30. On the Divisor Function and Class Numbers of Real Quadratic Fields. I

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

(Communicated by Shokichi IYANAGA, M. J. A., May 14, 1990)

The purpose of this paper is to provide sharp lower bounds for class numbers, $h(d)$, of real quadratic fields $Q(\sqrt{d})$ of narrow Richaud-Degert type; (R-D types); i.e., $d=l^2+r$ where $|r|\in\{1,4\}$. These results generalize those of Halter-Koch [2]. Moreover, the proof of the results presented herein are clearer and more informative than those given in [2], in the sense that one can literally count (in a combinatorial sense), up to the bounds presented. Furthermore this generalizes certain results given in Azuhata [1], Mollin [4]–[6], Hasse [3], and Yokoi [11]–[13]. In what follows $\tau(x)$ denotes the number of distinct positive divisors of x.

Theorem 1. *Let $K=Q(\sqrt{d})$; d square-free.*

(1) *If $d=a^2+1$; $a>1$ odd then $h(d)\geq 2\tau(a)-2$;*

(2) *If $d=4a^2+1$; $a>1$ then $h(d)\geq\tau(a)-1$;*

(3) *If $d=a^2+4$, $a>1$ odd then $h(d)\geq\tau(a)-1$;*

(4) *If $d=a^2-4$; $a>3$ odd then $h(d)\geq\left(\dfrac{\tau(a-2)\tau(a+2)}{4}\right)=\dfrac{\tau(d)}{4}$;*

(5) *If $d=4a^2-1$; $a\geq 1$ then $h(d)\geq\dfrac{\tau(2a-1)\tau(2a+1)}{2}=\dfrac{\tau(d)}{2}$.*

Proof. (1) Let $a=\prod_{i=1}^{r}p_i^{e_i}$ with p_i's distinct primes and P_i an O_K-prime (where O_K is the ring of integers of K) above p_i. Also set $p_0=2$; with P_0 above p_0 and $e_0=1$.

Claim 1. If $1\neq A=\prod_{i=0}^{r}P_i^{f_i}\sim 1$ with $0\leq f_i\leq e_i$ then $f_i=e_i$ for all i with $0\leq i\leq r$. (Here $\sim$ denotes equivalence in the class group of K.)

The P_i's are not inert so $A\sim 1$ implies $A=(x+y\sqrt{d})$ for some primitive integer (i.e. having no rational divisors other than ± 1), $x+y\sqrt{d}\in O_K$. Thus:

$$|N(A)|=|N(x+y\sqrt{d})|=\prod_{i=0}^{r}p_i^{f_i}=x^2-dy^2.$$

By [6, Lemma 1.1, p. 40]:

$$\prod_{i=0}^{r}p_i^{f_i}\geq 2a=\prod_{i=0}^{r}p_i^{e_i}\quad\text{whence } f_i=e_i,$$

thus securing Claim 1.

Claim 2. All ideals $\prod_{i=0}^{r}P_i^{f_i}$ for $0\leq f_i\leq e_i$ are inequivalent except for $1\sim\prod_{i=0}^{r}P_i^{e_i}$.

Let $\prod_{i=0}^{r}P_i^{f_i}\sim\prod_{i=0}^{r}P_i^{g_i}$ for some $0\leq f_i$; $g_i\leq e_i$. Suppose that some $f_i>g_i$, so that (after possibly renumbering) we may assume without loss of generality that $f_i > g_i$ for $0 \le i \le t \le r$ and $f_i \le g_i$ for $t+1 \le i \le r$. Thus:

$$\prod_{i=0}^{t} P_i^{f_i-g_i} \sim \prod_{i=t+1}^{r} P_i^{g_i-f_i}. \quad \text{But, } \prod_{i=0}^{r} P_i^{e_i} \sim 1. \quad \text{Therefore,}$$

$$\prod_{i=0}^{t} P_i^{f_i-g_i-e_i} \prod_{i=t+1}^{r} P_i^{-e_i} \sim \prod_{i=0}^{t} P_i^{f_i-g_i} \quad \text{and so:}$$

$$1 \sim \prod_{i=0}^{t} P_i^{e_i+g_i-f_i} \prod_{i=t+1}^{r} P_i^{g_i-f_i+e_i} = B = (u+v\sqrt{d}),$$

say. Hence, as above; if $B \ne 1$ then (as above):

$$|N(B)| = \prod_{i=0}^{t} p_i^{e_i+g_i-f_i} \prod_{i=t+1}^{r} p_i^{g_i-f_i+e_i} \ge \prod_{i=0}^{r} p_i^{e_i};$$

whence:

$$\prod_{i=t+1}^{r} p_i^{g_i-f_i} \ge \prod_{i=0}^{t} p_i^{f_i-g_i}.$$

Similarly:

$$\prod_{i=0}^{t} p_i^{f_i-g_i} \ge \prod_{i=t+1}^{r} p_i^{g_i-f_i}.$$

Thus $f_i = g_i$ for $i=0, \cdots, r$, contradicting our assumption. Therefore no such t exists and so $f_i = g_i$ for $i=0, 1, \cdots, r$ *unless* $B=1$; i.e., unless $g_i=0$; $f_i = e_i$ for $i=0, 1, \cdots, r=t$.

Now we count the number of distinct ideals $\prod_{i=0}^{r} P_i^{f_i}$ for $0 \le f_i \le e_i$ and we get $2\prod_{i=1}^{r}(e_i+1)-2$ of them (since we must exclude $\prod_{i=0}^{r} P_i^{e_i}$ and P_0 because $P_0 \sim \prod_{i=1}^{r} P_i^{e_i}$ since $P_0 = \bar{P}_0$, the conjugate of P_0).

Hence $h(d) \ge 2\tau(a)-2$, which completes (1).

(2) $d=4a^2+1$. Let $a=\prod_{i=1}^{r} P_i^{e_i}$ then as in (1) all $\prod_{i=1}^{r} P_i^{f_i}$ are inequivalent for $0 \le f_i \le e_i$ except for $\prod_{i=1}^{r} P_i^{e_i} \sim 1$. Since 2 does not enter into the picture here we have:

$$h(d) \ge \tau(a)-1.$$

(3) Exactly the same analysis as (2) yields the same result.

(4) $d=a^2-4$. Let $a-2=\prod_{i=1}^{r} P_i$ then by the same methodology as above we have all $\prod_{i=1}^{r} P_i^{f_i}$ for $0 \le f_i \le 1$ being inequivalent unless $\prod_{i=1}^{r} P_i \sim 1$. However since all P_i are ramified then $P_i = \bar{P}_i$, so: $\prod_{j \in S} P_j \sim \prod_{j \in S'} P_j$ where $S \cap S' = \phi$ and $S \cup S' = \{i\}_{i=1}^{r}$. Hence we must remove $1+\frac{1}{2}\sum_{i=1}^{r-1}\binom{r}{i} = 2^{r-1}$ ideals as being equivalent to ones already counted, $\left(\text{where } \binom{r}{i} \text{ is the binomial coefficient}\right)$. Thus we have exactly $\tau(a-2)-2^{r-1}$ inequivalent ideals. Since $\tau(a-2)=2^r$ then we have in fact, $\tau(a-2)/2=2^{r-1}$ of them. A similar analysis of $a+2$ yields $\tau(a-2)/2$ inequvalent ideals. Moreover using the techniques of (1) it can be shown that none of the ideals from $a-2$ are equivalent to those of $a+2$ except for the trivial ideal. Thus $h(d) \ge (\tau(a-2)\tau(a+2)/2)-(\tau(a-2)\tau(a+2)/4)$, i.e., $h(d) \ge \tau(a-2)\tau(a+2)/4$.

(5) $d=4a^2-1$. By a similar analysis to that of (4) we get the result $h(d) \ge \tau(2a-1)\tau(2a+1)/2$.

The ramification of 2 accounts for the difference.

Remark 1. From Gauss's genus theory it follows that $h(d) \ge 2^{r-1}$

where r is the number of distinct prime divisors of the discriminant of K (excluding one prime $p\equiv 3 \pmod 4$). Thus Theorem 1 (4)–(5) rediscovers this fact for those forms. Moreover, the proof is far more elementary.

Remark 2. To illustrate the sharpness of the bounds consider

(1) $h(10)=2=2\tau(3)=2$;

(2) $h(3)=1=\tau(3)-1$;

(3) $h(29)=1=\tau(5)-1$;

(4) $h(165)=2=\tau(165)/4$;

(5) $h(35)=2=\tau(35)/2$.

Remark 3. The techniques used above do not generalize to extended R-D types; i.e., those forms $d=l^2+r$ where $r\,|\,4l$, studied in [7]–[10]. The reason is that [6, Lemma 1.1, p. 40] has too "narrow" a bound. (Note that we found all extended R-D types of class number one (with one possible exception) in [9].)

Acknowledgements. The author's research is supported by NSERC Canada grant no. A8484. Moreover the current research is supported by a Killam research fellowship held at the University of Calgary in 1990.

References

[1] T. Azuhata: On the fundamental units and the class numbers of real quadratic fields. Nagoya Math. J., **95**, 125–135 (1984).

[2] F. Halter-Koch: Quadratische Ordnungen mit grosser Klassenzahl. J. Number Theory, **34**, 82–94 (1990).

[3] H. Hasse: Über mehrklassige aber eingeschlechtige reell-quadratische Zahlkörper. Elem. Math., **20**, 49–59 (1965).

[4] R. A. Mollin: Lower bounds for class numbers of real quadratic fields. Proc. Amer. Math. Soc., **96**, 545–550 (1986).

[5] ——: Lower bounds for class numbers of real quadratic and biquadratic fields. ibid., **101**, 439–444 (1987).

[6] ——: 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).

[7] R. A. Mollin and H. C. Williams: On prime valued polynomials and class numbers of real quadratic fields. ibid., **112**, 143–151 (1988).

[8] ——: Prime producing quadratic polynomials and real quadratic fields of class number one. Number Theory (eds. J. M. De Koninck and C. Levesque). Walter de Gruyter Publishers, Berlin, New York, pp. 654–663 (1988).

[9] ——: Solution of the class number one problem for real quadratic fields of extended Richaud-Degert type (with one possible exception). Number Theory (ed. R. A. Mollin). Walter de Gruyter Publishers, Berlin, New York, pp. 417–425 (1990).

[10] ——: Class number one for real quadratic fields, continued fractions and reduced ideals. Number Theory and Applications (ed. R. A. Mollin) (NATO ASI series). vol. C265, Kluwer Academic Publishers, pp. 481–496 (1989).

[11] H. Yokoi: On the diophantine equation $x^2-py^2=\pm 4q$ and the class number of real subfields of a cyclotomic field. Nagoya Math. J., **91**, 151–161 (1983).

[12] ——: On real quadratic fields containing units with norm 1. ibid., **33**, 139–152 (1968).

[13] ——: On the fundamental unit of real quadratic fields with norm 1. J. Number Theory, **2**, 106–115 (1970).