4. On the Divisor Function and Class Numbers of Real Quadratic Fields. IV

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

(Communicated by Shokichi IYANAGA, M. J. A., Jan. 13, 1992)

In this paper we conclude the investigation begun in [2]–[3] and [7]. We refer the reader to [2]–[3] for the notation and background material used herein.

Our first result generalizes Corollaries 2.1 and 2.2 of [7], (which we were only able to prove for ERD-types therein), and give, thereby, corrections to [4, Theorems 2.1–2.2, pp. 120–121]. First we deal with the case where $d\not\equiv 1 \pmod 4$.

Theorem 1. *Let $d=b^2+r\not\equiv 1 \pmod 4$ with $|r|<2b$ and r odd. Set $A=(2b-|r-1|)/2$ and assume $P_d(A)\cap \mathcal{R}_I(d)=\{2, A\}$ where I is the ideal over 2 and $P=\{$primes $p : p\,|\,A\}$. Thus*

$$h(d)\geq\tau(A).$$

Proof. Since $A<\sqrt{d}$ then $P_d(A)\cap Q_I(d)\subseteq P_d(A)\cap \mathcal{R}_I(d)$, and so the result now follows from Theorem 2.1 of [7].

Remark 1. The weaker hypothesis given in Theorem 2.1 of [4]; (viz., that no divisor m of $(2a-|r-1|/4)$ with $1<m<(2a-|r-1|/4)$ appears in $\mathcal{R}_1(d)$), is insufficient to yield the conclusion therein, which is weaker than Theorem 2, below. For example if $d=385=20^2-15$ then $A=6$. Here $h(d)=2$ but $\tau(A)-1=3$. The problem is that $4\in\mathcal{R}_1(d)$. In fact any time that there is a divisor of A^2 (not just A) with $1<m<A$ with $m\in\mathcal{R}_1(d)$ then Theorem 2.2 of [4] fails to hold.

Theorem 2. *Let $d=b^2+r\equiv 1 \pmod 4$ with $|r|<2b$ and r odd. Set $A=(2b-|r-1|)/4$, $P=\{$primes $p : p\,|\,A\}$ and assume $P_d(A)\cap\mathcal{R}_1(d)=\{1, A\}$ then*

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

where $n=n(A)$.

Proof. This follows from Theorem 2.1 of [7].

Remark 2. Corollary 2.2 of [7] is immediate from the above. Thus Theorem 1–2 correct [4, Theorems 2.1–2.2, pp. 120–121] for the cases where r is odd. Now we look at the case where r is even.

Theorem 3. *Let $d=b^2+r$ with r even and $|r|<2b$ and set*

$$A=\begin{cases}2b-|r-1| & \text{if } d\not\equiv 1 \pmod 4\\ b-|r/4-1| & \text{if } d\equiv 1 \pmod 4\end{cases}.$$

Assume that if $m\,|\,A^2$ where $m>1$ is divisible by only unramified primes then $m\notin Q_1(d)$ (i.e., no such m is the norm of a primitive principal ideal). Then with $n=n(A)$,

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

Proof. Since $\sigma^2\alpha A = (b+\alpha\sigma)^2 - d$ where $\alpha = 1$ if $r > 0$ and -1 otherwise, then $A = \prod_{i=1}^n p_i^{e_i}$ with $e_i > 0$, where $(\Delta/p_i) \neq -1$ for $1 \leq i \leq n$ and $e_i = 1$ whenever $(\Delta/p_i) = 0$. Moreover, since $N(b+\alpha\sigma+\sqrt{d}) = \alpha\sigma^2 A$ then there are $\mathfrak{p}_i$'s above p_i such that $\mathcal{A} = \prod_{i=1}^s \mathfrak{p}_i^{e_i} \sim 1$.

Now assume that

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

with $1 \leq f_i$; $g_i \leq e_i$. Let $\{p_i\}_{i=1}^{s_1}$ be all of the unramified primes in $\{p_i\}_{i=1}^s$ and order those primes so that $f_i \geq g_i$ for $i = 1, 2, \cdots, s_0$ and $f_i < g_i$ for $i = s_0+1, \cdots, s_1$. Also order the ramified primes so that $f_i \neq g_i$ for $i = s_1+1, \cdots, s_2$ and so that $f_i = g_i$ for $i = s_2+1, \cdots, s$. Thus (*) becomes,

$$(**) \qquad 1 \sim \prod_{i=1}^s \mathfrak{p}_i^{f_i - g_i} \sim \prod_{i=1}^{s_0} \mathfrak{p}_i^{f_i - g_i} \prod_{i=s_0+1}^{s_1} \bar{\mathfrak{p}}_i^{g_i - f_i} \prod_{i=s_1+1}^{s_2} \mathfrak{p}_i = I.$$

If $m = N(I) > \sqrt{\Delta}/2$ then $m = A$ since m divides $A < \sqrt{\Delta}$. Thus $f_i = e_i$ and $g_i = 0$ for $i = 1, 2, \cdots, s_0$; $g_i = e_i$ and $f_i = 0$ for $i = s_0+1, \cdots, s_1$ and $s_2 = s$; i.e., (**) becomes,

$$(***) \qquad 1 \sim \prod_{i=1}^{s_0} \mathfrak{p}_i^{e_i} \prod_{i=s_0+1}^{s_1} \bar{\mathfrak{p}}_i^{e_i} \prod_{i=s_1+1}^{s} \mathfrak{p}_i.$$

Hence

$$1 \sim \prod_{i=1}^{s_0} \mathfrak{p}_i^{2e_i} \prod_{i=s_0+1}^{s_1} \bar{\mathfrak{p}}_i^{2e_i}.$$

Since $\mathcal{A} \sim 1$ then $\mathcal{A}^2 \sim 1$ so $J_1 = \prod_{i=1}^{s_0} \mathfrak{p}_i^{2e_i} \sim \prod_{i=s_0+1}^{s_1} \mathfrak{p}_i^{2e_i} = J_2 \sim 1$. By hypothesis no such ideals can exist. Therefore one of $J_1 = 1$ or $J_2 = 1$, say $J_2 = 1$; i.e., $s_0 = s_1$ and (***) becomes

$$1 \sim \prod_{i=1}^{s_0} \mathfrak{p}_i^{e_i} \prod_{s_0+1}^{s_2} \mathfrak{p}_i.$$

We have shown that the only possible equivalences among the $1 \neq \prod_{i=1}^s \mathfrak{p}_i^{f_i}$ for $0 \leq f_i \leq e_i$ are

$$\prod_{i=1}^{s_0} \mathfrak{p}_i^{e_i} \prod_{i \in \mathcal{Y}} \mathfrak{p}_i \sim \prod_{i \in \mathcal{Y}'} \mathfrak{p}_i$$

where $\mathcal{Y} \cup \mathcal{Y}' = \{s_0+1, \cdots, s\}$ and $\mathcal{Y} \cap \mathcal{Y}' = \phi$. (When $J_1 = 1$ a similar result follows.)

There are clearly $2^n = \sum_{i=0}^n \binom{n}{i}$ such combinations where $n = s - s_0$.

The above then completes the correction of [4] and concludes the investigation of class numbers and the divisor function begun in [2]–[3] and [7], including a complete generalization for ERD-types.

Remark 3. In [2]–[4] we have assumed d to be square-free since we feel that the essential and interesting problems involve the analysis of the class number of the real quadratic fields. Thus, although Halter-Koch's [1] looks at seemingly more general results by allowing d to be non-square-free, the only interesting applications are to maximal orders and they are the only applications given in [1]. Hence although our results can be easily generalized to arbitrary orders we feel that this is an uninteresting exercise.

Acknowledgements. The author gratefully acknowledges the support of NSERC Canada grant ♯A8484. Also the author thanks the referee for useful observations.

References

[1] F. Halter Koch: Quadratische Ordnungen mit grosser Klassenzahl. J. Number Theory, **34**, 82–94 (1990).
[2] R. A. Mollin: On the divisor function and class numbers of real quadratic fields. I. Proc. Japan Acad., **66A**, 109–111 (1990).
[3] ——: On the divisor function and class numbers of real quadratic fields. II. ibid., **66A**, 274–277 (1990).
[4] ——: Class numbers bounded below by the divisor function. C. R. Math. Rep. Acad. Sci. Canada, **12** 119–124 (1990).
[5] ——: Powers in continued fractions and class numbers of real quadratic fields (to appear in Utilitas Math.).
[6] ——: Applications of a new class number two criterion for real quadratic fields. Computational Number Theory (eds. A. Petho *et al.*). Walter de Gruyter, pp. 83–94 (1991).
[7] R. A. Mollin and H. C. Williams: On the divisor function and class numbers of real quadratic fields. III. Proc. Japan Acad., **67A**, 338–342 (1991).