Publ. Math. Debrecen
43 / 3–4 (1993), 315–328

Reduced ideals, the divisor function, continued fractions and class numbers of real quadratic fields

By R. A. MOLLIN (Calgary) and L.-C. ZHANG (Springfield)

Abstract. The aim of this paper is to give lower bounds for class numbers of real quadratic fields in terms of the divisor function, and to develop useful criteria for reduced ideals in terms of both continued fractions and the solvability of diophantine equations, which we then relate back to the aforementioned class number bounds.

§1. Introduction

The purpose of this paper is to explore the relationships between reduced ideals, continued fractions, solutions of diophantine equations, the divisor function and class number of real quadratic fields.

We set the stage by developing the machinery necessary for the rest of the paper in section 2. Section 3 deals with developing criteria for lower bounds on the *class number* $h(d)$ of real quadratic fields $Q(\sqrt{d})$. The first such result, Theorem 3.1, is a general lower bound achieved through a (combinatorial) count of certain ideals. This generalizes results of the first author in [4]–[7], of HALTER–KOCH in [1]–[2] and of MOLLIN–WILLIAMS in [10]. Thereafter we look at the consequences of Theorem 3.1 including a complete result for extended Richaud–Degert types which corrects and generalizes result in the literature.

In section 4 we explore new and old criteria for reduced ideals and develop necessary and sufficient conditions for reduced ideals to be equivalent in terms of the solvability of certain diophantine equations. This leads to a connection with the results of section 3, and we conclude with an open problem concerning that interface.

1991 *Mathematics Subject Classification*: 11R11, 11R09, 11R29.
The first author's research is supported by NSERC Canada grant # A8484.

§2. Notation and preliminaries

Throughout d will be a square-free positive integer, and $K = Q(\sqrt{d})$, the real quadratic field with *radicand* d. Let $[\alpha, \beta]$ be the $\mathbb{Z}$–module $\{\alpha x + \beta y : x, y \in \mathbb{Z}\}$. Thus the *maximal order* (or ring of integers) $\mathcal{O}_K$ of K is $[1, \omega]$ where $\omega = (\sigma - 1 + \sqrt{d})/\sigma$ with $\sigma = 2$ if $d \equiv 1 \pmod 4$, and $\sigma = 1$ otherwise. The *discriminant* of K is then $\Delta = (\omega - \bar{\omega})^2$ where $\bar{\omega}$ is the algebraic *conjugate* of ω. For $\alpha \in K$, the *norm* of α is $N(\alpha) = \alpha\bar{\alpha}$.

It is well-known (eg. see [18, §3]), that I is an ideal of $\mathcal{O}_K$ if and only if I has a representation as $I = [a, b + c\omega]$ where $a > 0$, $c > 0$, $c \mid b$, $c \mid a$ and $ac \mid N(b + c\omega)$. In fact for a given I in $\mathcal{O}_K$, the integers a and c are unique, with a being the least positive integer in I, denoted $L(I) = a$. If $c = 1$ then I is called *primitive*, and in this case $a = L(I) = N(I) =$ *norm of* I. Furthermore, since $I = (c)[a/c, b/c + \omega]$, (where (c) denotes the *principal ideal* generated by c), then we shall restrict our attention to primitive ideals henceforth. Note furthermore that the *conjugate ideal* $\bar{I} = [a, b + \bar{\omega}]$.

An ideal I is called *reduced* if I is primitive and there does *not* exist a non-zero $\alpha \in I$ with *both* $|\alpha| < N(I)$ *and* $|\bar{\alpha}| < N(I)$.

Theorem 2.1. *I is a reduced ideal in $\mathcal{O}_K$ if and only if there exists some $\beta \in I$ such that $I = [N(I), \beta]$ with $\beta > N(I)$, and $-N(I) < \bar{\beta} < 0$.*

Proof. This is Theorem 3.5 of [18]. □

We will use Theorem 2.1 in section 4 to find some more useful criteria for reduced ideals. Now we discuss the *continued fraction expansion* of ω which we will need throughout the paper. We denote this expansion by

$$\omega = \langle a, \overline{a_1, a_2, \ldots, a_k} \rangle \quad \text{of}$$

period lenght k, where $a = a_0 = \lfloor \omega \rfloor$, (here $\lfloor\ \rfloor$ denotes the greatest integer function), $a_i = \lfloor (P_i + \sqrt{d})/Q_i \rfloor$ for $i \geq 1$ with $(P_0, Q_0) = (\sigma - 1, \sigma)$ and recursively for $i \geq 0$ we have $P_{i+1} = a_i Q_i - P_i$ and $Q_{i+1} Q_i = d - P_{i+1}^2$.

For further details on reduced ideals and continued fractions the reader is referred to [11], [17] and [18].

§3. The divisor function

In this section we develop several criteria for the class number of K to be bounded below by the divisor function of a certain canonical integer. The following extends and generalizes work of Halter–Koch in [1]–[2], and continues work of Mollin in [4]–[7] as well as that of Mollin–Williems in [10]. Our first result is quite general and so has a high degree of applicability as we shall see.

In what follows $\tau(x)$ denotes the number of positive divisors of $x \in \mathbb{N}$.

Theorem 3.1. *Let $A > 0$ be the norm of a primitive principal ideal in $\mathcal{O}_K$ and $A < \sqrt{\Delta}$. Assume furthermore that no divisor m of A with $1 < m < A$ is the norm of a principal reduced ideal in $\mathcal{O}_K$. Thus, $h(d) \geq \tau(A) - 2^{s-1}$ where s is the number of* distinct *prime divisors of A.*

Proof. Let $A = \prod_{i=1}^{s} P_i^{e_i}$ be the prime factorization of A and let $N(\mathcal{A}) = A$ where $1 \sim \mathcal{A} = \prod_{i=1}^{s} \mathcal{P}_i^{e_i}$ where $\mathcal{P}_i$ sits above p_i for each i. We now fix these ideals $\mathcal{P}_i$, (since we observe that we are not, in general, allowed a choice of either $\mathcal{P}_i$ or $\bar{\mathcal{P}}_i$).

Assume

$$(*) \qquad 1 \neq \prod_{i=1}^{s} \mathcal{P}_i^{f_i} \sim \prod_{i=1}^{s} \mathcal{P}_i^{g_i} \neq 1$$

where $0 \leq f_i\,;\, g_i \leq e_i$ and let $\mathcal{I}_0$ be the set of all indices in $\mathcal{I}=\{1, 2, 3, \ldots, s\}$ such that p_i is unramified for all $i \in \mathcal{I}_0$, and let $\mathcal{I}_1$ and $\mathcal{I}_2$ be subsets of $\mathcal{I}_0$ such that $f_i \geq g_i$ for all $i \in \mathcal{I}_1$ whereas $f_i < g_i$ for all $i \in \mathcal{I}_2$. Also let $\mathcal{I}_3 \subseteq \mathcal{I}$ be all those indices i such that p_i is ramified and $f_i \neq g_i$. Thus $(*)$ becomes

$$(**) \qquad 1 \sim \prod_{i\in\mathcal{I}} \mathcal{P}_i^{f_i-g_i} \sim \prod_{i\in\mathcal{I}_i} \mathcal{P}_i^{f_i-g_i} \prod_{i\in\mathcal{I}_2} \bar{\mathcal{P}}_i^{g_i-f_i} \prod_{i\in\mathcal{I}_3} \mathcal{P}_i = I$$

If $m = N(I) > \sqrt{\Delta}/2$ then since m divides $A < \sqrt{\Delta}$ then $m = A$ is forced; whence, we must have $f_i = e_i$ and $g_i = 0$ for all $i \in \mathcal{I}_1, g_i = e_i$ and $f_i = 0$ for all $i \in \mathcal{I}_2$, and $\mathcal{I}_3 = \mathcal{I} - \mathcal{I}_0$, where $e_i = 1$ for all $i \in \mathcal{I}_3$. Hence $(**)$ becomes

$$1 \sim \prod_{i\in\mathcal{I}_1} \mathcal{P}_i^{e_i} \prod_{i\in\mathcal{I}_2} \bar{\mathcal{P}}_i^{e_i} \prod_{i\in\mathcal{I}_3} \mathcal{P}_i$$

or equivalently, (since $\mathcal{P}_i = \bar{\mathcal{P}}_i$ for all $i \in \mathcal{I}_3$),

$$(***) \qquad \prod_{i\in\mathcal{I}_2} \mathcal{P}_i^{e_i} \prod_{i\in\mathcal{I}_3} \mathcal{P}_i \sim \prod_{i\in\mathcal{I}_1} \mathcal{P}_i^{e_i}$$

The number of distinct possible such equivalences in $(***)$ is clearly 2^{s-1}.

Now assume $m < \sqrt{\Delta}/2$; whence, I is a principal reduced ideal whose norm divides A. By hypothesis $m = 1$ or A. If $m = A$ then we proceed as above. If $m = 1$ then $f_i = g_i$ for all $i = \mathcal{I}$, which secures the result. □

Corollary 3.1. *With the hypothesis as in the statement of Theorem 3.1, if $s > 1$ then $h(d) > 1$.*

PROOF. $\tau(A) = \prod_{i=1}^{s}(e_i + 1) \geq 2^s$; whence, $h(d) \geq \tau(A) - 2^{s-1} \geq 2^s - 2^{s-1} = 2^{s-1} > 1$. □

Remark 3.1. There are several palatable consequences of Theorem 3.1 not the least of which is the following application which corrects Theorems 2.1–2.2 of [4]. Although we gave what we called corrected versions of the latter in [5]–[7], the assumptions used in Theorem 2.1 of [6] and Theorems 1–3 of [7] were very strong, whereas those of Theorem 3.1 above are minimal and maintain the intention of [4] to get a very general lower bound for $h(d)$ in terms of the divisor function. To see that our bound in the above is in fact sharp, we cite the following example which also has two other purposes: to give a counterexample to Theorem 2.2 of [4] and to motivate the next result which explicitly corrects [4].

Example 3.1. Let $d = 385 = 20^2 - 15 = 5 \cdot 7 \cdot 11$. Consider the continued fraction expansion of $(1 + \sqrt{d})/2$:

i	0	1	2	3	4	5	6	7
P_i	1	19	17	15	5	13	11	11
Q_i	2	12	8	20	18	12	22	⋮
a_i	10	3	4	1	1	2	1	⋮

Hence the hypothesis of Theorem 3.1 is satisfied for $A = 6$. Here $h(d) = 2 = \tau(A) - 2^{s-1}$.

Corollary 3.2. *Let $d = b^2 + r$ with $|r| < 2b$ and set*

$$A = \left\{ \begin{array}{ll} 2b/\sigma - |r/\sigma^2 - 1| & \text{if } r \text{ is even} \\ (2b - |r-1|)/\sigma^2 & \text{if } r \text{ is odd} \end{array} \right\}.$$

Assume that no divisor m of A with $1 < m < A$ is the norm of a principal reduced ideal. Thus $h(d) \geq \tau(A) - 2^{s-1}$ where s is the number of distinct prime divisors of A.

PROOF. By Theorem 3.1 we need only show that $A < \sqrt{\Delta}$ and that A is the norm of a primitive principal ideal.

If $r > 0$ is even then
$A = 2b/\sigma - (r/\sigma^2 - 1) \leq 2b/\sigma < \sqrt{\Delta}$.

If $r < 0$ is even then
$A = 2b/\sigma + r/\sigma^2 - 1 \leq 2(b-1)/\sigma < \sqrt{\Delta}$.

If $r > 0$ is odd then
$A = (2b - (r-1))/\sigma^2 \le 2b/\sigma^2 < \sqrt{\Delta}$, and if $r < 0$ is odd then
$A = (2b + r - 1)/\sigma^2 \le 2(b-1)/\sigma^2 < \sqrt{\Delta}$.

Finally, we have

$$\sigma^2 \alpha A = \begin{cases} (b + \alpha\sigma)^2 - d & \text{if } r \text{ is even} \\ (b+\alpha)^2 - d & \text{if } r \text{ is odd} \end{cases}, \text{ where } \alpha = \left\{ \begin{array}{r} -1 \text{ if } r < 0 \\ 1 \text{ if } r > 0 \end{array} \right\}. \quad \square$$

Remark 3.2. Although Theorems 2.1–2.2 of [4] are false as they stand, and although Corollary 3.2 gives the (intended) correct version, Applications I–II of [4] *are* correct since they refer to ERD–types; (i.e., extended Richaud–Degert types: $d = b^2 + r$ where $4b \equiv 0 \pmod{r}$). It turns out that the assumption of Corollary 3.2 holds for ERD–types; i.e., we have

Corollary 3.3. *If d, A and s are as in Corollary 3.2 and d is of ERD–type then*

$$h(d) \ge \tau(A) - 2^{s-1}.$$

Proof. In view of Theorem 1.1 of [10] we need only check the continued fraction expansion of ω for each case. In what follows $\mathcal{A} \sim 1$ with $N(\mathcal{A}) = A$.

Case 1. $d \not\equiv 1 \pmod 4$.

(a) $r > 0$.

i	0	1	2
P_i	0	b	b
Q_i	1	r	1
a_i	b	$2b/r$	$2b$

Here $A = 2b - r + 1 > \sqrt{\Delta}/2$ and $\mathcal{A}$ is not reduced.

(b) $r < 0$.

i	0	1	2	3
P_i	0	$b-1$	$b+r$	$b+r$
Q_i	1	$2b+r-1$	$-r$	$\vdots$
a_i	$b-1$	1	$-2(b+r)/r$	$\vdots$

Here $A = 2b + r - 1$ and $\mathcal{A}$ *is* reduced.

Case 2. $d \equiv 1 \pmod 4$.

(a) $r > 0$, even.

i	0	1	2
P_i	1	b	b
Q_i	2	$r/2$	2
a_i	$(b+1)/2$	$4b/r$	b

Here $A = b - r/4 + 1 > \sqrt{\Delta}/2$ and $\mathcal{A}$ is not reduced.

(b) $r > 0$, odd.

i	0	1	2	3	4
P_i	1	$b-1$	$(r+1)/2$	$b-r$	$b-r$
Q_i	2	$b+(r-1)/2$	$b-(r-1)/2$	$2r$	$\vdots$
a_i	$b/2$	1	1	$b/r-1$	$\vdots$

Here $A = (2b-(r-1))/4$ and $\mathcal{A}$ *is* reduced.

(c) $r < 0, r$ even.

i	0	1	2	3
P_i	1	$b-2$	$b+r/2$	$b+r/2$
Q_i	2	$2b+r/2-2$	$-r/2$	$\vdots$
a_i	$(b-1)/2$	1	$-4b/r-2$	$\vdots$

Here $A = b + r/4 - 1$ and $\mathcal{A}$ is reduced.

(d) $r < 0$, odd.

i	0	1	2	3
P_i	1	$b-1$	$b+r$	$b+r$
Q_i	2	$b+(r-1)/2$	$-2r$	$\vdots$
a_i	$b/2$	2	$-b/r-1$	$\vdots$

Here $A = (2b+r-1)/4$ and $\mathcal{A}$ is reduced.

In each and every one of the above cases we see that there is no divisor m of A with $1 < m < A$ such that m is the norm of a principal reduced ideal. $\square$

Remark 3.3. The choice of A in Corollaries 3.2–3.3 is no accident. It is in fact a very natural one as the following elucidation will show.

Definition 3.1. If $I = [a, (c + \sqrt{\Delta})/2]$ is a primitive ideal then the *Lagrange neighbour* $I^+ = [a^+, (c^+ + \sqrt{\Delta})/2]$ is defined by $c^+ = -c + 2a\lfloor (c + \sqrt{\Delta})/2a \rfloor$ and $a^+ = (\Delta - (c^+)^2)/4a$. In fact $I \sim I^+$ and if I is reduced then so is I^+.

Remark 3.4. Now consider the A in Corollaries 3.2–3.3. If r is even then

$$I = [2b/\sigma - |r/\sigma^2 - 1|,\ (b + \alpha\sigma + \sqrt{d})/\sigma] \text{ and } I^+ = [|r|/\sigma^2,\ (b - |r| + \sqrt{d})/\sigma]\,.$$

If r is odd then

$$I = [(2b - |r - 1|)/\sigma^2,\ (b + \alpha + \sqrt{d}\,)/\sigma]$$

and

$$I^+ = [|r|,\ (b - |r| + \sqrt{d}\,)/\sigma]\,.$$

In the case where d is an ERD–type then, as seen in the proof of Corollary 3.3, when I is reduced then I and I^+ are the *only* reduced principal ideals (other than I), except when $r > 0$ is odd and $d \equiv 1 \pmod 4$ in which case we have the additional reduced ideal of norm $(2b + (r - 1))/4$. This is why the hypothesis of Corollary 3.2 is satisfied for ERD–types.

The following illustrates Corollaries 3.2–3.3.

Example 3.2.

(i) Let $d = 777 = 3 \cdot 7 \cdot 37 = 28^2 - 7$. Here $A = 12$ and $h(d) = 4 = \tau(A) - 2$

(ii) If $d = 5482 = 74^2 + 6$ then $A = 143 = 11 \cdot 13$. Here the period length of $\sqrt{d}$ is 53 and neither 11 nor 13 appears as a Q_i therein. We have $h(d) = 2 = \tau(A) - 2$.

(iii) If $d = 21037 = 145^2 + 12$ then $A = 143$ and the period length of $(1 + \sqrt{d})/2$ is 31 with neither 11 nor 13 appearing as a $Q_i/2$ therein. Here $h(d) = 2 = \tau(A) - 2$.

It is conceivable that we could construct infinitely many such d's with $h(d) = 2$ and A a product of 2 primes. In Example 3.1, $d = 385$ is also of this type and $A = (2b - |r - 1|)/\sigma^2$ which along with Examples (i)–(iii) above are the forms in Theorems 2.1–2.2 of [4]. The reason that Examples 3.1–3.2 are counterexamples to the latter is that the assumptions in Theorems 2.1–2.2 of [4] are too weak by taking into account only relationships

generated by the ramified primes (in $(***)$ of the proof of Theorem 3.1). Thus the latter fail to hold whenever there is a non-principal ambiguous ideal with norm dividing A, as is the case with the above 3 examples. Observe that, for example, if $d = 385$ then the ideal above 2 generates the class group, is non-principal, ambiguous and divides A. This motivates the next result ensuing from Theorem 3.1.

Theorem 3.2. *Let $A > 0$ be the norm of a primitive principal ideal and assume that no divisor m of $A < \sqrt{\Delta}$ with $1 < m < A$ is the norm of a reduced ideal which is in an ambiguous class (including the principal class). Thus,*

$$h(d) \geq \tau(A) - 2^n$$

where n is the number of distinct primes dividing A, which ramify *in K.*

Proof. We proceed as in the proof of Theorem 3.1 and we get $(***)$ which implies

$$\prod_{i\in\mathcal{I}_1} \mathcal{P}_i^{e_i} \prod_{i\in\mathcal{I}_2} \bar{\mathcal{P}}_i^{e_i} \prod_{i\in\mathcal{I}_3} \mathcal{P}_i \sim 1 \sim \prod_{i\in\mathcal{I}_1} \mathcal{P}_i^{e_i} \prod_{i\in\mathcal{I}_2} \mathcal{P}_i^{e_i} \prod_{i\in\mathcal{I}_3} \mathcal{P}_i$$

which in turn implies that $\prod\limits_{i\in\mathcal{I}_2} \mathcal{P}_i^{2e_i} \sim 1$. Therefore $J = \prod\limits_{i\in\mathcal{I}_2} \mathcal{P}_i^{e_i}$ is an ambiguous ideal and $N(J)$ divides A. If $N(J) > \sqrt{\Delta}/2$ then since $N(J)$ divides $A < \sqrt{\Delta}$ we must have $N(J) = A$. Thus $\mathcal{I}_1 = \emptyset = \mathcal{I}_3$ which means $f_i = 0$ for all $i \in \mathcal{I}$, contradicting the non-triviality of $\prod\limits_{i=1}^{s} \mathcal{P}_i^{f_i}$.

If $N(J) < \sqrt{\Delta}/2$ then by hypothesis $N(J) = 1$ or A. If $N(J) = A$ then we have a contradiction as above. If $N(J) = 1$ then $\mathcal{I}_2 = \emptyset$ and so $(***)$ generates only the relationships

$$\prod_{i\in\mathcal{I}-\mathcal{I}_0} \mathcal{P}_i \sim \prod_{i\in\mathcal{I}_0} \mathcal{P}_i^{e_i}\,.$$

There are 2^n such relationships. □

Example 3.3. If $d = 145 = 5 \cdot 29$ and $A = 6$ then neither 2 nor 3 is the norm of an ideal in an ambiguous class because $C_K = \langle \mathcal{P}_2 \rangle = \langle \mathcal{P}_3 \rangle$ where $\mathcal{P}_2 \mid 2$ and $\mathcal{P}_3 \mid 3$. Moreover neither $\mathcal{P}_2^2 \sim 1$ nor $P_3^2 \sim 1$. In fact $h(d) = 4 > \tau(A) - 1 = 3$. Theorem 3.2 has, however, such a strong hypothesis that it cannot give any information if the class group has exponent 2 because in such a case, if m divides A and $1 < m < A$ then m is *necessarily* a norm of an ambiguous reduced ideal. However ERD–types satisfy the conclusion of Theorem 3.2 *without* the restriction on ambiguous ideals.

Theorem 3.3. *If $= b^2 + r$ is of ERD–type and A is as in Corollary 3.2 then*

$$h(d) \geq \tau(A) - 2^n$$

where n is the number of ramified prime divisors of A.

PROOF. We proceed exactly as in the proof of Theorem 3.2 except that when $N(J) < \sqrt{\Delta}/2$ we do not invoke the hypothesis of Theorem 3.2, but rather we observe that from the analysis in the proof of Corollary 3.3, for each ERD case we must have $N(J) = 1$ or A. □

Remark 3.5. Theorem 3.3 shows that Theorems 2.1–2.2 of [4] are correct for ERD–types and it was this fact that led to the more general albeit incorrect versions given (without proof) in [4].

Remark 3.6. For narrow RD–types (i.e., those $d = b^2 + r$ with $|r| = 1$ or 4), there are much stronger bounds as given in [5]. These much stronger bounds come from Lemma 1.1 of [8] which only has real substance *for* the narrow RD–types. It does point to more general relevance via the following result which we proved in [6].

In what follows an element $\alpha \in \mathcal{O}_K$ is said to be primitive if $(\alpha) \neq 1$ is not divisible by any rational ideal except (1); i.e., $\alpha = (x + y\sqrt{d})/\sigma$ satisfies $\gcd(x, y)$ divides σ.

Proposition 3.1. *If $A > 0$ is any real number then the following are equivalent*

(1) $|x^2 - dy^2| = \sigma^2 m$ *for* $1 < m < A$ *implies that* $m = t^2$ *with* $\gcd(x, y) = t$.
(2) $|N(\alpha)| \geq A$ *for all primitive* $\alpha \in \mathcal{O}_K$.

Remark. It turns out that for narrow RD–types, the A given in Corollary 3.2 satisfies Proposition 3.1. In fact for narrow RD–types this A is exactly $B = (2t_d/\sigma - N(\epsilon_d) - 1)/{u_d}^2$ where $\epsilon_d = (t_d + u_d\sqrt{d})/\sigma$ is the fundamental unit of K. It is clear that this bound will not be very useful as the fundamental unit becomes "large". In [12]–[13] we explored this bound further to completely solve a problem of H. YOKOI involving certain real quadratic fields of class number 1 (which it turns out includes all of the ERD–types). Furthermore, as we proved in [14]; if $h(d) = 1$ then p is inert in K for all primes $p < B$. For narrow RD–types this means p is inert for all primes $p < \sqrt{\Delta}/2$. In [14] we proved that the latter condition can *only* hold for narrow RD–types. In [15] we showed that p is inert for all primes p with $2 < p < \sqrt{\Delta}/2$ if and only if $h(d) = 1$ and $d = b^2 \pm 2$. There are conjectures which remain open (as given in [9]) pertaining to the exact list of such d's with $h(d) = 1$. In [15] we completely classified those d's such that there is *exactly* one non-inert prime $p < \sqrt{\Delta}/2$. In [3]

we classified those d's for which there are no *split* primes $p < \sqrt{\Delta}/2$. In the latter case the the d's are forced to be of ERD–type, but not in the former case. In just completed work the authors of [3] have classified and listed all ERD–types with class groups of exponent 2. Previously in [16] we solved the class number 1 problem for ERD–types (with one possible exceptional value remaining whose existence would be a counterexample to the Riemann hypothesis).

§4. Reduced ideals

In this section we develop criteria for ideals to be reduced in a way heretofore not exploited in the literature. Moreover we then establish necessary and sufficient conditions for two reduced ideals to be equivalent in terms of the solution of certain diophantine equations. We then link the latter to the results of section 3, and conclude with an open problem.

Theorem 4.1. *Let $I = [a, c+\omega]$ be a primitive ideal in $\mathcal{O}_K$, then I is reduced if and only if $\lfloor -(c+\bar{\omega})/a \rfloor a > a - c - \omega$.*

Proof. If I is reduced then by Theorem 2.1 there is a $\beta \in I$ with $I = [a, \beta]$ and both $\beta > a$ and $-a < \bar{\beta} < 0$. From the definition of equality for ideals (see [18, §3, p.410]), we have that $\beta = ta + c + \omega$ for some rational integer t; whence,

$$ta + c + \omega > a \tag{1}$$

and

$$-a < ta + c + \bar{\omega} < 0\,. \tag{2}$$

From (2) we get that $-(c+\bar{\omega})/a - 1 < t < -(c+\bar{\omega})/a$; whence, $t = \lfloor -(c+\bar{\omega})/a \rfloor$. From (1) then

$$\lfloor -(c+\bar{\omega})/a \rfloor a > a - c - \omega\,. \tag{3}$$

Conversely assume that (3) holds and set $\beta = \lfloor -(c+\bar{\omega})/a \rfloor a + c + \omega \in I$; whence, $I = [a, \beta]$. Since (3) implies that $\beta > a - c - \omega + c + \omega = a$, and $0 = (-(c+\bar{\omega})/a)a + c + \bar{\omega} > \bar{\beta} > (-(c+\bar{\omega})/a - 1)a + c + \bar{\omega} = -a$ then by Theorem 2.1 I is reduced. □

As applications of Theorem 4.1 we easily achieve the well-known results [18, Corollary 3.5.1, and Theorem 3.6, p.412] as follows.

Corollary 4.1. *If $I = [a, c+\omega]$ is reduced then $a < \sqrt{\Delta}$.*

Proof. By Theorem 4.1 we achieve $-c - \bar{\omega} = (-(c+\bar{\omega})/a) > \lfloor -(c+\bar{\omega})/a \rfloor a > a - c - \omega$; whence, $a < \omega - \bar{\omega} = \sqrt{\Delta}$. □

Corollary 4.2. *If $I = [a, c+\omega]$ is a primitive ideal with $a < \sqrt{\Delta}/2$ then I is reduced.*

PROOF. We have that

$$\lfloor -(c+\bar{\omega})/a \rfloor a > (-(c+\bar{\omega})/a - 1)a = -c - \bar{\omega} - a = \\ = (a - c - \omega) + (\omega - \bar{\omega} - 2a) > a - c - \omega\,,$$

where the latter inequality holds because $\omega - \bar{\omega} - 2a = \sqrt{\Delta} - 2a > 0$. □

The following is not well-known and is valuable since it is often difficult to determine when primitive ideals with norms between $\sqrt{\Delta}$ and $\sqrt{\Delta}/2$ are reduced.

Corollary 4.3. *Let $I = [a, c+\omega]$ be a primitive ideal with $0 \le c < a$ and $\sqrt{\Delta}/2 \le a < \sqrt{\Delta}$. Then I is reduced if and only if $a - \omega < c < -\bar{\omega}$.*

PROOF. If I is reduced then Theorem 4.1 implies $\lfloor -(c+\bar{\omega})/a \rfloor a > a - c - \omega$.

Claim 1. $\lfloor -(c+\bar{\omega})/a \rfloor \ge 0$.

If $\lfloor -(c+\bar{\omega})/a \rfloor \le -1$ then $-a > a - c - \omega$; whence, $\omega - a > a - c > \sqrt{\Delta}/2 - c$; i.e., $\omega + c > a + \sqrt{\Delta}/2$. If $d \not\equiv 1 \pmod 4$ this says $c > a$, a contradiction. If $d \equiv 1 \pmod 4$ this says that $(1+\sqrt{d})/2 + c > a + \sqrt{d}/2$; i.e., $c + 1/2 > a$, again a contradiction. Claim 1 then implies that $-c - \bar{\omega} > 0$; i.e., $c < -\bar{\omega}$.

Claim 2. $-(c+\bar{\omega})/a < 1$.

Since $a + c + \bar{\omega} \ge a + \bar{\omega} > \sqrt{\Delta}/2 + \bar{\omega} > 0$ then the result follows.

Claims 1 and 2 imply that $\lfloor -(c+\bar{\omega})/a \rfloor = 0$. By (3) we get $0 > a - c - \omega$; i.e., $c > a - \omega$.

Conversely assume that $a - \omega < c < -\bar{\omega}$. Thus, $0 < -(c+\bar{\omega})/a < 1$; whence, $\lfloor -(c+\bar{\omega})/a \rfloor = 0 > a - c - \omega$. Theorem 4.1 now says that I is reduced. □

Now we develop necessary and sufficient conditions for two reduced ideals to be equivalent in terms of the solutions of certain diophantine equations.

Theorem 4.2. *Let $I_i = [a_i, c_i + \omega]$ for $i = 1, 2$ be primitive ideals in $\mathcal{O}_K$. Thus $I_1 \sim I_2$ if and only if there are coprime integers x and y satisfying the following three conditions.*

(1) $(\sigma a_1 x + (\sigma c_1 + \sigma - 1)y)^2 - dy^2 = \pm\sigma^2 a_1 a_2$.
(2) $a_2 \mid a_1 x + (c_1 + c_2 + \sigma - 1)y$.
(3) $\sigma^2 a_1 a_2 \mid \sigma^2 a_1 (c_2 - c_1)x + (d - (\sigma c_1 + \sigma - 1)^2)y$.

PROOF. We will only address the case where $d \not\equiv 1 \pmod 4$ since similar arguments apply in the remaining cases.

$I_1 \sim I_2$ if and only if there exists a $\gamma = a_1x + (c_1 + \omega)y \in I_1$ such that

$$(\gamma)I_2 = (a_2)I_1; \quad \text{i.e.}$$
$$a_1a_2x + a_2c_1y + a_2y\omega,\ a_1c_2x + c_1c_2y + dy + (a_1x + (c_1 + c_2)y)\omega]$$
$$= [a_1a_2,\ a_2c_1 + a_2\omega]; \quad \text{i.e., there exists an}$$
$$M = \begin{pmatrix} c_{11} & c_{12} \\ c_{21} & c_{22} \end{pmatrix} \in SL_2(\mathbb{Z})$$

such that

$$\begin{pmatrix} c_{11} & c_{12} \\ c_{21} & c_{22} \end{pmatrix} \begin{pmatrix} a_1 & a_2 & 0 \\ a_2 & c_1 & a_2 \end{pmatrix} = \begin{pmatrix} a_1a_2x + a_2c_2y & a_2y \\ a_1c_2x + c_1c_2y + dy & a_1x + (c_1 + c_2)y \end{pmatrix}.$$

It is clear that

i) $a_1a_2c_{11} + a_2c_1c_{12} = a_1a_2x + a_2c_2y$,
ii) $a_2c_{12} = a_2y$,
iii) $a_1a_2c_{21} + a_2c_1c_{22} = a_1c_2x + c_1c_2y + dy$,
iv) $c_{22}a_2 = a_1x + (c_1 + c_2)y$,

and

v) $c_{11}c_{22} - c_{12}c_{21} = \pm 1$.

By ii) and i), we see that $c_{12} = y$ and $c_{11} = x$.

From iv) $$c_{22} = \frac{a_1x + (c_1 + c_2)y}{a_2} \in \mathbb{Z}\,.$$

By iii) and iv), we find that

$$c_{21} = \frac{a_1(c_2 - c_1)x - (d - c_1^2)y}{a_1a_2} \in \mathbb{Z}\,.$$

Substitutions for $c_{11}, c_{12}, c_{21}, c_{22}$ in v) give

$$(a_1x + c_1y)^2 - dy^2 = \pm a_1a_2, \text{ and}$$
$$(x, y) = 1\,. \qquad \square$$

Corollary 4.4. *With the hypothesis as in Theorem 4.2 any prime $p \mid d$ with $p \equiv 1 \pmod 4$ satisfies $(a_1a_2/p) = 1$.*

Proof. From the conclusion of Theorem 4.2 we have $((\pm\sigma^2 a_1a_2)/p) = 1$. Since $p \equiv 1 \pmod 4$ the result follows. $\square$

Corollary 4.5. *Let Q_i for $0 < i < k$ be those appearing in the continued fraction expansion of ω; then for any $p \mid d$ with $p \equiv 1 \pmod 4$ we must have $((Q_i/\sigma)/p) = 1$.*

PROOF. Since $[Q_i/\sigma,\ (P_i - (\sigma - 1))/\sigma + \omega] \sim [1, \omega]$ then by Corollary 4.4 the result follows. □

Now we link the above with the results of the previous section.

Remark. Let $d = b^2 + r$ with $|r| < 2b$ and

$$A = \left\{ \begin{array}{ll} 2b/\sigma - |r/\sigma^2 - 1| & \text{if } r \text{ is even} \\ (2b - |r-1|)/\sigma^2 & \text{if } r \text{ is odd} \end{array} \right\}.$$

If a_i denotes a divisor of A then

$$I_i = \left\{ \begin{array}{ll} [a_i,\ (b + \alpha\sigma + \sqrt{d})/\sigma], & r \text{ even} \\ [a_i,\ (b + \alpha + \sqrt{d})/\sigma], & r \text{ odd} \end{array} \right.$$

where $\alpha = \left\{ \begin{array}{ll} 1 & \text{if } r > 0 \\ -1 & \text{if } r < 0 \end{array} \right\}$ is reduced.

The results of section 3 tell us that, for example, when d is of ERD–type $I_i \not\sim I_j$ for any divisors of A unless $a_i a_j = A$. Thus the conditions of Theorem 4.2 cannot hold unless $a_1 a_2 = A$. It would be valuable to find a direct proof of this fact. We have not been able to do so, and we leave it is an interesting open problem. Moreover it would be valuable to investigate this question for non–ERD–types.

References

[1] F. HALTER-KOCH, Quadratische Ordnungen mit Grosser Klassenzahl, *J. Number Theory* **34** (1990), 82–94.

[2] F. HALTER-KOCH, Quadratische Ordnungen mit Grosser Klassenzahl II, *J. Number Theory*, (*to appear*).

[3] S. LOUBOUTIN, R. A. MOLLIN and H. C. WILLIAMS, Class numbers of real quadratic fields, continued fractions, reduced ideals, prime-producing quadratic polynomials, and quadratic residue covers, *Canad. J. Math.* **44** (1992), 824–842.

[4] R. A. MOLLIN, Class numbers bounded below by the divisor function, *C. R. Math. Rep. Acad. Sci. Canada* **12** (1990), 119–124.

[5] R. A. MOLLIN, On the divisor function and class numbers of real quadratic fields I, *Proc. Japan Acad.* **66A** (1990), 109–111.

[6] R. A. MOLLIN, On the divisor function and class numbers of real quadratic fields II, *Proc. Japan Acad.* **66A** (1990), 274–277.

[7] R. A. MOLLIN, On the divisor function and class numbers of real quadratic fields IV, *Proc. Japan Acad.* **68A** (1992), 15–17.

[8] R. A. MOLLIN, On the onsolubility 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.

[9] R. A. MOLLIN, Powers in continued fractions and class numbers of real quadratic fields, *Utilitas Math.* **42** (1992), 25–30.
[10] R. A. MOLLIN and H. C. WILLIAMS, On the divisor function and class numbers of real quadratic fields III, *Proc. Japan Acad.* **67A** (1991), 338–342.
[11] R. A. MOLLIN and H. C. WILLIAMS, Computation of the class number of a real quadratic fields, *Utilitas Math.* (1992), 259–308.
[12] R. A. MOLLIN and H. C. WILLIAMS, Solution of a problem of Yokoi, *Proc. Japan Acad.* **66A** (1990), 141–145.
[13] R. A. MOLLIN and H. C. WILLIAMS, A complete generalization of Yokoi's p-invariants, *Colloquium Math.* **LXIII** (1992), 285–294.
[14] R. A. MOLLIN and H. C. WILLIAMS, On prime-valued polynomials and class numbers of real quadratic fields, *Nagoya Math. J.* **112** (1988), 143–151.
[15] R. A. MOLLIN and H. C. WILLIAMS, Classification and enumeration of real quadratic fields having exactly one non-inert prime less than a Minkowski bound, *Canad. Math. Bull.*, (*to appear*).
[16] R. A. MOLLIN and H. C. WILLIAMS, Solution of the class number one problem for real quadratic fields of extended Richaud-Degert type (with one possible exception, in Number Theory (R. A. Mollin ed.), *Walter de Gruyter*, *New York*, 1990, pp. 417–425.
[17] H. C. WILLIAMS, Continued fractions and number theoretic computations, *Rocky Mountain J. Math.* **15** (1985), 621–655.
[18] H. C. WILLIAMS and M. C. WUNDERLICH, On the parallel generation of the residues for the continued fraction factoring algorithm, *Math. Comp.* **177** (1987), 405–423.

R. A. MOLLIN
MATHEMATICS DEPT.
UNIVERSITY OF CALGARY
CALGARY, ALTA
T2N, 1N4, CANADA

L.–C. ZHANG
MATHEMATICS DEPT.
SOUTWEST MISSOURI STATE UNIVERSITY
901 SOUTH NATIONAL AVE.
SPRINGFIELD, MISSOURI, 65804
USA

(Received April 6, 1992)