SOLUTIONS OF DIOPHANTINE EQUATIONS AND DIVISIBILITY OF CLASS NUMBERS OF COMPLEX QUADRATIC FIELDS

by R. A. MOLLIN

(Received 16 November, 1994)

1. Introduction. We show how the solution to certain diophantine equations involving the discriminant of complex quadratic fields leads to the divisibility of the class numbers of the underlying fields. This not only generalizes certain results in the literature such as [2], [4]–[6] but also shows why certain hypotheses made in these results are actually unnecessary since, as our criteria demonstrate, these hypotheses are forced by the solution of the diophantine equations involved. Our methods are based only on the most elementary properties of a principal ideal in a complex quadratic field.

2. Notation and preliminaries. Let $D < -1$ be a square-free integer and set $\Delta = 4D/\sigma^2$, where $\sigma = 2$ if $D \equiv 1 (\mathrm{mod}\ 4)$ and $\sigma = 1$ otherwise. The value Δ is called a *discriminant* and D is called a *radicand*. When applied to a quadratic field $K = Q(\sqrt{D})$, we call Δ the discriminant of K and D the radicand of K.

Let $[\alpha, \beta] = \alpha\mathbf{Z} \oplus \beta\mathbf{Z}$ with $\alpha, \beta \in K$. Then the *ring of integers* of K is $[1, \omega_\Delta] = \mathcal{O}_\Delta$, where $\omega_\Delta = (\sigma - 1 + \sqrt{D})/\sigma$. It is known that an ideal I of $\mathcal{O}_\Delta$ may be written as $I = [a, b + c\omega_\Delta]$, where $a, b, c \in \mathbf{Z}$, with $a > 0$, $c > 0$, $c \mid a$, $c \mid b$ and $ac \mid N(b + c\omega_\Delta)$, where $N(\alpha) = \alpha\alpha'$ is the *norm* from K to Q and α' is the *algebraic conjugate* of α. I is called *primitive* if $c = 1$. Equivalence of ideals in the *class group* C_Δ of $\mathcal{O}_\Delta$ is denoted by $I \sim J$, and the order of C_Δ is h_Δ, the *class number* of $\mathcal{O}_\Delta$ (or simply of K).

3. Diophantine equations and class numbers. Before presenting our first main result, we state a key lemma which we proved in [7] (for arbitrary complex quadratic orders).

LEMMA 3.1. *If $\Delta < 0$ is a discriminant and $I = [a, b + \omega_\Delta]$ is a primitive ideal of $\mathcal{O}_\Delta$ with $N(b + \omega_\Delta) < N(\omega_\Delta)^2$, then I is principal if and only if $a = 1$ or $a = N(b + \omega_\Delta)$.*

THEOREM 3.1. *Let Δ be a discriminant with radicand $D = b^2 - \sigma^2 m^t < 0$, where $t, m, b \in \mathbf{Z}$, with $t > 1$, $m > 1$, and $b > 0$. If t is even, then $t/2$ divides h_Δ, and if $b \neq 2m^{t/2} - 1$, then t divides h_Δ. If t is odd, and $b \neq \lfloor \sigma m^{t/2} \rfloor$, then t divides h_Δ.*

Proof. First we establish two claims.

Claim 1. Either $N(\omega_\Delta)^2 > N((b + \sqrt{D})/\sigma)$, or else $b = 2m^{t/2} - 1$.

If $N(\omega_\Delta)^2 \leq N((b + \sqrt{D})/\sigma)$, then $b \geq \sigma m^{t/2} - 1$. However, $b < \sigma m^{t/2}$. Thus, $b = \lfloor \sigma m^{t/2} \rfloor$. If t is odd, this contradicts the hypothesis, so $b = \sigma m^{t/2} - 1$. If $\sigma = 1$, then $N(\omega_\Delta)^2 = D^2 = 4m^t - 4m^{t/2} + 1 > N(b + \sqrt{D}) = m^t$. This establishes Claim 1.

We may form the ideals $I^c = [m^c, (b + \sqrt{D})/\sigma]$, where $1 \leq c \leq t$.

Claim 2. $I^g \sim 1$, where $g = \gcd(t, h_\Delta)$.

There exist integers u and v such that $g = tu + h_\Delta v$. Therefore, $I^g = I^{tu + h_\Delta v} \sim (I^t)^u (I^{h_\Delta})^v \sim 1$, since $N(I^t) = m^t = N((b + \sqrt{D})/\sigma)$ and clearly $I^{h_\Delta} \sim 1$. This secures Claim 2.

By Lemma 3.1 and Claims 1–2, we conclude that $g = t$, i.e. $t \mid h_\Delta$, unless $b = 2m^{t/2} - 1$. In the latter case, $D = 1 - 4m^{t/2}$. In this instance, we form the ideal $J = [m^{g_1}, (1 + \sqrt{D})/2]$, where $g_1 = \gcd(t/2, h_\Delta)$. We may use the same reasoning as above to conclude that $J \sim 1$. Moreover, since $m^{t/2} = N((1 + \sqrt{D})/2) < N(\omega_\Delta)^2 = m^t$, then by Lemma 3.1 $g_1 = t/2$, i.e. $t/2$ divides h_Δ.

Theorem 3.1 has numerous applications and it generalizes and helps to explain many related results in the literature. We cite a few as immediate consequences.

COROLLARY 3.1 (Gross and Rohrlich [**5**]). *Let $\Delta = D = 1 - 4m^t$ be a discriminant with $m > 1$ and t prime. Then $t \mid h_\Delta$.*

COROLLARY 3.2 (Cowles [**4**]). *Let $\Delta = b^2 - 4m^t \equiv 1 \pmod 4$ be a negative discriminant where m and t are odd primes. If one of the prime ideals over m is not principal in $\mathcal{O}_\Delta$, then $t \mid h_\Delta$.*

COROLLARY 3.3 (Mollin [**6**]). *Let $\Delta = b^2 - 4m^t \equiv 1 \pmod 4 < 0$ be a discriminant with $m > 1$ nd $t > 1$. If m^c is not the norm of a primitive element of $\mathcal{O}_\Delta$ whenever c properly divides t, then $t \mid h_\Delta$.*

REMARK 3.1. In Cowles' result above and our generalization of it stated in Corollary 3.3, there is an unnecessary hypothesis. This is explained by Theorem 3.1, namely that it is *not possible* for m^c to be the norm of a primitive principal ideal when $\Delta = b^2 - 4m^t < 0$ and $1 \le c < t$, unless $b = \lfloor \sigma m^{t/2} \rfloor$ or $b = 2m^{t/2} - 1$. What the proof of Theorem 3.1 shows is that, with the exception of this special case, $I^c \nsim 1$ for *any* such c. See Remark 3.3. Furthermore, we have the following corollary.

COROLLARY 3.4 (Mollin [**6**]). *Let Δ be a discriminant with radicand $D = b^2 - \sigma^2 m^t$, where $b > 0$, $m > 1$, and $t > 1$. If $b^2 \le \sigma^2 m^{t-1}(m - 1)$, then $t \mid h_\Delta$.*

REMARK 3.2. What the condition in Corollary 3.4 precludes is the possibility that $b = \lfloor \sigma m^{t/2} \rfloor$, but it is unnecessarily strong. In fact, we improve upon this as follows.

COROLLARY 3.5. *If Δ is a discriminant with radicand $D = b^2 - \sigma^2 m^t < 0$, where $t > 1$, $m > 1$, $b > 0$ and $b^2 \le \sigma^2 m^t - 2\sigma^2 m^{t/2} + \sigma - 1$, then $t \mid h_\Delta$.*

Proof. By Theorem 3.1, we need only ensure that $b \ne \lfloor \sigma m^{t/2} \rfloor$ and $b \ne 2m^{t/2} - 1$. If $b = \lfloor \sigma m^{t/2} \rfloor$, then $(\sigma m^{t/2} - 1)^2 \le b^2 \le \sigma^2 m^t - 2\sigma^2 m^{t/2} + \sigma - 1$. Thus, $2\sigma^2 m^{t/2} \le 2\sigma m^{t/2} + \sigma - 2$, a contradiction.

If $b = 2m^{t/2} - 1$, then $(2m^{t/2} - 1)^2 = b^2 \le 4m^t - 8m^{t/2} + 1$ and so $-4m^{t/2} \le 8m^{t/2}$, a contradiction.

REMARKS 3.3. It should be remarked that Theorem 3.1 speaks about divisibility of class numbers but says little (which cannot be determined easily by other methods) about the actual solutions of the Diophantine equations. The reasons for this are as follows. Consider a radicand $D < 0$, and the equation

$$D = b^2 - \sigma^2 m^t, \tag{3.1}$$

where b and t are unknowns.

https://doi.org/10.1017/S0017089500031438 Published online by Cambridge University Press

Suppose that

$$t \geq 2\log((1-D)/(2\sigma))/\log m. \tag{3.2}$$

Then it is not difficult to see that $-1 \leq b - \sigma m^{t/2} < 0$, i.e. either $b = \lfloor \sigma m^{t/2} \rfloor$ or $b = \sigma m^{t/2} - 1$. Thus, if (3.2) holds, and t is odd for example, then the solvability of (3.1) is equivalent to the solvability of $D = \lfloor \sigma m^{t/2} \rfloor^2 - \sigma^2 m^t$.

Illustrations of the power of Theorem 3.1 as a divisibility criterion are given in the following examples.

EXAMPLE 3.1. Let $D = 34933^2 - 4 \cdot 5^{13} = -3{,}662{,}498{,}011 = -61 \cdot 60{,}040{,}951$ with $h_\Delta = 12{,}714 = 13 \cdot 978$. Here $t = 13$, and $\lfloor \sigma m^{t/2} \rfloor = \lfloor 2 \cdot 5^{13/2} \rfloor = 69{,}877 > b = 34{,}933$.

The next example illustrates Theorem 3.1 when $b = 2m^{t/2} - 1$.

EXAMPLE 3.2. Let $D = 249^2 - 4 \cdot 5^6 = -499$. Then $b = 249 = 2m^{t/2} - 1 = 2 \cdot 5^3 - 1$ and $h_\Delta = 3 = t/2$.

The final example illustrates Corollary 3.5.

EXAMPLE 3.3. If $D = 174688^2 - 5^{15} = -1{,}680{,}781 = -151 \cdot 11{,}131$, then $h_\Delta = 660 = 15 \cdot 44$ with $t = 15$ and $\lfloor m^{t/2} \rfloor = 174{,}692 > b = 174{,}688$.

There is a treasure chest full of such examples to which Theorem 3.1 applies. These computations are limited only by the reader's imagination. Furthermore we may generalize results such as those of Ankeny and Chowla [**2**], wherein they show that there are infinitely many square-free radicands $D = b^2 - 3^t$, where $t \mid h_\Delta$. Our application is that we may easily show that there are infinitely many square-free radicands $D = 4 - m^t$ with $t \mid h_\Delta$ using the above techniques.

ACKNOWLEDGEMENT. The author's research is supported by NSERC Canada grant #A8484.

REFERENCES

1. R. Alter and K. K. Kubota, The diophantine equation $x^2 + 11 = 3^n$ and a related sequence, *J. Number Theory* **7** (1975), 5–10.

2. N. C. Ankeny and S. Chowla, On the divisibility of the class number of quadratic fields, *Pacific J. Math.* **5** (1955), 321–324.

3. J. H. E. Cohn, The Diophantine Equation $x^2 + 3 = y^n$, *Glasgow Math. J.* **35** (1993), 203–206.

4. M. J. Cowles, On the divisibility of the class number of imaginary quadratic fields, *J. Number Theory* **12** (1980), 113–115.

5. B. H. Gross and D. E. Rohrlich, Some results on the Mordell-Weil group of the Jacobian of the Fermat curve, *Invent. Math.* **44** (1978), 201–224.

6. R. A. Mollin, Diophantine equations and class numbers, *J. Number Theory* **24** (1986), 7–19.

7. R. A. Mollin, Orders in quadratic fields III, *Proc. Japan Acad. Ser. A Math. Sci.* **70** (1994), 176–181.

DEPARTMENT OF MATHEMATICS AND STATISTICS
UNIVERSITY OF CALGARY
CALGARY, ALBERTA
T2N 1N4
CANADA
e-mail address: ramollin@math.ucalgary.ca