84. On the Divisor Function and Class Numbers of Real Quadratic Fields. III

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

(Communicated by Shokichi IYANAGA, M. J. A., Dec. 12, 1991)

Abstract: Using the techniques which we developed concerning the interrelationships between reduced ideals and continued fractions we prove a general result which gives bounds from below for the class number $h(d)$ of a real quadratic field $Q(\sqrt{d})$. The proofs are combinatorial in nature. Applications are given as well.

§1. **Notation and preliminaries.** Throughout d will be a positive square-free integer. Let $\omega_d=(\sigma-1+\sqrt{d})/\sigma$ where $\sigma=2$ if $d\equiv 1 \pmod 4$ and $\sigma=1$ if $d\equiv 2, 3 \pmod 4$. Let $[\alpha, \beta]$ be the module $\{\alpha x+\beta y: x, y \in Z\}$ and note that the maximal order (ring of integers) $\mathcal{O}_K$ of $K=Q(\sqrt{d})$ is $[1, \omega_d]$. The discriminant Δ of K is $(\omega_d-\bar{\omega}_d)^2=4d/\sigma^2$, and the absolute norm of α is $N(\alpha)=\alpha\bar{\alpha}$ where $\bar{x}$ is the algebraic conjugate of x.

A non-zero ideal of $\mathcal{O}_K$ can be written as $I=[a, b+c\omega_d]$ where $a, b, c \in Z$, $a>0$, $c|b$, $c|a$ and $ac|N(b+c\omega_d)$. Here a and $|c|$ are unique and a is the least positive integer in I, denoted $L(I)=a$. Also the norm of $I=N(I)=|c|a$. The ideal conjugate to I, denoted $\bar{I}$ is given by $\bar{I}=[a, b+c\bar{\omega}_d]$. If $I=(\alpha)$ is principal then $N(I)=|N(\alpha)|$. If $I\sim J$ (where $\sim$ denotes equivalence of ideals in the class group C_K of K) then there is a $\gamma\in I$ such that $(\gamma)J=(L(J))I$.

An ideal is called *primitive* if $L(I)=N(I)$; i.e., $|c|=1$. (Henceforth we shall consider only primitive ideals.) I is called *reduced* if I is primitive and there does not exist a non-zero $\alpha\in I$ such that both $|\alpha|<L(I)$ and $|\bar{\alpha}|<L(I)$. A more illuminating geometrical interpretation of this is to consider the lattice of the ideal I, (i.e., points $(\alpha, \bar{\alpha})$) for all $\alpha \in I$, and look at the square centered at the origin with vertices (a, a), $(-a, a)$, $(-a, -a)$ and $(a, -a)$, where $a=N(I)$. Then if the only element of the ideal to be found inside this square is the zero element, we say that I is reduced.

Now we look at the connection between reduced ideals and continued fractions which will be central to our results contained herein.

If $I=[N(I), b+\omega_d]$ is primitive then the expansion of $(b+\omega_d)/N(I)$ as a continued fraction proceeds as follows. $(P_0, Q_0)=(\sigma b+\sigma-1, \sigma N(I))$, $a_0=\lfloor (P_0+\sqrt{d})/Q_0 \rfloor$, (where $\lfloor\ \rfloor$ denotes the greatest integer function), and re-

*) Department of Mathematics and Statistics, University of Calgary, Calgary, Alberta, T2N 1N4, Canada.

**) Computer Science Department, University of Manitoba, Winnipeg, Manitoba, R3T 2N2, Canada.

cursively for $i\geq 0$;

$$P_{i+1}=a_iQ_i-P_i,\ Q_{i+1}=(d-P_{i+1})^2/Q_i, \quad\text{and}\quad a_{i+1}=\lfloor(P_{i+1}+\sqrt{d})/Q_{i+1}\rfloor.$$

Thus, if I is a reduced ideal then the continued fraction expansion of $(b+\omega_d)/N(I)$ is $\langle a_0, \overline{a_1, a_2, \cdots, a_k}\rangle$ of period length k. Moreover as developed in [10] the continued fraction expansion of $(b+\omega_d)/N(I)$ yields all of the reduced ideals in $\mathcal{O}_K$ equivalent to I, in the following sense

$$I_0=[Q_0/\sigma, (P_0+\sqrt{d})/\sigma]=I\sim I_1=[Q_1/\sigma, (P_1+\sqrt{d})/\sigma]\sim\cdots$$
$$\sim I_{k-1}=[Q_{k-1}/\sigma, (P_{k-1}+\sqrt{d})/\sigma],$$

(and $I_k=I_0=I$, see [10, §3, p. 410]). Thus the $(P_i+\sqrt{d})/Q_i$ are the complete quotients in the continued fraction expansion of $(b+\omega_d)/N(I)$.

Remark 1.1. The above shows that the Q_i/σ_i's represent the norms of all reduced ideals equivalent to I. Also k represents the exact number of reduced ideals in the class containing I. We call the set of reduced ideals $I_0, I_1, \cdots, I_{k-1}$ a cycle of reduced ideals and call k the period length of the cycle.

The above development suggests the following generalization of (similar but weaker) results in [2]–[3] which we will need throughout the next section.

Theorem 1.1. *Let $I=[N(I), b+\omega_d]$ be a reduced ideal in $\mathcal{O}_K$. Moreover in what follows all Q_i's are those appearing in the continued fraction expansion of $(b+\omega_d)/N(I)$.*

(a) *If J is reduced and $I\sim J$ then $N(J)=Q_i/\sigma$ for some i with $1\leq i\leq k$.*

(b) *If J and $\bar{J}$ are the only ideals of norm $N(J)$, where J is reduced, and $N(J)=Q_i/\sigma$ for some i with $1\leq i\leq k$, then either $J=I_i$ or $\bar{J}=I_i$.*

§ 2. Class numbers and the divisor function.

In what follows we will need some notation. Let $P=\{p_1, p_2, \cdots, p_n\}$ be a set of $n\geq 1$ distinct primes, and let A be a positive integer. Set $P_d(A)=\{s=\prod_{i=1}^n p_i^{b_i}: b_i\geq 0, s\leq A \text{ and if } p_i\mid d \text{ then } b_i\leq 1\}$. Let I be a fixed reduced ideal in $\mathcal{O}_K$ and set $Q_I(d)=\{$norms of all primitive ideals J such that $J\sim I\}$. Finally set $\mathcal{R}_I(d)=\{Q_i/\sigma: 1\leq i\leq k$ in the continued fraction expansion of $(b+\omega_d)/N(I)\}$.

The following result generalizes results in [1] as well as [6, Theorem 2.1, p. 275]. It also continues work in [5] and [7]–[8].

$\tau(x)$ denotes the divisor function, i.e., the number of positive divisors of x, $n(x)$ denotes the number of distinct prime divisors of x which ramify in K, and $(/)$ denotes the Kronecker symbol.

Theorem 2.1. *Let P be a finite set of primes p with $(d/p)\neq -1$, A a positive integer, and I a primitive product of ramified ideals (possibly $I=1$).*

If $P_d(A)\cap Q_I(d)=\{A, N(I)\}$ then we have

$$h(d)\geq\begin{cases}\tau(A)-2^n & \text{if } N(I)\mid A\\ \tau(A) & \text{if } N(I) \text{ does not divide } A\end{cases}, \qquad \text{where } n=n(A/N(I)).$$

Proof. Let $\{p_1, p_2, \cdots\}$ be the (finite) set of distinct prime factors of A.

The set of indices $\{1, 2, \cdots\}$ of these primes will be divided into two (disjoint) subsets X and Y as follows. $i \in X$ if and only if p_i is unramified, and $j \in Y$ if and only if p_j is ramified.

Letting $A=\prod_{i\in X} p_i^{\nu_i} \prod_{j\in Y} p_j$ we see that any divisor of A can be expressed in the form $\prod_{i\in X} p_i^{\mu_i} \prod_{j\in Y_0} p_j$ where $0\le\mu_i\le\nu_i$ and $\phi\subseteq Y_0\subseteq Y$. Thus a combination $c=((\mu_i)_{i\in X}, Y_0)$ of an $|X|$-tuple (μ_i) of integers and a subset Y_0 of Y represents a divisor of A; whence, the set S of all these combinations has cardinality $\tau(A)$. Since $A\in Q_I(d)$ then $\prod_{i\in X\cup Y} \mathcal{P}_i^{\nu_i}\sim I$ for some $\mathcal{P}_i | p_i$. We now fix such primes $\mathcal{P}_i$ and let $\mathcal{F}(c)$ denote the ideal class of $\prod_{i\in X} \mathcal{P}_i^{\mu_i} \prod_{j\in Y_0} \mathcal{P}_j$ in K. Thus $\mathcal{F}$ is a map of S into the ideal class group of K.

Claim 1. If A is not divisible by $N(I)$ then $\mathcal{F}$ is one-to-one.

Let $\mathcal{F}(c_1)=\mathcal{F}(c_2)$ where c_1 and c_2 represent (respectively) $\prod_{i\in X\cup Y_0} \mathcal{P}_i^{\mu_i}$ and $\prod_{i\in X\cup Y_0'} \mathcal{P}_i^{\mu_i'}$. Thus, $\prod_{i\in X\cup Y_1} \mathcal{P}_i^{\mu_i-\mu_i'}\sim 1$, where we may assume without loss of generality that $\mu_i-\mu_i'=1$ for all $i\in Y_1\subseteq Y_0\cup Y_0'$ because $\mathcal{P}_i=\bar{\mathcal{P}}_i$ for all $i\in Y$. Furthermore it is clear that we may also assume without loss of generality that $\prod_{i\in X\cup Y_1} \mathcal{P}_i^{\mu_i-\mu_i'}\ge 1$. Since $I\sim\prod_{i\in X\cup Y} \mathcal{P}_i^{\nu_i}$ then $I\sim \prod_{i\in X} \mathcal{P}_i^{\nu_i-(\mu_i-\mu_i')} \prod_{i\in Y-Y_1} \mathcal{P}_i=J$, say. Since $N(J)\le A$ then by hypothesis either $N(J)=A$ or $N(J)=N(I)$. If $N(J)=A$ then $\mu_i=\mu_i'$ for all $i\in X$ and $Y_1=\phi$ (in which case $c_1=c_2$), or $\nu_i=\mu_i-\mu_i'$ for all $i\in X$ and $I=\prod_{i\in Y-Y_1}\mathcal{P}_i$; i.e., $N(I)|A$.

Claim 2. If $N(I)|A$ then $\mathcal{F}(c_1)=\mathcal{F}(c_2)$ for exactly 2^n distinct pairs (c_1, c_2) with $c_1\ne c_2$ where $n=n(A/N(I))$.

From the proof of Claim 1 we have that if $N(I)|A$ and $\mathcal{F}(c_1)=\mathcal{F}(c_2)$ then

$$(*)\qquad \prod_{i\in X} \mathcal{P}_i^{\nu_i} \prod_{i\in Y_1} \mathcal{P}_i\sim 1$$

and

$$I=\prod_{i\in Y-Y_1} \mathcal{P}_i.$$

The number of distinct relationship which (*) generates is clearly

$$\sum_{i=1}^{n}\binom{n}{i}=2^n.$$

In the following application an ERD-type means an Extended Richaud-Degert type; i.e., a form $d=b^2+r$ where $4b\equiv 0 \pmod r$.

Corollary 2.1. *Let* $d=b^2+r\not\equiv 1 \pmod 4$, *with* $|r|<2b$ *and* r *odd be of ERD-type. Then* $h(d)\ge\tau((2b-|r-1|)/2)$.

Proof. Let $P=\{$primes p dividing $A=(2b-|r-1|)/2\}$ and let I be the ideal above 2. Since $A<\sqrt{d}$ then by Theorem 1.1, $P_d(A)\cap Q_I(d)\subseteq P_d(A)\cap \mathcal{R}_I(d)$. Now we explicitly calculate the $\mathcal{R}_I(d)$ by looking at the continued fraction expansion $(\sqrt{d}+\alpha)/2$ where $\alpha=\begin{Bmatrix}1 \text{ if } d\equiv 3 \pmod 4\\ 0 \text{ if } d\equiv 2 \pmod 4\end{Bmatrix}$. To avoid trivialities we assume $d>2$.

Case 1. $\lfloor\sqrt{d}\rfloor=b$; i.e., $r>0$. Then

i	0	1	2	3	4
P_i	α	$b-1$	$(r+1)/2$	$\left\{\begin{matrix} b-r \text{ if } r<b \\ (r+1)/2 \text{ if } r=b \end{matrix}\right\}$	$\left\{\begin{matrix} b-r \text{ if } r<b \\ b-1 \text{ if } r=b \end{matrix}\right\}$
Q_i	2	$b+(r-1)/2$	$b-(r-1)/2$	$\left\{\begin{matrix} 2r \text{ if } r<b \\ b+(r-1)/2 \text{ if } r=b \end{matrix}\right\}$	
a_i	$(b+\alpha-1)/2$	1	$\left\{\begin{matrix} 1 \text{ if } r<b \\ 2 \text{ if } r=b \end{matrix}\right\}$	$\left\{\begin{matrix} (b-r)/r \text{ if } r<b \\ 1 \text{ if } r=b \end{matrix}\right\}$	

⋮

Case 2. $\lfloor\sqrt{d}\rfloor=b-1$; i.e., $r<0$. Then

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

Thus in either case we see by the choice of P that $\mathcal{R}_I(d)\cap P_d(A)=\{2, A\}$. We now invoke Theorem 2.1 and we have the result.

Remark 2.1. If $|r|=1$ in Corollary 2.1 then we have a sharper result in [5] where we used different techniques, (which exist only for narrow R-D-types as noted in [5, Remark 3, p. 111]). Nevertheless $r=1$ was the only result achieved by Halter-Koch in [1] for the $d\not\equiv 1 \pmod 4$ case. In yet unpublished work Halter-Koch has generalized his results which are different from the results contained herein. Finally in [6, Theorem 2.2, p. 276] we dealt with the case where r is even and $d=b^2+r$ is of ERD-type, by different techniques.

Now we look at the $d\equiv 1 \pmod 4$ case.

Corollary 2.2. *Let* $d=b^2+r\equiv 1 \pmod 4$ *be of ERD-type with* $|r|<2b$ *and* r *odd. Then* $h(d)\geq \tau((2b-|r-1|)/4)-2^n$ *where* n *is the number of prime divisors of* $gcd((2b-|r-1|)/4, d)$.

Proof. Let $A=(2b-|r-1|)/4$ and $P=\{\text{primes } p\,|\,A \text{ and } p \text{ not dividing } r\}$ then since $A<\sqrt{d}/2$ we invoke Theorem 1.1 to get that $P_d(A)\cap \mathcal{Q}_I(d)\subseteq P_d(A)\cap \mathcal{R}_I(d)$ for any reduced ideal I. Let $I=1$, then an analysis of $\mathcal{R}_I(d)$ easily shows that $P_d(A)\cap \mathcal{R}_I(d)=\{1, A\}$. The result follows from Theorem 2.1.

Example 2.3. $d=4b^2+r$ where r divides b and $r>0$ is odd. Then $h(d)\geq \tau(b-(r-1)/4)-2^n$ where n is the number of prime divisors of $gcd(b-(r-1)/4, d)$. For example if $r=1$ then this is Halter-Koch's only result along these lines in [1] where we get $h(4b^2+1)\geq \tau(b)-1$. A number of other examples are given in [4].

In fact if A satisfies a certain bound as in Corollaries 2.1–2.2 above then we can say something more in general.

Corollary 2.3. *If* $A<\sqrt{d}/2$ *and* I *and* P *are as in Theorem* 2.1 *with*

$P_d(A)\cap\mathfrak{R}_I(d)=\{N(I),A\}$ then $h(d)\geq\tau(A)-2^n$ where n is the number of ramified prime divisors of A.

Proof. Since $A<\sqrt{d}/2$ then as noted in section 1, I must be reduced so $P_d(A)\cap Q_I(d)\subseteq P_d(A)\cap\mathfrak{R}_I(d)$, and the result now follows from Theorem 2.1.

Acknowledgements. The first author's research is supported by NSERC Canada grant ♯A8484 while that of the second author is supported by NSERC grant ♯A7649. Also the authors welcome the opportunity to thank the referee for valuable comments, and for observations which clarified some of the results in the paper.

Note of the Editor. In "Corrigenda for Solution of a Problem of Yokoi" by the same authors, these Proc. 67 (A) page 253, line 7, $2t_d/(\sigma-N(\varepsilon_d)-1)u_d^2$ should be replaced by $((2t_d)/\sigma-N(\varepsilon_d)-1)/u_d^2$.

We regret that this misplacement of parentheses and slanting strokes was caused by our mistake.

References

[1] F. Halter Koch: Quadratische Ordnungen mit grosser Klassenzahl. J. Number Theory, **34**, 82–94 (1990).
[2] S. Louboutin: Continued fractions and real quadratic fields. ibid., **30**, 167–176 (1988).
[3] ——: Groupes des classes d'ideaux triviaux. Acta Arithmetica, LIV, 61–74 (1989).
[4] R. A. Mollin: Class numbers bounded below by the divisor function. C. R. Math. Rep. Acad. Sci. Canada, **12**, 119–124 (1990).
[5] ——: On the divisor function and class numbers of real quadratic fields. I. Proc. Japan Acad., **66**A, 109–111 (1990).
[6] ——: On the divisor function and class numbers of real quadratic fields. II. ibid., **66**A, 274–277 (1990).
[7] ——: Lower bounds for class numbers of real quadratic fields. Proceed. Amer. Math. Soc., **96**, 545–550 (1986).
[8] ——: Lower bounds for class numbers of real quadratic and biquadratic fields. ibid., **101**, 439–444 (1987).
[9] R. A. Mollin and H. C. Williams: Class number one for real quadratic fields, continued fractions and reduced ideals. Number Theory and Applications (NATO ASI series) (ed. R. A. Mollin). C**265**, Kluwer Academic Publishers, pp. 481–496 (1989).
[10] H. C. Williams and M. C. Wunderlich: On the parallel generation of the residues for the continued fraction factoring algorithm. Math. Comp., **177**, 405–423 (1987).