72. On the Divisor Function and Class Numbers of Real Quadratic Fields. II

By R. A. MOLLIN
Department of Mathematics and Statistics, University of Calgary

(Communicated by Shokichi IYANAGA, M. J. A., Nov. 9, 1990)

Abstract: The purpose of this paper is to continue work begun in [12] by providing lower bounds for the class numbers of real quadratic fields $\boldsymbol{Q}(\sqrt{d})$ in terms of the divisor function. These results generalize those of Halter-Koch in [5] as well as Azuhata [1]-[2], Mollin [7]-[11], and Yokoi [17]-[23].

§1. **Notation and preliminaries.** Throughout d is a positive square-free integer, and $K=\boldsymbol{Q}(\sqrt{d})$, and $h(d)$ is the class number of K. The maximal order in K is denoted $\mathcal{O}_K$, and the discriminant of K is $\Delta=4d/\sigma^2$ where $\sigma=\begin{Bmatrix} 2 \text{ if } d\equiv 1 \pmod 4 \\ 1 \text{ if } d\equiv 2, 3 \pmod 4 \end{Bmatrix}$. Let $w_d=(\sigma-1+\sqrt{d})/\sigma$.

If $[\alpha, \beta]$ is the module $\{\alpha x+\beta y : x, y \in Z\}$ then we observe that the maximal order $\mathcal{O}_K=[1, w_d]$. It can be shown (for example see Ince [6, pp. v–vii]) that I is an ideal in $\mathcal{O}_K$ if and only if $I=[a, b+cw_d]$ where $a, b, c \in Z$ (the rational integers) with $c|b$, $c|a$ and $ac|N(b+cw_d)$; where N is the norm from K to $\boldsymbol{Q}$. Moreover if $a>0$ then a is unique and is the smallest positive rational integer in I, denoted $a=L(I)$. Thus $N(I)=cL(I)$. If $c=1$ we say that I is a primitive *ideal*, and so $N(I)=L(I)$. Since $I=(c)[a/c, b/c+w_d]$ then we may restrict our attention to primitive ideals, (where (c) denotes the principal ideal generated by (c)).

A primitive ideal I is called *reduced* if it does *not* contain any non-zero element α such that both $|\alpha|<N(I)$ and $|\bar{\alpha}|<N(I)$ where $\bar{\alpha}$ is the algebraic conjugate of α.

Proof of the following facts can be found in [14]–[16].

Theorem 1.1. (a) *If I is a reduced ideal then $N(I)<\sqrt{\Delta}$.*

(b) *If I is a primitive ideal and $N(I)<\sqrt{\Delta}/2$ then I is reduced.*

Let $I=[N(I), b+w_d]$ be primitive then the expansion of $(b+w_d)/N(I)$ as a continued fraction $\langle a_0, \overline{a_1, a_2, \cdots, a_k}\rangle$ of period length k and the sequences of integers P_i, Q_i, $i\geq 0$ are obtained recursively as follows:

$$(P_0, Q_0)=(\sigma b+\sigma-1, \sigma N(I)), \qquad P_{i+1}=a_iQ_i-P_i$$

where $a_i=\lfloor (P_i+\sqrt{d})/Q_i \rfloor$ with $\lfloor\ \ \rfloor$ being the greatest integer function, and $d=P_{i+1}^2+Q_iQ_{i+1}$.

Let $I=[N(I), b+w_d]$ primitive and reduced. Then the expansion of $(b+w_d)/N(I)$ into a continued fraction yields *all* of the reduced ideals in $\mathcal{O}_K$ equivalent to I; i.e. $I_1=[Q_0/\sigma, (P_0+\sqrt{d})/\sigma]=I\sim I_2=[Q_1/\sigma, (P_1+\sqrt{d})/\sigma]$

$\sim \cdots \sim I_k = [Q_{k-1}/\sigma, (P_{k-1}+\sqrt{d})/\sigma]$ and $I_{k+1}=I$ (where $\sim$ denotes equivalence in the class group of $\mathcal{O}_k$). Thus the $(P_i+\sqrt{d})/Q_i$ are complete quotients in the continued fraction of $(b+w_d)/N(I)$. From [16] we get:

Theorem 1.2. *Let $I=[N(J), b_J+w_d]$ be a reduced ideal in $\mathcal{O}_K$.*

(a) *If J is reduced and $I\sim J$, then $N(J)=Q_i/Q_0$ for some i with $0\leq i \leq k$.*

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

Let τ denote the divisor function where $\tau(x)$ is the number of distinct positive divisors of an integer x. $(\ /\ )$ will denote the Kronecker symbol.

If $A>0$ is a real number and $\mathcal{P}=\{p_1, \cdots, p_n\}$ is a set of distinct primes then $\mathcal{P}(A)=\{s=\prod_{i=1}^n p_i^{e_i}\colon e_i\geq 0$ and $s\leq A\}$. Let $Q(d)$ denote the set of all norms of primitive, principal ideals in $\mathcal{O}_K$. Finally set $R(d)=\{Q_i/Q_0\colon i=1, \cdots, k$ in the continued fraction expansion of $w_d\}$.

§2. Class numbers and the divisor function. The results in this section generalize those in [5]–[6].

Theorem 2.1. *Let $A>0$ be a real number and $\mathcal{P}=\{p_1, \cdots, p_n\}$ a set of primes such that $(d/p_i)=1$ for all $p_i\in\mathcal{P}$ and $\mathcal{P}(A)\cap Q(d)=1$. Then $h(d)\geq \tau(q)$ for all $q\in\mathcal{P}(A)$.*

Proof. Let $q\in\mathcal{P}(A)$ with $q=\prod_{i=1}^n p_i^{e_i}$. Let $\mathcal{P}_i$ be over p_i in $\mathcal{O}_K$. Set $\mathcal{A}=\prod_{i=1}^n \mathcal{P}_i^{f_i}$ where $0\leq f_i\leq e_i$.

Claim 1. If $\mathcal{A}\sim 1$ then $f_i=0$ for all i, where $\sim$ denotes equivalence in the class group C_K of K.

If $\mathcal{A}\neq 1$ then since all primes p_i split in K then $\mathcal{A}$ is primitive and principal. Thus, $N(\mathcal{A})\in\mathcal{P}(A)\cap Q(d)=1$, a contradiction, unless $f_i=0$ for all i.

Claim 2. If $1\neq\prod_{i=1}^n\mathcal{P}_i^{f_i}\sim\prod_{i=1}^n\mathcal{P}_i^{g_i}\neq 1$ for $0\leq f_i\,;\, g_i\leq e_i$ then $f_i=g_i$ for all i.

Consider $\prod_{i=1}^n\mathcal{P}_i^{f_i-g_i}\sim 1$. If some $f_i-g_i<0$ then (since we did not specify above) we may replace $\mathcal{P}_i$ by $\bar{\mathcal{P}}_i$, the conjugate of $\mathcal{P}_i$, without loss of generality. Therefore we have $\prod_{i=1}^n\mathcal{P}_i^{f_i-g_i}\sim 1$ with $f_i-g_i\geq 0$ for all i. By Claim 1 we are done. Hence we have $\tau(q)$ inequivalent ideals.

Example 2.1. Let $d=145$, $\mathcal{P}=\{2, 3\}$, and $A=3$. Then $\mathcal{P}(A)=\{1, 2, 3\}$ and by Theorems 1.1–1.2, $\mathcal{P}(A)\cap Q(d)\subseteq R(d)=\{1, 3\}$. Hence $\mathcal{P}(A)\cap Q(d)=1$. By Theorem 2.1, $h(d)\geq\tau(2)=\tau(3)=2$. Halter-Koch's result [5] yields only $h(d)\geq 1$. In fact $h(d)=4$.

Remark 2.1. In general if $d=4l^2+1$, $\mathcal{P}=\{$primes p with $p<l\}$ and $A=$largest prime in $\mathcal{P}$ then $\mathcal{P}(A)\cap Q(d)=1$ because $\mathcal{P}(A)\cap Q(d)\subseteq R(d)$ by Theorems 1.1–1.2, and $R(d)=\{1, l\}$. Thus $h(d)\geq\tau(A)$ if there exists a prime $p\in\mathcal{P}$ with $(d/p)=1$; i.e. $h(d)=1$ implies that d is not a quadratic residue modulo d. This was proved in [6] and [4] for example by entirely different techniques.

In particular if l is even then $d\equiv 1 \pmod 8$ and $h(d)=1$ if and only if

$d=17$. In [3] Callialp used analytic techniques to prove that for l even $h(d)=1$ for only finitely many $d=4l^2+1$.

Our result is much more precise in that there is exactly one; viz. $d=17$ and $h(d)=1$. Moreover our techniques are much more straightforward and simpler. This was also found by other techniques in [7].

Example 2.2. If $\mathscr{P}=\{p\}$ and f is maximal with respect to $p^f \leq A$ then clearly $f=\lfloor \log A/\log p \rfloor$ whence, $h(d) \geq \tau(p^f)=f+1>(\log A/\log p)$.

The following generalizes Halter-Koch's [5, Satz 3, p. 92] for Extended-Richaud Degert (ERD)-types, i.e., those of the form $d=l^2+r$ with $4l \equiv 0 \pmod{r}$.

Theorem 2.2. *Let $d=l^2+r$ be of ERD-type, $A=\sqrt{\Delta}/2$ and $\mathscr{P}=\{$primes $p: p|l$ with $(r/p)=1, r \not\equiv 1 \pmod{p}\}$. Then $h(d) \geq \tau(q)$ for all $q \in \mathscr{P}(A)$.*

Proof. All we need to show is that $\mathscr{P}(A) \cap Q(d)=1$. Since $\mathscr{P}(A) \cap Q(d) \subseteq R(d)$ by Theorems 1.1–1.2 then we need merely do an exhaustive check of each continued fraction table for the various ERD-types. Such a calculation was done in [11] and the result follows.

Example 2.3. Let $d=l^2+2$, $A=\sqrt{d}$, $\mathscr{P}=\{p \mid l: (2/p)=1\}$ then $h(d) \geq \tau(q)$ for all $q \in \mathscr{P}(A)$. For example if $d=p^2+2$ where $p \equiv \pm 1 \pmod{8}$ then $h(d) \geq \tau(p)=2$.

Example 2.4. Let $d=9l^2-2$, $A=\sqrt{d}$, $l>1$ with $\mathscr{P}=\{3\}$ then $h(d) \geq \tau(3)=2$. We also found this result by different methods in [8, Corollary 1.4, p. 11].

We conclude with results related to [5, Lemma 1, p. 88] which is found also in [9, Lemma 1.1, p. 40].

In [10] we proved the following which we easily see is related to Theorem 2.1. Herein we set the fundamental unit of K to be $\varepsilon_d=(t_d+u_d\sqrt{d})/\sigma$ and set $B=((2t_d/\sigma)-N(\varepsilon_d)-1)/u_d^2$.

Theorem 2.3. *If $h(d)=1$ then p is inert in K for all primes $p<B$.*

Remark 2.2. Let $n(B)$ denote the *nearest integer* to B. In [13] we found with one possible exception) all $h(d)=1$ when $n(B) \neq 0$. This completed the task of Yokoi begun [17]–[20] where he dealt with the special case where d is a prime congruent to 1 module 4.

We conclude with a result related to Theorems 2.1 and 2.3. First we define an element $\alpha \in \mathcal{O}_K$ to be *primitive* if (α) is not divisible by any rational ideal except (1), and $(\alpha) \neq (1)$. A version of this was proved in [6].

Proposition 2.1. *Let $A>0$ be 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* $\alpha \in \mathcal{O}_K$.

Proof. (1)→(2): Let $\alpha=(x+y\sqrt{d})/\sigma \in \mathcal{O}_K$ be primitive. Thus $|N(x+y\sqrt{d})|=\sigma^2 m$. If $1<m<A$ then $m=t^2$ with $\gcd(x,y)=t$, whence $t=1$. Thus α is a unit, contradicting primitivity.

(2)→(1): Let $|x^2-dy^2|=\sigma^2 m$ for $1<m<A$. Let $\gcd(x,y)=t$, then

$|(x/t)^2-d(y/t)^2|=\sigma^2 m/t^2$. Thus $\alpha=(x/t)+\sqrt{d}(y/t)$ is primitive if $m\neq t^2$ so $m/t^2\geq A$, a contradiction. Hence, $m=t^2$.

Corollary 2.1. If (1) fails $A>B$.

Proof. By [9, Lemma 1.1, p. 40] if (1) fails then $m\geq B$. However, $B\leq m<A$.

Acknowledgements. The author gratefully acknowledges the financial support of NSERC Canada Grant No. A8484. Moreover, the author's current research is supported a Killam research award held at the University of Calgary in 1990. The author wishes also to thank the referee for useful comments.

References

[1] T. Azuhata: On the fundamental units and the class numbers of real quadratic fields. Nagoya Math. J., **95**, 125–135 (1984).
[2] ——: On the fundamental units and the class numbers of real quadratic fields. II. Tokyo Math. J., **10**, 259–270 (1987).
[3] F. Callialp: Non-nullité des fonctions zeta des corps quadratiques réels pour $0<s<1$. C. R. Acad. Sci. Paris, sér. A–B, **291**, A623–A625 (1980).
[4] S. Chowla and J. Friedlander: Class numbers and quadratic residues. Glasgow Math. J., **17**, 47–52 (1976).
[5] F. Halter-Koch: Quadratische Ordnungen mit grosser Klassenzahl. J. Number Theory, **34**, 82–94 (1990).
[6] ——: Prime producing quadratic polynomials and class numbers of quadratic orders (preprint).
[7] R. A. Mollin: Necessary and sufficient conditions for the class number of a real quadratic field to be one, and a conjecture of S. Chowla. Proc. Amer. Math. Soc., **102**, 17–21 (1988).
[8] ——: Diophantine equations and class numbers. J. Number Theory, **24**, 7–19 (1986).
[9] ——: On the insolubility of a class of diophantine equations and the nontriviality of the class numbers of related real quadratic fields of Richaud-Degert type. Nagoya Math. J., **105**, 39–47 (1987).
[10] ——: Class number one criteria for real quadratic fields. I. Proc. Japan Acad., **63A**, 121–125 (1987).
[11] ——: Class numbers and the divisor function (to appear).
[12] ——: On the divisor function and class numbers of real quadratic fields. I. Proc. Japan Acad., **66A**, 109–111 (1990).
[13] ——: Solution of a problem of Yokoi. ibid., **66A**, 141–145 (1990).
[14] R. A. Mollin and H. C. Williams: Class number one for real quadratic fields, continued fractions and reduced ideals. Number Theory and Applications (ed. R. A. Mollin) (NATO ASI series). Kluwer Academic Publishers, Dordrecht, pp. 481–496 (1989).
[15] H. C. Williams: Continued fractions and number theoretic computations. Rocky Mountain J. Math., **15**, 621–655 (1985).
[16] H. C. Williams and M. C. Wunderlich: On the parallel generation of the residues for the continued fraction factoring algorithm. Math. Comp., **48**, 405–423 (1987).
[17] H. Yokoi: Class number one problem for real quadratic fields (The conjecture of Gauss). Proc. Japan Acad., **64A**, 53–55 (1988).
[18] ——: Some relations among new invariants of prime numbers p congruent to 1 mod 4. Advanced Studies in Pure Math., **13**, Investigations in Number Theory, pp. 493–501 (1988).
[19] ——: The fundamental unit and class number one problem of real quadratic fields with prime discriminant (preprint).
[20] ——: Bounds for fundamental units and class numbers of real quadratic fields with prime discriminant (preprint).
[21] ——: On the fundamental unit of real quadratic fields with norm 1. J. Number Theory, **2**, 106–115 (1970).
[22] ——: On real quadratic fields containing units with norm-1. Nagoya Math. J., **33**, 139–152 (1968).
[23] ——: New invariants of real quadratic fields. Number Theory (ed. R. A. Mollin). Walter de Gruyter, Berlin, pp. 635–639 (1990).