Can. J. Math. Vol. 47 (5), 1995 pp. 1023–1036.

PROOF, DISPROOF AND ADVANCES CONCERNING CERTAIN CONJECTURES ON REAL QUADRATIC FIELDS $Q(\sqrt{N^2+4})$

R. A. MOLLIN AND H. C. WILLIAMS

ABSTRACT. The purpose of this paper is to address conjectures raised in [2]. We show that one of the conjectures is false and we advance the proof of another by proving it for an infinite set of cases. Furthermore, we give hard evidence as to why the conjecture is true and show what remains to be done to complete the proof. Finally, we prove a conjecture given by S. Louboutin, for *Mathematical Reviews*, in his discussion of the aforementioned paper.

1. **Introduction.** In [2] Leu raised 2 conjectures concerning real quadratic fields $Q(\sqrt{n^2+4})$ where $D = n^2 + 4$ is square-free. To state them we first need some notation.

DEFINITION 1.1. Let D be the discriminant of a real quadratic field $Q(\sqrt{D})$, and let $M_D = \sqrt{D}/2$, the Minkowski bound. If $(*/*)$ denotes the Kronecker symbol then

$$S_D = \{r : r \text{ is prime}, r < \sqrt{D}/2 \text{ and } (D/r) \neq -1\}.$$

Thus, if h_D denotes the class number of $Q(\sqrt{D})$ we have:

CONJECTURE 1.1. *Let $D = n^2 + 4$ be square free, then $h_D = 2$ if and only if $D = pq$ for primes $p < q$ with $p \equiv q \equiv 1 \pmod 4$ and $1 \leq |S_D| \leq 2$ such that if $r \in S_D$ with $(D/r) = 1$ then $r^2 > \sqrt{D}/2$.*

This conjecture was actually stated by Leu [2, Conjecture, p. 309] in an unnecessarily complicated fashion with conditions which were not needed (see Remark 3.2). In Section 3, we give a proof of the sufficiency for $h_D = 2$ which is much simpler and more informative than that given in [2] (see Theorem 3.1). Moreover, we prove the necessity when the prime $p = 4k^2 + 1$ and show how we "just miss" a proof when p is of the form $k^2 + 4$ (see Theorem 3.2ff). Primes p of these two forms are carefully chosen because we know, with one possible exception (which is ruled out by the generalized Riemann hypothesis, GRH) the complete list of those values for which Conjecture 1.1 holds (see Example 3.1), and in that list p is always one of the above two forms. In any discussion which follows, we will call the aforementioned exceptional value a "GRH-ruled out exception". In point of fact, we used such techniques in [7] to list all possible values $D = k^2 + r$ where $r \mid 4k$ (called *extended Richard-Degert types*, or simply ERD-types)

The authors' research was supported by NSERC Canada grant #A8484 (respectively #A7649).
Received by the editors August 24, 1994.
AMS subject classification: Primary: 11R11, 11R29; secondary: 11J70.

with $h_D = 2$, and one GRH-ruled out exception. Previously in [6] we had solved the $h_D = 1$ problem for ERD-types with one GRH-ruled out exception. This included the Chowla conjecture (see [8]) and several conjectures given by the authors in [4]–[5]. This technique, (which is now standard and easily applied to a vast array of class number problems for real quadratic fields) consists of using a result of Tatuzawa [15] to give a complete list of discriminants which, due to Tatuzawa's result, may be lacking in at most one value. We then use the GRH and the analytic class number formula to show that the list is indeed complete (see [9] for a detailed description of these techniques). Hence, the exceptional value resulting from Tatuzawa's result would necessarily be a counterexample to the GRH. This explains then why we call it a "GRH-ruled out exception". In point of fact, we were able to refine our techniques and make our procedures more efficient in [10] where we found a complete list (with one GRH-ruled out exception) of *all* real quadratic fields $Q(\sqrt{D})$ with $h_D = 2$ when the continued fraction expansion of w (see definition in Section 2) has period length less than 25. We note that D's of ERD-type have period length of the continued fraction expansion of w being at most 6. Leu's proof of Conjecture 1.1 under the assumption of GRH in [2] does not take into account any of the above results. Previously we proved a similar result for a list of all D's with $h_D = 1$ and period length of the continued fraction expansion of w less than 25 in [11]. What we now seek therefore, is an *unconditional* proof that these lists are complete. The difficulty is verifying this for even the restricted forms considered in this paper shows how far we have yet to go. In fact, we believe that to complete the proof of Conjecture 1.1 may be as difficult as giving an unconditional proof of the Chowla conjecture.

Another conjecture given by Leu in [2] is

CONJECTURE 1.2. *If $D = n^2 + 4$ is square-free then $|S_D| \leq 2h_D - 1$.*

We show that this conjecture is false (see Table 3.1ff) and give evidence that there are in fact infinitely many counterexamples.

In his review of Leu's paper [2], S. Louboutin (see MR #93f: 11075) says that Conjecture 1.1 is a "deceptively reasonable one". He goes on to say that "... it is reasonable to conjecture that ..."

CONJECTURE 1.3. *For all integers $m > 0$ there exists a prime p such that whenever $D = pq = n^2+4$ where $q > p$ is also prime we have $l(\alpha) \geq 2m+3$ where $\alpha = (\sqrt{D}+p)/2p$, and $l(\alpha)$ is the period length of the continued fraction expansion of α (see Section 2).*

We have stated this conjecture in our terminology for convenience sake, (see Section 2 for details on notation). In Section 3 we give a complete proof of this conjecture, (see Theorem 3.3). Our earlier contention that the proof of Conjecture 1.1 is seriously difficult is borne out by Louboutin's last comment in his review pertaining to Conjecture 1.3. He says, "Hence, the author's conjecture could not be proved algebraically even if he changed $|S_D| = 1$ or 2 into $1 \leq |S_D| \leq l$ for any $l \geq 2$." Therefore, any advance toward the proof of Conjecture 1.1 should be viewed as significant progress.

2. **Notation and preliminaries.** Throughout, D will be a positive square-free integer and $w = (\sigma - 1 + \sqrt{D})/\sigma$ where $\sigma = 2$ if $D \equiv 1 \pmod 4$ and $\sigma = 1$ otherwise. The discriminant Δ of $Q(\sqrt{D}) = K$ is given by $\Delta = (2/\sigma)^2 D$. If $[\alpha, \beta]$ denotes the module $\{\alpha x + \beta y : x, y \in \mathbb{Z}\}$ then the *maximal order* O_Δ of K is $[1, w]$. We use $\bar{\alpha}$ to denote the *algebraic conjugate* of α and $N(\alpha)$ to denote the value of $\alpha\bar{\alpha}$, the *norm* of α.

An ideal of O_Δ can be written as $I = [a, b+w]$ where $a, b, c \in \mathbb{Z}$ with $a, c > 0, c|b, c|a$ and $ac|N(b+cw)$. Conversely, if $a, b, c \in \mathbb{Z}$ with $c|b, c|a$ and $ac|N(b+cw)$ then $[a, b+cw]$ is an ideal of O_Δ. In an ideal $I = [a, b+cw]$ with $a, c > 0$ the *norm* of I, $N(I)$ is given by $N(I) = ac > 0$. If $c = 1$ then I is a *primitive* ideal. The *conjugate* of $I = [a, b+w]$ is $I' = [a, b+\bar{w}]$. A primitive ideal I is *reduced* if it does not contain any non-zero element α such that both $|\alpha| < N(I)$ and $|\bar{\alpha}| < N(I)$.

At this juncture we introduce the connection between reduced ideals and continued fractions. Let $\alpha \in K$ then we can write $\alpha = (P_0 + \sqrt{D})/Q_0$ where $P_0, Q_0 \in \mathbb{Z}$. If we put $a_0 = \lfloor \alpha \rfloor$ (where $\lfloor\ \rfloor$ is the greatest integer function) and define

$$\begin{aligned} P_{i+1} &= a_i Q_i - P_i \\ Q_i Q_{i+1} &= D - P_{i+1}^2 \quad \text{and} \\ a_{i+1} &= \lfloor (P_{i+1} + \sqrt{D})/Q_{i+1} \rfloor \quad (i = 0, 1, 2, \ldots) \end{aligned}$$

then

$$\alpha = \langle a_0, a_1, \ldots, a_i, \ldots \rangle$$

is the continued fraction expansion of α. Moreover, we have

THEOREM 2.1. *Let $I_1 = I = [a, b+w]$ be a reduced ideal of O_Δ. If $\alpha = (b+w)/a$ then all of the reduced ideals in the same equivalence class as I and only these are given by*

$$I_j = [Q_{j-1}/\sigma, (P_{j-1} + \sqrt{D})/\sigma]$$

for $j = 1, 2, 3, \ldots$ where the values of the P_j's and Q_j's are found by expanding α into a continued fraction.

THEOREM 2.2. *If I is a reduced ideal of O_Δ then $N(I) < \sqrt{\Delta}$. If I is a primitive ideal of O_Δ such that $N(I) < \sqrt{\Delta}/2$, then I is a reduced ideal of O_Δ.*

By Theorem 2.2, there can only be a finite number of reduced ideals of O_Δ and since all the I_j's from Theorem 2.1 are reduced then we see that the sequence of reduced ideals $I_1, I_2, \ldots, I_j, \ldots$ produced by the continued fraction must be purely periodic, *i.e.*, there must exist a minimal positive integer l such that $I_{l+1} = I_1$. We call $l(\alpha) = l = l(I)$ the *period length* of the continued fraction expansion of α. For convenience sake, we denote the period length of continued fraction expansion of w by $l(1)$.

Let C_Δ denote the *class group* of K and let h_Δ be its order; *i.e.*, the *class number* of K. Equivalence of ideals is denoted by $I \sim J$, and the *class* of I is denoted by $\{I\}$. We also have

THEOREM 2.3. *(1) If I is a reduced ideal of O_Δ then there exists an ideal of $J \sim I$ such that $N(J) < \sqrt{\Delta}/2$.*

(2) C_Δ is generated by the primitive ideals I with $N(I) < \sqrt{\Delta}/2$.

Immediate from the above is

THEOREM 2.4. *Let $\Delta > 0$ be a discriminant and $\bigcup_{i=1}^{k}\{J_i\}$ classes of primitive ideals in O_Δ, then $C_\Delta = \bigcup_{i=1}^{k}\{J_i\}$ if and only if for each prime $p < \sqrt{\Delta}/2$ with $(\Delta/p) \neq -1$, there exists an integer i with $1 \leq i \leq k$ and a reduced ideal $I_i = [a_i, b_i + w] \sim J_i$ such that in the continued fraction expansion of $\alpha_i = (b_i + w)/a_i$ we have $Q_j/\sigma = p$ for some j with $1 \leq j \leq l_i = l(\alpha_i)$.*

REMARK 2.1. If $I = [a, b + w]$ is a reduced ideal in an *ambiguous* class of C_Δ (*i.e.*, $I^2 \sim 1$) then in the continued fraction expansion of $\alpha = (b + w)/a$ we must have either $Q_{\frac{l+1}{2}} = Q_{\frac{l-1}{2}}$ (when $l(\alpha) = l$ is odd) or $P_{\frac{l}{2}} = P_{\frac{l}{2}+1}$ when l is even (see [9]).

We also have

THEOREM 2.5. *If I is a reduced ideal in O_Δ and ϵ_Δ is the fundamental unit of $Q(\sqrt{\Delta})$ then $N(\epsilon_\Delta) = (-1)^{l(I)}$.*

For complete details and proofs concerning the above results, the reader is referred to [9] and [16].

Finally we include the following result for the sake of completeness since we will have occasion to use it in the next section.

THEOREM 2.6. *Let $D = n^2 + 4$ be square-free and set $-N(b + w) = mt$ where $|b| < (\sqrt{D} - 1)/2$ and $m < n$, then $h(d) \geq \max\{\tau(m), \tau(m) + d(t) - 1\}$ where τ is the divisor function and $d(t)$ denotes the number of prime (not necessarily distinct) divisors of t.*

PROOF. This is a trivial consequence of Mollin et. al. [14, Theorem 2.1 p. 94]. ■

3. **Conjecture 1.1.** We first prove the "easy" direction of Conjecture 1.1, *i.e.*, the sufficiency for $h_D = 2$.

THEOREM 3.1. *If $D = n^2 + 4 = pq$, for primes $p < q$ and $1 \leq |S_D| \leq 2$ with $r^2 > \sqrt{D}/2$ whenever $(D/r) = 1$ and $r \in S_D$, then $h_D = 2$.*

PROOF. By Theorems 2.3–2.4, $h_D = 1$ if and only if $S_D = \emptyset$. Therefore, we may assume that $h_D > 1$. Consider the reduced ideal $I = [p, (p + \sqrt{D})/2]$. In the continued fraction expansion of $\alpha = (p+\sqrt{D})/(2p)$ we must have that $l(\alpha) = l$ is odd by Theorem 2.5 (and $l > 1$ since $l = 1$ implies that $D = P_1^2 + 4p^2$ forcing $p^2|D$, a contradiction). By Remark 2.1, we must have that $Q_{\frac{l+1}{2}} = Q_{\frac{l-1}{2}} < \sqrt{D}$. Hence, $D = P_{\frac{l+1}{2}}^2 + Q_{\frac{l+1}{2}}^2$. Clearly p cannot divide $Q_{\frac{l+1}{2}}$ since D is square-free; thence, $Q_{\frac{l+1}{2}} = 2r_1^{s_1}r_2^{s_2}$ with $r_i \in S_D$ and $(D/r_i) = 1$ for $s_i \geq 0$. If $s_i > 0$ for $i = 1, 2$ then

$$D = P_{\frac{l+1}{2}}^2 + 4r_1^{2s_1}r_2^{2s_2} \geq P_{\frac{l+1}{2}}^2 + 4r_1^2r_2^2 > D$$

(since $r_i^2 > \sqrt{D}/2$ by hypothesis), a contradiction. Therefore, $s_2 = 0$ say, and $Q_{\frac{l+1}{2}} = 2r_1^{s_1}$. If $s_1 > 1$ then $Q_{\frac{l+1}{2}} > 2r_1^2 > \sqrt{D}$, a contradiction; whence $s_1 = 1$. Since $Q_{\frac{l+1}{2}} = 2r_1$ then $\mathcal{R}_1 \sim \mathcal{P}$ and so $\mathcal{R}_1^2 \sim \mathcal{P}^2 \sim 1$ where $\mathcal{R}_1$ lies over r_1 and $\mathcal{P}$ lies over p. Furthermore, $\mathcal{R}_1 \not\sim 1$ since $l(1) = 1$. We have thus far shown that if $|S_D| = 1$ or if $p \in S_D$ then $h_D = 2$, so we now assume that $S_D = \{r_1, r_2\}$ with $(D/r_i) = 1$ for $i = 1, 2$. Consider $D = P_1^2 + Q_0Q_1 = P_1^2 + 2pQ_1$. Since $S_D = \{r_1, r_2\}$, then $p > \sqrt{D}/2$; whence, $Q_1 < \sqrt{D}$. Moreover, $Q_1 \neq 2$ since $R_1 \sim 1$ as above. Thus, the only odd prime which can divide Q_1 is r_2, so $Q_1 = 2r_2^{s_2}$. If $s_2 > 1$ then $Q_1 > \sqrt{D}$ (since $r_2^2 > \sqrt{D}/2$ by hypothesis), a contradiction. Hence, $Q_1 = 2r_2$, whence $\mathcal{R}_2 \sim \mathcal{P}$ and $\mathcal{R}_2^2 \sim \mathcal{P}^2 \sim 1$. Hence, $h_D = 2$ and the result is secured. ∎

Now we look at the converse of Theorem 3.1.

Since $D = n^2+4$ then it follows from the genus theory of Gauss that $h_D = 2$ necessarily implies $D = pq$ for primes $p \equiv q \equiv 1 \pmod 4$. Suppose that $q > p$ and

$$p = a^2 + 4b^2 \quad \text{with } a, b > 0$$

and

$$q = s^2 + 4t^2 \quad \text{with } s, t > 0.$$

Since D must be a sum of 2 squares in essentially two distinct ways, we must have that

$$D = (as + 4bt)^2 + 4(bs - at)^2$$

and

$$D = (as - 4bt)^2 + 4(bs + at)^2$$

from which it follows that

$$bs - at = \epsilon = \pm 1 \tag{3.1}$$

and

$$bs + at = c \tag{3.2}$$

where c is divisible only by primes in S_D.

REMARK 3.1. It is evident that $S_D \neq \emptyset$. In fact, as noted in the proof of Theorem 3.1, $h_D = 1$ if and only if $S_D = \emptyset$. If D were not of the form $D = n^2 + 4$ then we would not be able to assert that $h_D = 1$ implies $S_D = \emptyset$ since it is possible, in general, to have $S_D = \emptyset$ while $h_D = 1$ when the primes in S_D have principal prime ideals above them. However, in our special case $l(1) = 1$ which means that there are *no nontrivial principal reduced ideals*. However we may always assert that $S_D = \emptyset$ implies $h_D = 1$ by Theorem 2.3.

REMARK 3.2. In [2] Leu states Conjecture 1.1 with more conditions given than are required. Thus his proof of the sufficiency (which we proved in a simpler fashion with only minimal assumptions in Theorem 3.1) uses facts which actually follow from $|S_D| \leq 2$. First of all he addresses the case where $S_D = \{p\}$ which we have shown cannot occur. (To see this, we look at the proof of Theorem 3.1. If $S_D = \{p\}$ then $Q_{\frac{l+1}{2}}$ would be forced to equal 2, *i.e.*, $\mathcal{P} \sim 1$. Therefore, $h_D = 1$ which forced $S_D = \emptyset$, by Remark 3.1, a contradiction). Therefore, [2, Lemma 1, p. 310] is vacuous. Secondly, in proving the sufficiency he uses the additional assumptions that both $pr > \sqrt{D}/2$ when $(D/r) = 1$, and $(p/q) = -1$. Both of these facts follow from $|S_D| \leq 2$ as Theorem 3.1 clearly shows. Thus the use of the Redei-Reichardt result [2, Proposition D, p. 310] (*i.e.*, that $(p/q) = -1$ if and only if h_D is not divisible by 4) is unnecessary, as is [2, Proposition C, p. 310] which asserts that all primes $p|D$ satisfy $p \equiv 1 \pmod 4$, since our elucidation at the outset of this section shows that this actually follows from Gauss. Finally, our comments at the beginning of this section concerning $S_D = \emptyset$ shows that [2, Theorem 1, p. 310] is unnecessarily stated.

It is however, worth noting that in [3] Leu showed *unconditionally*, that if there are *no* inert primes less than M_Δ and S_Δ consists *only* of primes p with $(\Delta/p) = 1$, then $\Delta > 0$ implies that $\Delta \in \{2, 3, 5, 13, 17, 33, 73, 97\}$ none of which satisfies our criterion. Therefore, we must have inert primes less that M_Δ. However, in [12] we were able to classify those D's for which $|S_D| = 1$, and were able to list all of them with one GRH-ruled out exception. One sub-class of that classification is naturally our $D = n^2 + 4$ but the only ones with $h_D = 2$ for such D on that list are $D = 85$ and 269.

Now we examine the converse of Theorem 3.1

As delineated earlier, we know all of the square-free $D = n^2 + 4$ having $h_D = 2$, with one (GRH-ruled outed) exception. We now list them here with their associated continued fraction expansions for the classes of order 2 in $\mathcal{O}_D$.

EXAMPLE 3.1. (i) $D = 85 = 5 \cdot 17 = p \cdot q = 9^2 + 4$
The continued fraction expansion of $(5 + \sqrt{D})/6$ is:

i	0	1	2	3
P_i	5	7	5	5
Q_i	6	6	10	6
a_i	2	2	1	2

(ii) $D = 365 = 5 \cdot 73 = p \cdot q = 19^2 + 4$
The continued fraction expansion of $(15 + \sqrt{D})/14$ is:

i	0	1	2	3
P_i	15	13	15	15
Q_i	14	14	10	14
a_i	2	2	3	2

(iii) $D = 533 = 13 \cdot 41 = p \cdot q = 23^2 + 4$

The continued fraction expansion of $(15+\sqrt{D})/22$ is:

i	0	1	2	3	4	5
P_i	15	7	15	13	13	15
Q_i	22	22	14	26	14	22
a_i	1	1	2	1	2	1

(iv) $D = 629 = 17 \cdot 37 = p \cdot q = 25^2 + 4$
The continued fraction expansion of $(17+\sqrt{D})/10$ is:

i	0	1	2	3
P_i	17	23	17	17
Q_i	10	10	34	10
a_i	4	4	1	4

(v) $D = 965 = 5 \cdot 193 = p \cdot q = 31^2 + 4$
The continued fraction expansion of $(9+\sqrt{D})/26$ is:

i	0	1	2	3	4	5
P_i	9	17	9	25	25	9
Q_i	26	26	34	10	34	26
a_i	1	1	1	5	1	1

(vi) $D = 1685 = 5 \cdot 337 = p \cdot q = 41^2 + 4$
The continued fraction expansion of $(11+\sqrt{D})/34$ is:

i	0	1	2	3	4	5
P_i	11	23	11	35	35	11
Q_i	34	34	46	10	46	34
a_i	1	1	1	7	1	1

(vii) $D = 1853 = 17 \cdot 109 = p \cdot q = 43^2 + 4$
The continued fraction expansion of $(29+\sqrt{D})/22$ is:

i	0	1	2	3	4	5
P_i	29	37	29	17	17	29
Q_i	22	22	46	34	46	22
a_i	3	3	1	1	1	3

(viii) $D = 2813 = 29 \cdot 97 = p \cdot q = 53^2 + 4$
The continued fraction expansion of $(39+\sqrt{D})/38$ is:

i	0	1	2	3	4	5
P_i	39	37	39	29	29	39
Q_i	38	38	34	58	34	38
a_i	2	2	2	1	2	2

REMARK 3.3. We observe in Example 3.1 that all p's are of the form $p = k^2 + 4$ or $4k^2 + 1$. We now prove Conjecture 1.1 when p is of the form $4k^2 + 1$.

THEOREM 3.2. *Conjecture 1.1 holds when* $p = 4k^2 + 1$ *for some integer* $k \geq 1$.

https://doi.org/10.4153/CJM-1995-054-7 Published online by Cambridge University Press

PROOF. Let $q = r^2 + 4s^2$; whence, $r = 2m + 1$ and

$$D = (4k^2+1)(r^2+4s^2) = (r+4ks)^2 + 4(s-kr)^2 = (r-4ks)^2 + 4(s+kr)^2$$

Since D is representable as a sum of 2 squares in only 2 (essentially) distinct ways then we must have $s - kr = \epsilon$ where $|\epsilon| = 1$.

Since $n = r + 4ks$ then $n = r + 4k(kr + \epsilon) = pr + 4k\epsilon$. Therefore, $D = (pr + 4k\epsilon)^2 + 4 = p^2r^2 + 8\epsilon prk + 4p$. Now consider the continued fraction expansion of $(p + \sqrt{D})/(2p)$.

CASE 1. $\epsilon = 1$

i	0	1	2	3
P_i	p	pr	$(4k^2-1)r+4k$	pr
Q_i	$2p$	$4rk+2$	$4rk+2$	$2p$
a_i	$m+1$	$2k$	$2k$	r

CASE 2. $\epsilon = -1$ (in which case $r \geq 3$ since, if $r = 1$ then $q = 1 + 4(k-1)^2 < p$, a contradiction).

i	0	1	2	3
P_i	p	$pr-2p$	$(p-4k)r+2$	$(p-2)r-4k$
Q_i	$2p$	$(2p-4k)r-2(p-1)$	$4kr-2$	$4kr-2$
a_i	m	1	$2k-1$	$2k-1$

i	4	5
P_i	$(p-4k)+r+2$	$pr-2p$
Q_i	$(2p-4k)r-2(p-1)$	$2p$
a_i	1	$r-2$

Now, if we assume that $h_D = 2$ then, by Theorem 2.6, all $Q_i/2$'s in either case *must* be primes. Hence in Case 1, $|S_D| \leq 2$ clearly. In Case 2, we would have $|S_D| \leq 2$ if we could show that $Q_1/2 > \sqrt{D}/2$. Suppose, to the contrary, that $Q_1/2 < \sqrt{D}/2$ then

$$Q_1/2 = (p-2k)r - p + 1 < \sqrt{\Delta}/2$$

which implies that

$$pr - 2kr - p + 1 \leq (pr - 4k)/2$$

from which a calculation shows that

$$4k^2(r-2) + 4k(1-r) + r \leq 0,$$

or

$$\big(2(r-2)k - r\big)(2k-1) \leq 0.$$

Since $k \geq 1$ then we must have

$$k \leq r/(2r-4)$$

https://doi.org/10.4153/CJM-1995-054-7 Published online by Cambridge University Press

Hence,

$$k < \begin{cases} 2 & \text{if } r = 3 \\ 1 & \text{if } r \neq 3 \end{cases}$$

Since $k \geq 1$, then $r = 3$, $k = 1$ which implies that $s = 2$ and $q = 25$, a contradiction. The converse is Theorem 3.1. ∎

We now examine the only other case for p's appearing in Example 3.1; viz., $p = k^2+4$. From (3.1)–(3.2) we get that $b = 1$ and $a = k$. Therefore, $s = kt \pm 1$.

CASE 1. $s = kt - 1$. Thus the continued fraction expansion of $(p + \sqrt{D})/(2p)$ is

i	0	1	2	3	4	5
P_i	p	$tp-p$	$tp-c$	$kc-tp$	$tp-c$	$tp-p$
Q_i	$2p$	$(2tp-c-p)/2$	$2c$	$2c$	$(2tp-c-p)/2$	$2p$
a_i	$t/2$	2	$(k-1)/2$	$(k-1)/2$	2	$t-1$

CASE 2. $s = kt + 1$ which implies that the continued fraction expansion of $(p + \sqrt{D})/(2p)$ is

i	0	1	2	3	4
P_i	p	$tp-p$	$(c+p)/2$	$tp-c$	$kc-tp$
Q_i	$2p$	$(2tp+c-p)/2$	$(2tp-c+p)/2$	$2c$	$2c$
a_i	$t/2$	1	1	$(k-1)/2$	$(k-1)/2$

i	5	6	7
P_i	$tp-c$	$(c+p)/2$	$tp-p$
Q_i	$(2tp-c+p)/2$	$(2tp+c-p)/2$	$2p$
a_i	1	1	$t-1$

REMARK 3.4. Again by Theorem 2.6, all $Q_i/2$'s in either case must be primes. However, there is a good reason why they cannot all be primes in general. For example, if $D = 87029 = 29 \cdot 3001$ then the continued fraction expansion of $(29 + \sqrt{D})/58$ has period length 7 and all $Q_i/2$'s are primes. Moreover, $[29, (29 + \sqrt{D})/2]$ is ambiguous. However, $h_D = 10$ and so there is (of course) another ideal; viz., $[5, (3 + \sqrt{D})/2]$ which has order 5. Nevertheless, in our cases 1-2 above there is no clear algebraic way to show that D is a quadratic residue modulo any integer $m < \sqrt{\Delta}/2$ where $m \neq Q_i/2$ for any i with $1 \leq i \leq l(I)$ where the Q_i's appear in the continued fraction expansion of $(p+\sqrt{D})/(2p)$ with $I = [p, (p+\sqrt{D})/2]$ (as is the case with $D = 87029$ where $(D/5) = 1$ and $t = 10$). It is in fact quite frustrating that in cases 1-2 above we have $|S_D| \leq 3$ and we cannot eliminate the additional prime. If this could be done then we would have shown that the conjecture is true for p of the form either $k^2 + 4$ or $4k^2 + 1$. Then, in order to complete the proof of the conjecture we clearly would need only to show that if $h_D = 2$ then $b = 1$.

4. Proof of Conjecture 1.3 and disproof of Conjecture 1.2. In order to prove Conjecture 1.3, we begin with results for more general D's than those considered in the last section. (P and Q are also not necessarily primes).

THEOREM 4.1. *Let $D = PQ$ where $P = A^2 + B^2$, g.c.d. $(A, B) = 1$, $A > B > 0$, and $A/B = \langle q_0, q_1, \ldots, q_l \rangle$. If $Q = (rA_l + 2A_{l-1})^2 + (rB_l + 2B_{l-1})^2$ with $r \geq 1$ odd, then the continued fraction expansion of $(P + \sqrt{D})/(2P)$ is given by*

$$\langle (r+1)/2, \overline{q_l, q_{l-1}, \ldots, q_0, q_0, q_1, \ldots, q_l, r} \rangle.$$

PROOF. It is well-known that

$$\langle q_l, q_{l-1}, \ldots, q_1, q_0 \rangle = A_l/A_{l-1}$$

and

$$\langle q_l, q_{l-1}, \ldots, q_2, q_1 \rangle = B_l/B_{l-1}.$$

Put

$$L = A_{l-1}A_l + B_lB_{l-1},$$
$$M = A_{l-1}^2 + B_{l-1}^2.$$

We then get

$$\begin{aligned}\langle q_l, q_{l-1}, \ldots, q_1, q_0, q_0, q_1, \ldots, q_{l-1}, q_l \rangle &= \big((A_l/B_l)A_l + B_l\big)/\big((A_l/B_l)/A_{l-1} + B_{l-1}\big) \\ &= P/L\end{aligned}$$

and

$$\begin{aligned}&\langle q_l, q_{l-1}, \ldots, q_1, q_0, q_0, q_1, \ldots, q_{l-1} \rangle \\ &\qquad = \big((A_{l-1}/B_{l-1})A_l + B_l\big)/\big((A_{l-1}/B_{l-1})/A_{l-1} + B_{l-1}\big) \\ &\qquad = L/M.\end{aligned}$$

Let

$$\theta = \langle \overline{q_l, q_{l-1}, \ldots, q_1, q_0, q_0, q_1, \ldots, q_{l-1}, q_l, r} \rangle.$$

Then

$$\theta = \big(\theta(rP + L) + P\big)/\big(\theta(rL + M) + L\big).$$

Suppose that $r \geq 1$ and r is odd. Set

$$\begin{aligned}\lambda &= \langle (r+1)/2, \theta \rangle \\ &= (r+1)/2 + 1/\theta \\ &= \langle (r+1)/2, \overline{q_l, q_{l-1}, \ldots, q_0, q_0, \ldots, q_{l-1}, q_l, r} \rangle.\end{aligned}$$

Now

$$\theta^2(rL + M) + \theta L = \theta rP + \theta L + P,$$

which implies that

$$\theta^2(rL + M) = \theta rP + P.$$

https://doi.org/10.4153/CJM-1995-054-7 Published online by Cambridge University Press

If $\gamma = \frac{1}{\theta}$ then

$$P\gamma^2 + \gamma rP - (rL + M) = 0.$$

Thus, $\lambda = (r+1)/2 + \gamma$,

$$\gamma = \left(-rP + \sqrt{r^2P^2 + 4P(rL+M)}\right)/(2P)$$

and,

$$\lambda = \left(P + \sqrt{r^2P^2 + 4P(rL+M)}\right)/(2P).$$

Put $N = r^2P^2 + 4P(rL+M)$, then

$$N = P[r^2P + 4(rL+M)] = PQ = D.$$

Therefore, the continued fraction expansion of $(P+\sqrt{D})/(2P)$ is given by

$$\langle (r+1)/2, \overline{q_l, q_{l-1}, \ldots, q_0, q_0, \ldots, q_l, r} \rangle. \qquad \blacksquare$$

DEFINITION 4.1. Let $r > 1$ be a rational number and denote by $m(r)$ the value of t where $r = \langle q_0, q_1, q_2, \ldots, q_t \rangle$ with $q_t > 1$.

THEOREM 4.2. *For any positive integer m there exists an infinitude of primes p of the form $A^2 + B^2$ with $A > B$ such that $m(A/B) \geq m$.*

PROOF. We make use of the results of Hecke [1] from which we can easily deduce that there exists an infinitude of primes of the form $x^2 + y^2$ with

$$c_1 < \frac{x}{y} < c_2$$

for any given pair of positive reals c_1 and c_2 with $c_1 < c_2$. Consider

$$A_n/B_n = \langle a_0, a_1, a_2, \ldots, a_n \rangle$$

where $n \geq m$, and the only constraint we put on the a_i's is that they be positive integers. Now if

$$\begin{aligned} \lambda &= \langle a_0, a_1, a_2, \ldots, a_n, \theta \rangle \\ &= (\theta A_n + A_{n-1})/(\theta B_n + B_{n-1}), \end{aligned}$$

and $\theta = b/c$ with b and c being relatively prime integers then, if $\lambda = x/y$ we get $x = bA_n + cA_{n-1}$ and $y = bB_n + cB_{n-1}$. It follows that

$$b = (xB_{n-1} - yA_{n-1})(-1)^{n-1}$$

and

$$c = (yA_n - xB_n)(-1)^{n-1}.$$

https://doi.org/10.4153/CJM-1995-054-7 Published online by Cambridge University Press

If n is odd then $A_n/B_n > A_{n-1}/B_{n-1}$ and

$$b = xB_{n-1} - yA_{n-1}, \quad c = yA_n - xB_n.$$

Let p be a prime of the form $x^2 + y^2$ where

$$A_{n-1}/B_{n-1} < x/y < A_n/B_n.$$

In this case we have $b, c > 0$. If n is even then $A_{n-1}/B_{n-1} > A_n/B_n$. Let p be a prime of the form $x^2 + y^2$, where $A_n/B_n < x/y < A_{n-1}/B_{n-1}$. In this case we also have $b, c > 0$. Thus, in either case, we see that $\theta > 0$ and that the length of the continued fraction expansion of $\lambda = x/y$ is at least $n \geq m$. ∎

THEOREM 4.3. *For all integers $m > 0$, there exists a prime p such that whenever $D = pq = n^2 + 4$ where $q > p$ is also prime, we have that $l(\alpha) \geq 2m + 3$ where $\alpha = (\sqrt{D} + p)/(2p)$.*

PROOF. If $D = pq = n^2 + 4$, we may assume without loss of generality that $q > p$. By (3.1)–(3.2) we get that

$$n = as + 4bt = (ps - 4b\epsilon)/a,$$

so that $D = (ps - 4b\epsilon)^2/a^2 + 4 = (p^2s^2 - 8\epsilon psb + 4p)/a^2$. Also $bs \equiv \epsilon \pmod{a}$. Therefore if $b^*b \equiv 1 \pmod{a}$ then $s \equiv b^*\epsilon \pmod{a}$. Since a is odd, we may assume without loss of generality that b^* is even. Since $s \equiv b^*\epsilon \pmod{a}$ we can write $s = b^*\epsilon + ar$. Since s is odd, b^* is even, and a is odd, we must have that r is odd. Thus,

$$\begin{aligned} D &= \big(p^2(b^*\epsilon + ar)^2 - 8\epsilon pb(b^*\epsilon + ar) + 4p\big)/a^2 \\ &= \big(p^2a^2r^2 + 2\epsilon(b^*p - 4b)par + p(b^{*2} - 8bb^* + 4)\big)/a^2 \\ &= p^2r^2 + 2\epsilon(b^*p - 4b)pr/a + p(b^{*2} - 8bb^* + 4)/a^2. \end{aligned}$$

CASE 1. $a > 2b$. Thus, $a/2b = \langle q_0, q_1, \ldots, q_l\rangle = A_l/B_l$ with $q_l > 1$. We have that $A_lB_{l-1} - B_lA_{l-1} = (-1)^{l-1}$. We may now assume that $\epsilon = (-1)^l$; for if $\epsilon \neq (-1)^l$, set $q_{l+1} = 1$, replace the values of q_l by that of $q_l - 1$ and l by $l + 1$. We can then use $2A_{l-1}\epsilon$ for the value of b^*. In this instance,

$$A_l = a, B_l = 2b, B^* = 2A_{l-1}\epsilon,$$

and

$$B_{l-1} = (B_lA_{l-1} - \epsilon)/A_l = (2b\epsilon b^*/2 - \epsilon)/a = \epsilon(bb^* - 1)/a.$$

CASE 2. $a < 2b$. Put $2b/a = \langle q_0, q_1, \ldots, q_l\rangle = A_l/B_l$. We now assume that $\epsilon = (-1)^{l-1}$ and get

$$A_l = 2b, B_l = a, b^* = 2B_{l-1}\epsilon.$$

Also,

$$A_{l-1} = (A_lB_{l-1} - \epsilon)/B_l = \epsilon(bb^* - 1)/a.$$

https://doi.org/10.4153/CJM-1995-054-7 Published online by Cambridge University Press

In either case, we find that

$$\epsilon(b^*p - 4b)/(2a) = a\epsilon b^*/2 + 2b\epsilon(bb^* - 1)/a = A_{l-1}A_l + B_lB_{l-1},$$

and

$$(b^{*2}p - 8bb^* + 4)/(4a^2) = (b^*/2)^2 + \big((bb^* - 1)/a\big)^2 = A_{l-1}^2 + B_{l-1}^2.$$

Since, $p = A_l^2 + B_l^2$ which implies that

$$\begin{aligned} D/p &= q = pr^2 + 4(A_{l-1}A_l + B_lB_{l-1})r + 4(A_{l-1}^2 + B_{l-1}^2) \\ &= (rA_k + 2A_{k-1})^2 + (rB_l + 2B_{l-1})^2. \end{aligned}$$

Also, $b^*\epsilon + ar > 0$, since $s > 0$. Thus, if $a > 2b$ then $A_lr + 2A_{l-1} > 0$ which implies that $r \geq -1$. Also, if $a < 2b$ then $B_lr + 2B_{l-1} > 0$ implies that $r \geq -1$. If $r = -1$ then $q = (A_l - 2A_{l-1})^2 + (B_l - 2B_{l-1})^2 < A_l^2 + B_l^2 = p$, a contradiction. It follows that $r > 0$. By Theorem 4.1, we see that the value of $l(\alpha) = 2l + 3$. By Theorem 4.2, we know that there must exist, for any value of $m > 0$, some $p = A^2 + B^2$ such that $A > B$ and $m(A/B) > m$. Since $l \geq m$, we have $l(\alpha) \geq 2m + 3$ for this value of p. ∎

We have seen therefore, that if D is given by the above formula, there will be only 1 principal reduced ideal (the trivial one) but there can be an arbitrary number of reduced ideals equivalent to the reduced ideal $I = [p, (p + \sqrt{D})/2]$ depending upon the choice of the prime p. Finally, by Theorem 2.6, if $h_D = 2$ then all $Q_i/2$'s are primes and by (3.3), $l(I) \geq 2l + 3$.

Now we deal with Conjecture 1.2. As noted by Louboutin in his review of [2], (see MR: 93f: 11075), this conjecture is false. He notes only one counter example. We independently established this fact and did some computation and arrived at the following list of counterexamples for $D \leq 2 \cdot 10^6$, where $D = n^2 + 4$.

D	$2h_D - 1$	$\lvert S_D \rvert$	factors of D
237173	21	24	prime
316973	23	27	197, 1609
552053	29	33	prime
877973	39	42	37, 61, 5197
1585085	47	49	5, 61, 5197
1760933	59	60	373, 4721
1885133	51	56	1217, 1549

TABLE 4.1. Counterexamples to Conjecture 1.2.

We also compiled a list of counterexamples for $D \leq 10^9$ and found 518 counterexamples, too lengthy therefore to list here.

NOTE ADDED IN PROOF. All of the results in this paper will appear in the first author's book *Quadratics* to be published by C.R.C. Press 1995.

REFERENCES

1. E. Hecke, *Eine neue art von Zetafunctionen und ihre Beziehungen zur Verteilung der Primzahlen*, Math. Z. **6**(1920), 11–51.
2. M. G. Leu, *On a Criterion for the Quadratic Fields* $Q(\sqrt{n^2+4})$ *to be of Class Number Two*, Bull. London Math. Soc. **24**(1992), 309–312.
3. ———, *On a Problem of Ono and quadratic Non-Residues*, Nagoya Math. J. **115**(1989), 185–198.
4. R. A. Mollin, *Class Number One Criteria for Real Quadratic Fields I*, Proc. Japan Acad. Ser. A **63**(1987), 121–125.
5. R. A. Mollin and H. C. Williams, *Prime-Producing quadratic Polynomials and Real Quadratic Fields of Class Number One*. In: Number Theory (ed. J. M. Dekoninck and C. Levesque), Walter de Gruyter, Berlin, 1989, 654–663.
6. ———, *Solution of the Class Number One Problem for Real Quadratic Fields of Extended Richaud-Degert Type (with one possible exception)*. In: Number Theory (ed. R. A. Mollin), Walter de Gruyter, Berlin, New York, 1990, 417–425.
7. ———, *On a Solution of a Class Number Two Problem for a Family of Real Quadratic Fields*. In: Computational Number Theory, (ed. A. Pethö *et al.*), Walter de Gruyter, Berlin, New York, 1991, 95–101.
8. ———, *A Conjecture of S. Chowla Via the Generalized Riemann Hypothesis*, Proc. Amer. Math. Soc. **102**(1988), 794–796.
9. ———, *Computation of the Class Number of a Real Quadratic Field*, Utilitas Math. **41**(1992), 259–308.
10. ———, *On Real Quadratic Fields of Class Number Two*, Math. Comp. **59**(1992), 625–632.
11. ———, *On a Determination of Real Quadratic Fields of Class Number One and Related Continued Fraction Period Length Less Than 25*, Proc. Japan Acad. Ser. A. **67**(1991), 20–25.
12. ———, *Classification and Enumeration of Real Quadratic Fields Having Exactly One Non-Inert Prime Less Than a Minkowski Bound*, Canad. Math. Bull. **36**(1993), 108–115.
13. R. A. Mollin and A. J. van der Poorten, *A note on symmetry and Ambiguity*, Bull. Austral. Math. Soc., to appear.
14. R. A. Mollin, L.-C. Zhang and P. Kemp, *A Lower Bound For the Class Number of a Real Quadratic Field of* ERD-*type*, Canad. Math. Bull. **37**(1994), 90–96.
15. T. Tatuzawa, *On a Theorem of Siegel*, Japan J. Math. **21**(1951), 163–178.
16. H. C. Williams and M. C. Wunderlich, *On the Parallel Generation of the Residue for the Continued Fraction Factoring Algorithm*, Math. Comp. **177**(1987), 405-423.

Department of Mathematics and Statistics
University of Calgary
Calgary, Alberta
T2N 1N4
e-mail: ramollin@acs.ucalgary.ca

Computer Science Department
University of Manitoba
Winnipeg, Manitoba
R3T 2N2
e-mail: hugh_williams@csmail.cs.umanitoba.ca

https://doi.org/10.4153/CJM-1995-054-7 Published online by Cambridge University Press