R}) - x_j'(\mathbf{R}) = [2, \alpha] + [0, 2, \beta] > [2] + [0, 2, 1] = \tfrac{7}{3} > \sqrt{5},$$

https://doi.org/10.4153/CJM-1990-018-3 Published online by Cambridge University Press

or

$$x_j(\mathbf{R}) = [\overline{2,\dots,1}]$$

which implies

$$x_j(\mathbf{R}) - x_j'(\mathbf{R}) = [2,\alpha] + [0,1,\beta] > [2] + [0,1,1] = \tfrac{5}{2} > \sqrt{5}.$$

Hence $N_j = N(\mathbf{R}_j) < \sqrt{D/5}$. Since $\mathbf{R}_i$ and $\mathbf{R}_j$ together with their conjugate ideals are four non invariant reduced principal ideals with norm less than $\sqrt{D/5}$, this contradiction provides us with our assertion.

Let us first suppose that all the n_i's are equal to 1.

If $k \geqq 3$ and all the n_i are equal to one, let $\mathbf{I} = \mathbf{R}_1$, $\mathbf{J} = \mathbf{R}_2$ and $\mathbf{K} = \mathbf{R}_3$. Then

$$x_0(\mathbf{I}) = [\overline{1,\dots,1,b,1,\dots,1,a}], \quad x_0(\mathbf{J}) = [\overline{1,\dots,1,b,1,\dots,1,a,1}]$$

and

$$x_0(\mathbf{K}) = [\overline{1,\dots,1,b,1,\dots,1,a,1,1}].$$

Hence,

$$x_0(\mathbf{I}) = [1,1,\alpha] > [1,1,1] = \tfrac{3}{2}, \quad x_0(\mathbf{J}) = [1,1,\alpha] > [1,1,1] = \tfrac{3}{2}$$

and

$$x_0(\mathbf{K}) - x_0'(\mathbf{K}) = [1,\alpha] + [0,1,\beta] > 1 + [0,1,1] = \tfrac{3}{2}.$$

Thus, $\mathbf{I}$, $\mathbf{J}$, $\mathbf{K}$ and their conjugate ideals are six reduced non invariant principal ideals with norm lower than $\frac{2}{3}\sqrt{D}$. This case cannot occur.

If $k = 0$, the field is of Richaud-Degert type. Indeed, since

$$\frac{m+\sqrt{D}}{2} = [\overline{a,b}] = \frac{ab+\sqrt{\Delta}}{2b}$$

with $\Delta = ab(ab+4)$, b divides $4a$. If we write $4a = \lambda b$, then

$$D = \frac{\lambda^2 b^2}{4} + \lambda$$

and the field is of Richaud-Degert type.

If $k = 1$ and $n_1 = 1$ the field is also of Richaud-Degert type. Since

$$x_0(\mathbf{R}) = [\overline{a,1,b,1}] = \frac{a(b+2)+\sqrt{\Delta}}{2(b+2)} = \frac{m+\sqrt{D}}{2}$$

with

$$\Delta = (a+2)(b+2)(ab+2a+2b),$$

$b+2$ divides $2(a+2)$ and if we write

$$a = \frac{\lambda}{2}(b+2) - 2 \quad \text{then} \quad D = \frac{\lambda^2(b+2)^2}{4} - 2\lambda.$$

If $k = 2$ and $n_1 = n_2 = 1$, the field is again of Richaud-Degert type.

Let us now suppose that one (and exactly one) n_{i_0} equals 2. We first show that $k \leqq 2$. Let us suppose $k \geqq 3$. If

$$(n_{i_0}, n_{i_0+1}, n_{i_0+2}) = (2, 1, 1),$$

then

$$x_{i_0}(\mathbf{R}) = [2, 1, \alpha] > [2, 1, 1] = \tfrac{5}{2} > \tfrac{3}{2},$$
$$x_{i_0+1}(\mathbf{R}) = [1, 1, \alpha] > [1, 1, 1] = \tfrac{3}{2}$$

and

$$x_{i_0+2}(\mathbf{R}) - x'_{i_0+2}(\mathbf{R}) = [1, \alpha] + [0, 1, 2, \beta] > 1 + [0, 1, 2] = \tfrac{5}{3} > \tfrac{3}{2}.$$

This case cannot occur. If

$$(n_{i_0-1}, n_{i_0}, n_{i_0+1}) = (1, 2, 1),$$

then

$$x_{i_0}(\mathbf{R}) - x'_{i_0}(\mathbf{R}) = [2, 1, \alpha] + [0, 1, \beta] > [2, 1, 1] + [0, 1, 1] = 3,$$

hence

$$N_{i_0} < \tfrac{1}{3}\sqrt{D}.$$

This case cannot occur. Now, whenever $k \geqq 3$ and exactly one n_{i_0} of the n_i's equals 2, it is easily seen that one of the two sequences $(n_1, n_2, \ldots, n_k)$ or $(n_k, n_{k-1}, \ldots, n_1)$ contains the subsequence $(2, 1, 1)$ or $(1, 2, 1)$. This contradiction provides us with our assertion. Hence, we can suppose that $1 \leqq k \leqq 2$ holds.

If $k = 1$ and $n_1 = 2$ the field is also of Richaud-Degert type. Since

$$x_0(\mathbf{R}) = [\overline{a, 2, b, 2}] = \frac{a(b+1) + \sqrt{\Delta}}{2(b+1)} = \frac{m + \sqrt{D}}{2}$$

https://doi.org/10.4153/CJM-1990-018-3 Published online by Cambridge University Press

with

$$\Delta = (a+1)(b+1)(ab+a+b),$$

$b+1$ divides $a+1$ and if we write

$$a = \lambda(b+1)-1 \quad \text{then} \quad D = \lambda^2(b+1)^2 - \lambda.$$

If $k=2$ and $n_2 = 2$, then

$$x_0(\mathbf{R}) = [\overline{a,1,2,b,2,1}] = \frac{a(9b+6)+\sqrt{\Delta}}{2(9b+6)} = \frac{m+\sqrt{D}}{2}$$

and

$$x_4(\mathbf{R}) = [\overline{b,2,1,a,1,2}] = \frac{b(9a+12)+\sqrt{\Delta}}{2(9a+12)} = \frac{m'+\sqrt{D}}{2M},$$

with

$$\Delta = (3a+4)(9b+6)(3ab+2a+4b+4)$$

and M the norm of the second invariant ideal of the cycle of principal reduced ideals. Hence,

$$M = \frac{9a+12}{9b+6}, \quad a = \frac{M(3b+2)-4}{3} \quad \text{and} \quad D = M\,\frac{M(3b+2)^2+4}{9}.$$

If 3 divides M, then 9 divides M, which is impossible since M being the norm of a primitive invariant ideal is a square free integer. Hence, 3 does not divide M and $M \equiv -1$ [3]. In the same way, if $k=2$ and $n_1 = 2$, then

$$x_0(\mathbf{R}) = [\overline{a,2,1,b,1,2}] \quad \text{and} \quad D = M\,\frac{M(3b+4)^2+4}{9},$$

with $M \equiv -1$ [3].

LEMMA 12. $d = pq \equiv 5$ [8]. *If*

$$|f_p(k)| = \left|pk^2 + pk + \frac{p-q}{4}\right|$$

is prime or equal to one whenever $0 \leqq k \leqq \frac{1}{3}\sqrt{d} - 1$ *and if there exists* k *such that* $|f_p(k)| < \frac{1}{3}\sqrt{d}$ *and* $0 \leqq k \leqq \frac{1}{3}\sqrt{d} - 1$, *then* $d = p^2s^2 \pm 4p$ *and* $h(d) = 1$.

Proof. If $|f_p(k)| = 1$, we argue as in Theorem 9. Let us suppose that $|f_p(k)| = s$ is prime. Let r be such that $0 \leqq sr - k - 1 \leqq s - 1$. Then, as in Theorem 9, with $k' = sr - k - 1$, we get

$$f_p(k') = \pm r + psr(sr - (2k+1)), \quad sr = 2k+1 \quad \text{and} \quad d = p^2s^2r^2 \pm 4ps.$$

https://doi.org/10.4153/CJM-1990-018-3 Published online by Cambridge University Press

Since $d = pq$, $s = 1$ and this contradiction provides us with the result.

End of the proof of Theorem 10. If there exists k such that

$$0 \leqq k \leqq \tfrac{1}{3}\sqrt{d} - 1$$

and such that

$$|f_p(k)| \leqq \tfrac{1}{3}\sqrt{d},$$

Lemma 12 provides us with the result.

Otherwise, we show that we can apply Lemma 11. Since $p \equiv q \equiv 3$ [4], d is not the sum of two squares, the fundamental unit is with norm $+1$ and the 2-rank of the ideal class-group is zero. By Theorem 4, $h(d) = 1$. Let $\mathbf{I}$ be a primitive ideal with norm N such that

$$N \leqq \tfrac{2}{3}\sqrt{d} \quad \text{and} \quad p \nmid N.$$

Then $N < \sqrt{d} < q$, hence $q \nmid N$. By the remark following Theorem 4, $\mathbf{I}$ is equivalent to $\mathbf{I}_p$ and

$$N \in \left\{ |f_p(k)|;\ 0 \leqq k \leqq \tfrac{1}{3}\sqrt{d} - 1 \right\}.$$

Hence $N > \frac{1}{3}\sqrt{d}$ or $N = 1$. Let $\mathbf{I}$ be a primitive ideal with norm N such that $N < \sqrt{d}$ (this condition is satisfied if $\mathbf{I}$ is a reduced ideal, see [**5**]), and such that p divides N. Then p^2 does not divide N and $\mathbf{I} = \mathbf{I}_p\mathbf{J}$, with $\mathbf{J}$ a primitive ideal with norm M such that p does not divide M and such that

$$M \leqq \frac{N}{p} < \tfrac{1}{3}\sqrt{d}.$$

Hence, $M = 1$ and $\mathbf{I} = \mathbf{I}_p$.

Thus, if $\mathbf{I}$ is a reduced ideal with norm N, then $\mathbf{I} = \mathbf{R}$, or $\mathbf{I} = \mathbf{I}_p$ or G.C.D.$(d, N) = 1$ and $N > \frac{1}{3}\sqrt{d}$.

Now,

$$|f_p(k)| \leqq \frac{\alpha}{4}\sqrt{d}$$

if and only if

$$y^2 - \alpha y \leqq (2k+1)^2 \leqq y^2 + \alpha y, \quad \text{with } y = \frac{1}{p}\sqrt{d}.$$

Moreover,

$$g(y) = \frac{\sqrt{y^2 + \alpha y} - \sqrt{y^2 - \alpha y}}{2}$$

https://doi.org/10.4153/CJM-1990-018-3 Published online by Cambridge University Press

is decreasing whenever $y \geqq \alpha$, and the inequalities above admit the only solution $k = 0$ until $y \leqq y_0$, when

$$y_0 = \frac{\sqrt{\alpha^2 + 36} - \alpha}{2}$$

is solution of $y_0^2 + \alpha y_0 = 9$. Therefore, whenever $\alpha < 4/\sqrt{5}$, the inequalities above admit at most one solution (since we can suppose $y \geqq y_0$ and since $g(y_0) < 1$ whenever $\alpha < 4/\sqrt{5}$). Moreover, with $\alpha = \frac{8}{3}$,

$$g(y) \leqq g\left(\tfrac{8}{3}\right) < 2.$$

Therefore, whenever $\alpha = \frac{8}{3}$, the inequalities above admit at most two solutions. Thus, there exist at most one integer k such that

$$|f_p(k)| \leqq \sqrt{d/5}$$

and at most two integers k such that

$$|f_p(k)| \leqq \tfrac{2}{3}\sqrt{d},$$

hence at most two primitive ideals with norm N such that $N \leqq \sqrt{d/5}$ and $p \nmid N$, and at most four primitive ideals with norm N such that

$$N \leqq \tfrac{2}{3}\sqrt{d} \quad \text{and} \quad p \nmid N.$$

Thus, there exist at most four reduced non invariant principal ideals with norm less than $\frac{2}{3}\sqrt{d}$, at most two reduced non invariant principal ideals with norm less than $\sqrt{d/5}$ and there does not exist any non invariant principal reduced ideal with norm N such that $N < \frac{1}{3}\sqrt{d}$. We now apply Lemma 11.

If the field is of Richaud-Degert type, since $d = pq$, then

$$d = p^2s^2 \pm 4p, \quad d = 4p^2s^2 \pm p, \quad d = m^2 + 4 \quad \text{or} \quad d = 4m^2 + 1.$$

Since d is not the sum of two squares, then

$$d \neq 4m^2 + 1,\ m^2 + 4.$$

If

$$d = p\frac{p(3b + 2)^2 + 4}{9},$$

then

$$k_0 = \frac{3pb + p + 1}{9} - \frac{b + 1}{2} \leqq \tfrac{1}{3}\sqrt{d} - 1$$

https://doi.org/10.4153/CJM-1990-018-3 Published online by Cambridge University Press

while

$$|f_p(k_0)| = \left(k_0 + \frac{b+1}{2}\right)\left(p\left(k_0 - \frac{b-1}{2}\right) - 1\right)$$

is not prime. Numerical computations based on [**5**], Theorem 3 to settle whether $h(d) = 1$ or not seem to indicate that there does not exist any field with

$$d = p\frac{p(3b+4)^2+4}{9} \equiv 5\ [8] \quad \text{and} \quad h(d) = 1.$$

Moreover, under Riemann's hypothesis it can be proved by means of the methods introduced in [**4**], [**5**] that there does not exist any field, and by means of the methods introduced in [**11**] that there exists at most one such field.

REFERENCES

1. S. Chowla, *On Euler's polynomial*, J. of Nb. Th. *13* (1981), 443–445.

2. M. D. Hendy, *Prime quadratics associated with complex quadratic fields of class-number two*, P.A.M.S. *43* (1974), 253–266.

3. M. Kutsuna, *On a criterion for the class number of a quadratic number field to be one*, Nagoya Math. J. *79* (1980), 123–129.

4. S. Louboutin, *Arithmétique des corps quadratiques réels et fractions continues*, Thèse de Doctorat, Université Paris 7 (1987).

5. ——— *Continued fractions and real quadratic fields*, J. of Nb. Th. *30* (1988), 167–176.

6. ——— *Groupe des classes d'ideaux triviaux*, To appear, Acta Arithmetica *54*.

7. ——— *Prime producing quadratic polynomials and class-numbers of complex quadratic fields*, To appear.

8. R. A. Mollin, *Class number one criteria for real quadratic fields*, Proc. Japan Acad. *63*, Ser. A (1987).

9. R. A. Mollin and H. C. Williams, *On prime valued polynomials and class number of real quadratic fields*, Nagoya Math. J. *112* (1988), 143–151.

10. ——— *Prime producing quadratic polynomials and real quadratic fields of class-number one*, Théorie des nombres/ Number theory "Comptes Rendus de la Conférence Internationale de Théorie des Nombres tenue à l'Université Laval en 1987/ Proceedings of the International Number Theory Conference held at Université Laval in 1987 (W. de Gruyter, Berlin, New York, 1989).

11. ——— *Solution of the class-number one problem for real quadratic fields of Richaud-Degert type*, Proc. of the first Conf. of the Canadian Number Theory Assoc. held at the Banff Center, Banff, Alberta, April 17–27 1988 (W. de Gruyter, Berlin, New York, 1989).

12. ——— *Class-number one for real quadratic fields, continued fractions and reduced ideals*, Proc. of the NATO ASI on Nb. Th. and Applications, Banff 1988 (Kluwer Academic Publishers, Netherlands, 1989).

13. R. Sasaki, *A characterisation of certain real quadratic fields*, Proc. Japan Acad. *62*, Ser. A (1986), 97–100.

14. ——— *Generalized Ono invariants and Rabinovitch's theorem for real quadratic fields*, Nagoya Math. J. *109* (1988), 117–124.

15. H. Yokoi, *Class-number one problem for certain kind of real quadratic fields*, Proc. Int. Conf. on Class Numbers and Fundamental Units, Katata, Japan (1986).

University of Caen,
Caen, France

https://doi.org/10.4153/CJM-1990-018-3 Published online by Cambridge University Press