84. *Orders in Quadratic Fields. II*

By R. A. MOLLIN*) and L.-C. ZHANG**)

(Communicated by Shokichi IYANAGA, M. J. A., Nov. 12, 1993)

Abstarct: We provide very sharp lower bounds for the class numbers of arbitrary complex quadratic order.

Key words: Complex quadratic order; class number; quadratic polynomial.

The work herein continues that of [5] to which we refer the reader for background information and notation. This also complements the work of the authors in [6] where we dealt with the real case.

Our principal result (Theorem 1 below) provides a sharp lower bound for h_Δ when $\Delta < 0$ is the discriminant of any complex quadratic order, and yields as a consequence a complete generalization of the well-known result by Rabinowitsch [8] for $h_{\Delta_0} = 1$, and includes the more recent result by Sasaki [9] for $h_{\Delta_0} = 2$. Furthermore, our results yield sharper bounds than those given heretofore in the literature such as Oesterlé [7] and Buhler, Gross and Zagier [2]. Most recently Sasaki [9] gave the following lower bound

$$(*) \qquad h_{\Delta_0} \geq d(N(b + \omega))$$

where b is any non-negative integer with $b \leq |\Delta_0|/4 - 1$ and $d(m)$ is the number of (not necessarily distinct) prime divisors of m.

It is in the context of $(*)$ that we couch our main result which will be seen to be a much sharper bound as follows. In the following $D = f^2 D_0$ where D_0 is the radicand of $\boldsymbol{Q}(\sqrt{\Delta}) = \boldsymbol{Q}(\sqrt{D_0})$.

Theorem 1. *Let $\Delta < 0$ be a discriminant with odd conductor f. If b is any integer and M is any divisor of $N(b + \omega_\Delta)$ with $M < N(\omega_\Delta)$ and $gcd(M, f) = 1$ then $h_\Delta \geq \tau(M)$, the number of distinct positive divisors of M.*

Proof. It suffices to show that if $a_1 \neq a_2$ are both divisors of M then $I_1 = [a_1, b + \omega_\Delta]$ is not equivalent to $I_2 = [a_2, b + \omega_\Delta]$. Suppose, to the contrary that $I_1 \sim I_2$.

Claim. There exist relatively prime integers x and y satisfying

$$(1) \qquad ((\sigma a_1 x) + (\sigma b + \sigma - 1)y)^2 - Dy^2 = \sigma^2 a_1 a_2.$$

$$(2) \qquad a_2 \mid (a_1 x + (2b + \sigma - 1)y).$$

$$(3) \qquad \sigma^2 a_1 a_2 \mid (D - (\sigma b + \sigma - 1)^2)y.$$

We only prove the case where $\sigma = 1$ since the other case is similar. Since $I_1 \sim I_2$ then there exists an element $\gamma \in I_1$ such that $(\gamma)I_2 = (a_2)I_1$

*) Department of Mathematics and Statistics, The University of Calgary, Canada.
The first author's research is supported by NSERC Canada grant # A8484.
**) Mathematics Department, Southwest Missouri State University, U. S. A.
The second author's research is supported by an SMSU Faculty Summer Fellowship.

(e.g. see [4, section 3, p. 128] and also [1, Lemma 2.6, p. 110]). If $\gamma = a_1x + (b + \omega_\Delta)y$ where x and y are rational integers then

$$[(a_1a_2x + a_2by) + a_2y\omega_\Delta, \quad (a_1bx + (b^2 + D)y) + (a_1x + 2by)\omega_\Delta] = [a_1a_2, a_2b + a_2\omega_\Delta].$$

Thus there exists a $C = \begin{bmatrix} c_{11} & c_{12} \\ c_{21} & c_{22} \end{bmatrix} \in SL_2(\boldsymbol{Z})$ such that

$$[1, \omega_\Delta] \begin{bmatrix} a_1a_2 & a_2b \\ 0 & a_2 \end{bmatrix} \begin{bmatrix} c_{11} & c_{12} \\ c_{21} & c_{22} \end{bmatrix} =$$

$$[1, \omega_\Delta] \begin{bmatrix} a_1a_2x + a_2by & a_1bx + (b^2 + D)y \\ a_2y & a_1x + 2by \end{bmatrix}.$$

By comparing entries we have

$$a_1a_2c_{11} + a_2bc_{21} = a_1a_2x + a_2by \tag{4}$$

$$a_1a_2c_{12} + a_2bc_{22} = a_1bx + (b^2 + D)y \tag{5}$$

$$a_2c_{21} = a_2y \tag{6}$$

$$a_2c_{22} = a_1x + 2by. \tag{7}$$

From (4) and (6) we get that $c_{11} = x$ and $c_{21} = y$, and from (5) and (7) we get that $c_{22} = (a_1x + 2bx)/a_2$ and $c_{12} = y(D - b^2)/(a_1a_2)$. Since $|\det C| = 1$ we easily determine that (1) holds, and since c_{22} and c_{12} are integers we see that (2) and (3) hold. Finally, we complete the proof of Claim 1 by observing that $gcd(x, y) = gcd(c_{11}, c_{21}) = 1$.

Let $g = gcd(a_1, a_2)$ and set $a_i' = a_i/g$ for $i = 1, 2$. We may assume without loss of generality that $a_i' > a_2' \geq 1$. By (1) we have coprime integers x and y such that

$$(\sigma ga_1'x + (\sigma b + \sigma - 1)y)^2 - Dy^2 = \sigma^2g^2a_1'a_2' \tag{8}$$

$$ga_2' \mid (ga_1'x + (2b + \sigma - 1)y) \tag{9}$$

$$\sigma^2g^2a_1'a_2' \mid (D - (\sigma b + \sigma - 1)^2)y. \tag{10}$$

If $y = 0$ than by (8)

$$(\sigma ga_1'x)^2 = \sigma^2g^2a_1'a_2';$$

whence, $a_1' \mid a_2'$ a contradiction. Therefore $y \neq 0$.

Claim 2. $g \mid y$. Suppose that g does not divide y. Then there exists a prime p with p^e dividing g but not dividing y. If $p = 2$ then since

$$g \mid (2b + \sigma - 1)y \tag{11}$$

from (9) we must have $\sigma = 1$. Thus, from (10), $D \equiv (\sigma b + \sigma - 1)^2 = b^2 (mod\ 4)$. This is a contradiction since $D = f^2D_0$ with $D_0 \equiv 2, 3 (mod\ 4)$ and f is odd. Hence, $p > 2$ and from (11) we get that $p \mid (\sigma b + \sigma - 1)$. Hence, from (8), $p^2 \mid D$ whence $b \mid f$. However, $p \mid g \mid a_1 \mid M$ and $gcd(M, f) = 1$, a contradiction which secures the Claim 2.

Now set $y' = y/g$. From (8) we now get that

$$(\sigma a_1'x + (\sigma b + \sigma - 1)y')^2 - D(y')^2 = \sigma^2a_1'a_2'. \tag{12}$$

Since $(y')^2 \geq 1$ then (12) implies that $-D \leq (\sigma a_1'x + (\sigma b + \sigma - 1)y')^2 - D(y')^2 = \sigma^2a_1'a_2'$. However, $1 < a_1'a_2' \leq M < N(w_\Delta) = ((\sigma - 1)^2 - D)/\sigma^2$ a contradiction which secures the theorem.

Corollary 1. *If b is any integer with $|\sigma b + \sigma - 1| < \sqrt{-D}$ and M is any proper divisor of $N(b + \omega_\Delta)$ and $gcd(M, f) = 1$ with f odd then $h_\Delta \geq \tau(M)$.*

Proof. If $M \geq N(\omega_\Delta)$ then $N(b+\omega_\Delta)/2 \geq N(\omega_\Delta)$; i.e., $((\sigma b+\sigma-1)^2 - D)/(2\sigma^2) \geq ((\sigma-1)^2 - D)/\sigma^2$ which implies that $(\sigma b+\sigma-1)^2 \geq 2(\sigma-1)^2 - D$; i.e., that $|\sigma b+\sigma-1| \geq \sqrt{-D}$ a contradiction. The result now follows from Theorem 1.

Corollary 2 (Rabinowitsch [8]). *If $\Delta = \Delta_0 < 0$ is a discriminant then $h_\Delta = 1$ if and only if*

$$F_\Delta(x) = ((\sigma x+\sigma-1)^2 - D)/\sigma^2$$

is a prime for all non-negative integers $x \leq |\Delta|/4 - 1$.

Proof. First we observe two facts.

1. $F_\Delta(b) = N(b+\omega_\Delta)$, and
2. If $0 \leq b \leq |\Delta|/4 - 1$ then $F_\Delta(b) \leq N(\omega_\Delta)^2$.

Hence, if $F_\Delta(b)$ is not prime for some non-negative integer $b \leq |\Delta|/4 - 1$ then there exists a divisor $M > 1$ of $F_\Delta(b)$ with $M < N(\omega_\Delta)$. Hence, by Theorem 1, $h_\Delta \geq \tau(M) \geq 2$. Conversely, if $h_\Delta > 1$ then there exists a primitive, reduced, non-principal ideal $I = [a, b+\omega_\Delta]$ with $0 \leq b < a < M_\Delta = \sqrt{-\Delta/3} \leq |\Delta|/4 - 1$; whence, $N(b+\omega_\Delta) \leq N(\omega_\Delta)^2$ (see [1, §2]). Set $F_\Delta(b) = N(b+\omega_\Delta)$ and observe that $b \leq |\Delta|/4 - 1$. Since $a \mid F_\Delta(b)$ and I is not principal then $F_\Delta(b)$ cannot be prime.

Finally we illustrate the sharpness of our bound in Theorem 1.

Table. Lower bounds for h_Δ when $\Delta_0 = \Delta < 0$, and class group structure for C_Δ.

$-D$	σ	b	$N(b+\omega_\Delta)$	M	$N(\omega_\Delta)$	$\tau(M)$	h_Δ	C_Δ
14	1	2	18	6	14	4	4	C_4
23	2	1	8	4	6	3	3	C_3
26	1	8	90	18	26	6	6	$C_2 \times C_3$
41	1	7	90	30	41	8	8	C_8
110	1	40	1710	90	110	12	12	$C_2 \times C_2 \times C_3$
111	2	4	48	24	28	8	8	C_8
230	1	20	630	210	230	16	20	$C_2 \times C_2 \times C_5$
303	2	4	96	48	76	10	10	$C_2 \times C_5$
337	1	53	3146	286	337	8	8	C_8
357	1	4	112	56	357	8	8	$C_2 \times C_2 \times C_2$
379	2	5	125	25	95	3	3	C_3
411	2	16	375	75	103	6	6	$C_2 \times C_3$
443	2	11	243	81	111	5	5	C_5
466	1	22	950	190	466	8	8	C_8
467	2	26	819	63	117	6	7	C_7
473	1	11	594	198	473	12	12	$C_2 \times C_2 \times C_3$
485	1	55	3510	270	485	16	20	$C_2 \times C_2 \times C_5$
499	2	24	725	25	125	3	3	C_3
555	2	7	195	15	139	4	4	$C_2 \times C_2$
1155	2	52	3045	105	289	8	8	$C_2 \times C_2 \times C_2$
1365	1	105	12390	210	1365	16	16	$C_2 \times C_2 \times C_2 \times C_2$
3315	2	97	10335	195	829	8	8	$C_2 \times C_2 \times C_2$

Remark 1. The last four entries in Table are interesting in that they all have class groups of exponent $e_{\Delta} = 2$. In [6] Mollin was able to provide a complete list of all complex quadratic fields with class groups of exponent 2, under the assumption of a suitable Riemann Hypothesis. In point of fact $|\Delta| = |\Delta_0| = 3315$ in the largest one. We also see that our Theorem 1 above yields a much sharper bound than that given by Sasaki.

Acknowledgement. The authors thank the referee for suggestions which simplified the presentation of the results herein.

References

[1] J. Buchmann and H. C. Williams: A key-exchange system based on imaginary quadratic fields. J. Cryptology, **1**, 107–118 (1988).

[2] J. Buhler, B. Gross and D. Zagier: On the conjecture of Birch and Swinnerton-Dyer for an elliptic curve of rank 3. Math. Comp., **44**, 473–481 (1985).

[3] B. Gross and D. Zagier: Points de Heegener et dérivées de fonctions *L*. C. R. Acad. Sci. Paris., **297**, 85–87 (1983).

[4] H. Lenstra: On the calculation of regulators and class numbers of quadratic fields. Journées Arithmétiques (ed. J. V. Armitage). Cambridge University Press, pp. 123–150 (1982).

[5] R. A. Mollin: Orders in quadratic fields. I. Proc. Japan Acad., **69A**, 45–48 (1993).

[6] R. A. Mollin and L.-C. Zhang: Reduced ideals, the divisor function, continued fractions, and class numbers of real quadratic fields. Publicationes Mathematicae (to appear).

[7] J. Oesterlé: Nombres de classes des corps quadratiques imginaires. Sem. N. Boubaki, Exp. 631 (1983–1984).

[8] G. Rabinowitsch: Eindeutigkeit der Zerlegung in Primfaktoren in quadratischen Zahlkōrpern. J. reine angew. Math., **142**, 153–164 (1913).

[9] R. Sasaki: On a lower bound for the class number of an imaginary quadratic field. Proc. Japan Acad., **62A**, 37–39 (1986).