

CLASS NUMBERS, QUADRATICS, AND EXPONENTIAL DIOPHANTINE EQUATIONS

R. A. MOLLIN

Mathematics Department, University of Calgary

Calgary, Alberta, Canada, T2N 1N4

e-mail: ramollin@math.ucalgary.ca

Abstract

We look at the relationships between class numbers of quadratic structures (orders and fields) and the solutions of exponential Diophantine equations. We conclude with necessary and sufficient conditions for a class group to have an element of a given order.

1. Notation and Preliminaries

If D is a squarefree integer, then its discriminant is given by

$$\Delta = \begin{cases} 4D & \text{if } D \not\equiv 1 \pmod{4}, \\ D & \text{if } D \equiv 1 \pmod{4}. \end{cases}$$

Then Δ is called a *fundamental discriminant* with associated radicand D , and

$$\omega_{\Delta} = \begin{cases} (1 + \sqrt{D})/2 & \text{if } \Delta = D \equiv 1 \pmod{4}, \\ \sqrt{D} & \text{if } \Delta \equiv 0 \pmod{4} \end{cases}$$

is called the *principal surd* associated with Δ . This will provide the canonical basis element for our orders. First we need notation for a \mathbb{Z} -module

2000 Mathematics Subject Classification: Primary 11R11; Secondary 11R29, 11R65.

Key words and phrases: class number, quadratic order, Diophantine equations.

Received July 12, 2004

© 2004 Pushpa Publishing House

$$[\alpha, \beta] = \{\alpha x + \beta y : x, y \in \mathbb{Z}\},$$

where $\alpha, \beta \in K = \mathbb{Q}(\sqrt{\Delta})$, the real quadratic field of discriminant Δ and radicand D . For this reason, fundamental discriminants are often called *field discriminants*.

We need to be able to distinguish those \mathbb{Z} -modules that are ideals in \mathcal{O}_Δ .

Theorem 1 (Primitive Ideals and Norms). *Let Δ be a fundamental discriminant, and set $I \neq (0)$ be \mathbb{Z} -submodule of \mathcal{O}_Δ . Then I has a representation of the form $I = [a, b + c\omega_\Delta]$, where $a, c \in \mathbb{N}$ and $b \in \mathbb{Z}$ with $0 \leq b < a$. Furthermore, I is an ideal of \mathcal{O}_Δ if and only if this representation satisfies $c|a$, $c|b$, and $ac|N(b + c\omega_\Delta)$. (For convenience, we call I an \mathcal{O}_Δ -ideal.) If $c = 1$, then we say that a non-zero ideal I is a primitive \mathcal{O}_Δ -ideal. If I is a primitive \mathcal{O}_Δ -ideal, then a is the least positive rational integer in I , denoted $N(I) = a$ called the norm of I .*

Proof. See [5, Theorem 1.2.1, p. 9]. We need to know when ideals are equal.

Theorem 2 (Criteria for Ideal Equality). *If Δ is a fundamental discriminant and $I = [a, \alpha]$ is a primitive \mathcal{O}_Δ -ideal, then $I = [a, za + \alpha]$ for any integer z .*

Proof. See [5, Theorem 1.2.2, p. 10].

The class group of \mathcal{O}_Δ will be denoted by \mathcal{C}_Δ and equivalences of ideal I, J therein by $I \sim J$. We will also be using the fact that if $I^j \sim 1$ (namely if I^j is a principal ideal in \mathcal{C}_Δ), and d is the smallest positive integer such that $I^d \sim 1$, then $d|j$.

The following will be a useful criterion in our study of complex quadratic ideals in the next section.

Theorem 3. *If $\Delta < 0$ is a fundamental discriminant and $I =$*

$[a, b + \omega_\Delta]$ is a primitive \mathcal{O}_Δ -ideal, satisfying $N(b + \omega_\Delta) < N(\omega_\Delta)^2$, then I is principal if and only if either $a = 1$ or $a = N(b + \omega_\Delta)$.

Proof. See [5, Theorem 1.3.2, p. 16], and [5, Exercise 1.5.7, p. 29].

2. Results

The following results are complex analogues of the results for real quadratic orders presented in [7], and is a generalization of the real case in [5, Theorem 3.1.1, p. 67]. Although the following is generalizable to arbitrary quadratic orders, we only state the result for the maximal orders (in quadratic fields) so that we may simplify the presentation. The reader may use the ideas in [5, Theorem 3.1.1, p. 67] and [7] to derive the more general context.

Theorem 4. Let $D = t^2 - r$ be a negative squarefree integer with, $t, r \geq 1$, and $D \not\equiv 1 \pmod{4}$. Assume that there exist integers $m \geq 0$, $N > 1$, and $n > 1$, such that

$$N^n = 4m^2 - 4mt + r, \quad (1)$$

and if n is odd, $|2m - t| \neq [N^{n/2}], \lfloor N^{n/2} - 1 \rfloor$. Then \mathcal{C}_{4D} has a cyclic subgroup of order n .

Proof. Let $I = [N, 2m - t + \sqrt{D}]$, which is a primitive \mathcal{O}_{4D} -ideal with norm N , by Theorem 1. We consider two cases.

Case 1. $N(2m - t + \sqrt{D}) < N(\sqrt{D})^2$

We may invoke Theorem 3 to conclude that $I^n = [N^n, 2m - t + \sqrt{D}]$ is principal, since $N(2m - t + \sqrt{D}) = N^n$.

Now $g = \gcd(n, h_\Delta)$. Then there exist integers u and v such that $g = un + h_\Delta v$, so

$$I^g \sim I^{nu} I^{h_\Delta v} \sim (I^n)^u (I_\Delta^h)^v \sim 1.$$

Therefore, by Theorem 3, $g = n$, namely $n | h_\Delta$, and since $I^j \neq 1$ for any $j < n$ by Theorem 3, then I has order n . Thus, \mathcal{C}_Δ has a cyclic subgroup of order n .

Case 2. $N(2m - t + \sqrt{D}) \geq N(\sqrt{D})^2$

We first demonstrate that $2m - t = \lfloor N^{n/2} \rfloor$ in this case. We have that $N^n \geq D^2$, so it follows from Equation (1) that $(2m - t)^2 \geq D^2$. Since

$$D = (2m - t)^2 - N^n, \quad (2)$$

$$|2m - t| \geq N^n - (2m - t)^2,$$

so $(2m - t)^2 + |2m - t| \geq N^n$. Therefore, $(|2m - t| + 1)^2 \geq N^n$, from which we get $|2m - t| \geq N^{n/2} - 1$. However, since $D(2m - t)^2 - N^n < 0$, $|2m - t| < N^{n/2}$. Hence, if n is odd, $|2m - t| = \lfloor N^{n/2} \rfloor$ and if n is even, then $|2m - t| = N^{n/2} - 1$, contradicting the hypothesis.

Example 1. An illustration of the odd n case in Theorem 4 is given by the following. If $D = -118 = 15^2 - 7^3 \equiv 2 \pmod{4}$, then $m = 0$, $|2m - t| = t = 15 \neq 18 = \lfloor 7^{3/2} \rfloor = \lfloor N^{n/2} \rfloor$, and $t \neq \lfloor N^{n/2} - 1 \rfloor = 17$, so \mathcal{C}_Δ has a cyclic subgroup of order $n = 3$. In fact, $h_\Delta = 6$.

Lest we think that $m = 0$ is the only possibility, we provide the following.

Example 2. Let $D = -161 = 2^2 - 165 \equiv 3 \pmod{4}$, with $t = 2$, $r = 165$,

$$N^n = 3^8 = 4 \cdot 41^2 - 4 \cdot 41 \cdot 2 + 165 = 4m^2 + 4mt + r,$$

and since $|2m - t| = 80 = \lfloor N^{n/2} \rfloor - 1$, $\mathcal{C}_\Delta = \mathcal{C}_{-644}$ has a cyclic subgroup of order 8. In fact $h_\Delta = 16$ and \mathcal{C}_Δ is a direct product of cyclic group of order 2 and one of order 8.

An immediate consequence of the proof of Theorem 4 is the following.

Corollary 1. *If $D = (2m - t)^2 - N^n \not\equiv 1 \pmod{4}$ is a negative squarefree integer with $t \geq 1$, $m \geq 0$, $N > 1$, and $n > 1$, and*

$$N^{n/2} < -D, \quad (3)$$

then \mathcal{C}_Δ has a cyclic subgroup of order n .

Example 3. If $D = -97 = 48^2 - 7^4 \equiv 3 \pmod{4}$, where $t = 48$, $r = 7 = N$, $m = 0$, $n = 4$, $N^{n/2} = 7^2 < -D$, so the hypothesis of Corollary 1 holds and $\mathcal{C}_\Delta = \mathcal{C}_{-388}$ has a cyclic subgroup of order 4. In fact, $h_{-388} = 4$.

Remark 1. Condition (3) in Corollary 1 is tantamount to saying that

$$N(2m + t + \sqrt{D}) < N(\omega_\Delta)^2,$$

so as in the proof of Theorem 4, we immediately have the result. Note that conditions 1-2 in Theorem 4 are always satisfied, in this case, since $D + N^j < 0$ for any j properly dividing n by condition (3).

We also have the following consequences.

Corollary 2 (Mollin [4]). *If $D = t^2 - N^n \not\equiv 1 \pmod{4}$ is a negative squarefree integer with $t \geq 1$, $n > 1$, $N \geq 5$ odd, and*

$$t^2 \leq N^{n-1}(N - 1), \quad (4)$$

then $n | h_\Delta$.

Proof. Condition (4) implies that condition (3) holds, so $n | h_\Delta$.

Remark 2. We presented Corollary 2 in 1986 as an analogue of a result by Cowles (see Corollary 7 below). As with that result, we may improve the bound in (4) considerably. Since the essential issue is to force $N(t + \sqrt{D}) < N(\omega_\Delta)^2$, with $m = 0$, then

$$t \leq N^{n/2} - 1 \quad (5)$$

is the sharpest bound possible, so (5) should replace condition (4) in

Corollary 2, for the best possible result.

Corollary 3 (Murty [9, Theorem 1, p. 87]). *If $D = 1 - N^n$ is squarefree with $N, N > 1$ and $N \geq 5$ odd, then C_Δ has a cyclic subgroup of order n .*

The following is an illustration of the necessity of the conditions in the hypothesis of Theorem 4, and demonstrates the sharpness of the above bound for t .

Example 4. If $D = -341 = 2759646^2 - 377^5$, then $|2m - t| = t = 275946 = \lfloor 377^{5/2} \rfloor = \lfloor N^{n/2} \rfloor$, and 5 does not divide $h_\Delta = 28$. Note that $N^{n/2} \geq \lfloor N^{n/2} \rfloor > N^{n/2} - 1$, in reference to Remark 2.

Remark 3. Example 4 is special in that it was shown, in [1], to be the only exception when n is a prime, a refinement of [5, Theorem 3.1.1, p. 67] for the case of prime exponent. In other words, we have the following.

Corollary 4. *If $D \not\equiv 1 \pmod{4}$, where D is a negative squarefree integer, with $D = x^2 - N^p$, where $x \geq 1, N \geq 2$, and $p > 2$ is prime, then $p \mid h_{4D}$ except when $D = 341, N = 377$ and $p = 5$.*

Proof. See [1, Corollary 7, p. 62].

The following provides an example to show that Theorem 4 cannot be used for the $D \equiv 1 \pmod{4}$ case.

Example 5. Let $D = -71 = 11^2 - 192 = t^2 - r \equiv 1 \pmod{4}$. Then

$$N^n = 2^9 = 4 \cdot 16^2 - 4 \cdot 16 + 192 = 4m^2 - 4mt + r$$

and $|2m - t| = 21 \neq \lfloor N^{n/2} \rfloor = 22$. Yet 9 does not divide $h_\Delta = 7$.

Now we consider the case where $D \equiv 1 \pmod{4}$ and relate it to results in [1]-[5] and [7].

Theorem 5. *Suppose that $D = t^2 - 4r \equiv 1 \pmod{4}$ is a squarefree negative integer with $t, r \geq 1$, and there exist integers $m \geq 0, n > 1, N > 1$ with*

$$N^n = m^2 + mt + r.$$

Also, $2m + t \neq \lfloor 2N^{n/2} \rfloor$ when n is odd, and $2m + t \neq 2N^{n/2} - 1$ when n is even. Then C_D has a cyclic subgroup of order n .

Proof. Set $I = [N, (2m + t + \sqrt{D})/2]$. Then if $N((2m + t + \sqrt{D})/2) < N(\omega_\Delta)^2$, we argue as in the proof of Theorem 4 to conclude that I has order n so that we have the desired conclusion. On the other hand if

$$N\left(\frac{2m + t + \sqrt{D}}{2}\right) \geq N(\omega_\Delta)^2 = \left(\frac{1 - D}{4}\right)^2,$$

then we deduce, in an analogous fashion to that of the proof of Theorem 4 to conclude that

$$2N^{n/2} > 2m + t \geq 2N^{n/2} - 1.$$

Therefore, when n is odd, $2m + t = \lfloor 2N^{n/2} \rfloor$ and when n is even $2m + t = 2N^{n/2} - 1$, both contradictions to the hypothesis.

Now we show the proper context into which to put Example 5.

Example 6. Since $D = -71 = 11^2 - 4 \cdot 48 = t^2 - 4r$ and

$$N^n = 2^7 = 5^2 + 11 \cdot 5 + 48 = m^2 + mt + r,$$

and $2m + t = 21 = \lfloor 2 \cdot 2^{7/2} \rfloor - 1$, so the hypothesis of Theorem 5 is satisfied with $n = 7$. Thus, $C_\Delta = C_{-71}$ has a cyclic subgroup of order 7, and as we saw in Example 5, it is in fact a group of order 7.

As with Theorem 4, the following is immediate from Theorem 5.

Corollary 5. If $D = (2m + t)^2 - 4N^n \not\equiv 1 \pmod{4}$ is a negative squarefree integer with $t \geq 1$, $m \geq 0$, $N > 1$, and $n > 1$, and

$$N^{n/2} < (1 - D)/4, \tag{6}$$

then C_Δ has a cyclic subgroup of order n .

Example 7. Let $D = -39 = 5^2 - 4 \cdot 2^4 = t^2 - 4N^n$, with $m = 0$ and $N^{n/2} = 2^2 < 10 = (1 - D)/4$, so $C_\Delta = C_{-39}$ has a cyclic subgroup of order 4 and since $h_\Delta = 4$, it actually is a cyclic group of order 4.

The following consequences of Theorem 5 are from the literature.

Corollary 6 (Gross and Rohrlich [3, Theorem 5.3, p. 222]). *If $D = 1 - 4N^n$ is a squarefree negative integer with $N > 1$ and n prime, then $n \mid h_D$.*

Corollary 7 (Cowles [2]). *If $D = t^2 - 4N^n$ is a negative squarefree integer with $t \geq 1$, $N > 1$, $n > 1$, and*

$$t^2 \leq 4N^{n-1}(N - 1), \quad (7)$$

then $n \mid h_D$.

Proof. The inequality forces $N((t + \sqrt{D})/2) < N(\omega_D)^2$, so as in the proof of Theorem 5, $n \mid h_D$.

Remark 4. The bound given in Corollary 7 can be sharpened. What is at stake here is that $m = 0$ and we want to ensure that $N((t + \sqrt{D})/2) < N(\omega_D)^2$. This is given precision when

$$t < 2N^{n/2} - 1. \quad (8)$$

This is the sharpest bound possible, so Inequality (8) should replace Inequality (7) to give the most precise bound.

Observe that when $N((t + \sqrt{D})/2) < N(\omega_D)^2$, it must be the case that Condition (6) holds, so the hypothesis of Theorem 5 is always satisfied.

The following illustrates how “tight” the conditions in Theorem 5 happen to be, and just how sharp the bound in Remark 4 happens to be as well.

Example 8. Let $D = -499 = 249^2 - 4 \cdot 5^6 = t^2 - 4N^n = t^2 - 4r$, where

$m = 0$, and $2m + t = t = 249 = 2N^{n/2} - 1$, which negates the hypothesis of Theorem 5 with $n = 6$, and indeed $h_{-499} = 3$. Note that $125^2 = ((1 - D)/4)^2 = N^n = 5^6$. In other words, $N((2m + t)/2) = N(\omega_\Delta)^2$, just violating Theorem 3 at the borderline. This also shows that Inequality (8) in Remark 4 is exact.

However, if we view this differently and take $r = 25^3$ with $n = 3$, $N = 25$, and $m = 0$, then $249 = 2m + t = \lfloor 2N^{n/2} \rfloor - 1 = \lfloor 2 \cdot 25^{3/2} \rfloor - 1$, and the hypothesis of Theorem 5 holds with $n = 3$. This illustrates and explains more fully the result we found in [5, Theorem 3.1.1, p. 67], of which Theorems 4-5 are generalizations.

Example 9. If $D = -1967 = 3^2 - 4 \cdot 494 = t^2 - 4r$, with

$$N^n = 2^9 = 3^2 + 3 \cdot 3 + 494 = m^2 + mt + r.$$

Since $2m + t = 9 \neq 45 = \lfloor 2 \cdot 2^{9/2} \rfloor$, $C_\Delta = C_{-1967}$ has a cyclic subgroup of order 9. In fact, $h_\Delta = 36$.

The above illustrates the odd case. The following illustrates the necessity of the conditions in Theorem 5 in the odd case.

Example 10. If $D = -19 = 559^2 - 4 \cdot 5^7 = t^2 - 4r = t^2 - 4N^n$, then $t = 559$, $m = 0$, and $2m + t = t = 559 = \lfloor 2N^{n/2} \rfloor$, so the hypothesis of Theorem 5 fails. Indeed $h_\Delta = h_{-19} = 1$.

Remark 5. Example 10 is one exception of two in the case $D \equiv 5 \pmod{8}$ given in [1]. Below we cite the pertinent results pertaining to the above and present each of the examples as illustrations of our results. It is worth remarking that in [8], we gave two counterexamples, one from this author and one from another, to the main result in [1] and discussed the fact that they were the only two, and why. We will remark on these facts below as well. In fact, [8] was the genesis for the work in this paper.

Corollary 8. *If $D = x^2 - 4N^p \equiv 5 \pmod{8}$ is a negative squarefree integer, where $p > 3$ is prime $x \geq 1$, $N \geq 2$, then $p \mid h_D$ except when*

$D = -11$, $N = 3$ and $p = 5$; or $D = -19$, $N = 5$ and $p = 7$.

Proof. See [1, Corollary 7, p. 62].

Example 11. If $D = -11 = 31^2 - 4 \cdot 3^5 = t^2 - 4N^n$, then $m = 0$, and $2m + t = 31 = \lfloor 2N^{n/2} \rfloor$, so the hypothesis of Theorem 5 fails. In fact, $h_\Delta = h_{-11} = 1$.

Corollary 9. *If $D = x^2 - 4N^p \equiv 1 \pmod{8}$ is a negative squarefree integer with $p > 2$ prime, $x \geq 1$ and $N \geq 2$, then $p \mid h_\Delta = h_D$ except when $D = -7$, $N = 2$, and $p \in \{3, 5, 13\}$.*

Proof. See [1, Corollary 7, p. 62].

Example 12. If $D = -7 = t^2 - 4r$, where $N^n = 2^n = m^2 + mt + r$, and $(t, n, m, r) \in \{(1, 3, 2, 2), (5, 5, 3, 8), (181, 13, 0, 8192)\}$, then in each case we have: $2m + t = \lfloor 2N^{n/2} \rfloor$. Hence, the hypothesis of Theorem 5 fails and indeed $h_{-7} = 1$. Note that $t^2 + 7 = 2^n$ is the celebrated Ramanujan-Nagell equation.

Example 12 is related to the results in [8]. Therein we looked at the results of [1] in a new light as mentioned in Remark 5. For instance, $\mathbb{Q}(\sqrt{4k^n - 1}) = \mathbb{Q}(\sqrt{4k - 1})$ if and only, if $(4k^n - 1)/(4k - 1) = x^2$ for some $x \in \mathbb{Q}$. In [8], we demonstrated that for $n > 1$, the only integral value of x is $x = 3$, for which we get $\mathbb{Q}(\sqrt{63}) = \mathbb{Q}(\sqrt{7})$, with $n = 4$ and $k = 2$. This leads us to a similar equation, equation $x^2 = (7^n - 1)/(7 - 1)$ which is also written as $6x^2 + 1 = 7$. It is the solutions to this equation for which we found a counterexample in [8] to the main result in [1], which in turn led us to this paper.

As mentioned earlier, the results herein may be generalized to non-maximal orders. This is a good place to demonstrate this with an example related to the above. If $D = -63 = 1^2 - 4 \cdot 2^4 = t^2 - 4N^n$, with $m = 0$, then $2m + t = t = 1 \neq 2 \cdot 4^2 - 1 = 2N^{n/2} - 1$, so $\mathcal{C}_\Delta = \mathcal{C}_{-63}$ has a cyclic

subgroup of order 4. Indeed, C_Δ is a cyclic group of order 4.

Now we turn to necessary and sufficient conditions for the class group to have an element of a given order.

Theorem 6. *If $D = t^2 - r \not\equiv 1 \pmod{4}$ is a squarefree negative integer with $t \geq 1$, $r \geq 1$, and let $n > 1$ be an integer. Then the following are equivalent.*

(1) C_{4D} has a cyclic subgroup of order n generated by $I = [N, b + \sqrt{D}]$, where $|b| < \lfloor N^{n/2} \rfloor$ when n is odd.

(2) There exist integers $m \geq 0$, and $N > 1$ with $N^n = 4m^2 - 4mt + r$, where $|2m - t| \neq \lfloor N^{n/2} \rfloor$ when n is odd.

Proof. By Theorem 4, part 2 implies part 1. If part 1 holds, then we set $m = (t + b)/2$. This is an integer since we may use Theorem 2 to replace b by an appropriate integer if not. To see this, assume that b is even and t is odd. Then N is odd since D is squarefree. Therefore, we may replace b by $b \pm N$ which is odd. If b is odd and t is even, then N is odd since, if N is even, then r is odd so $r \equiv 1 \pmod{4}$ since $D \not\equiv 1 \pmod{4}$. Thus, $0 \equiv N^n \equiv b^2 - t^2 + r \equiv 1 - 0 + 1 \pmod{4}$ a contradiction. Hence, we may replace b by $b \pm N$ which is even.

With the above choice of m , $N^n = 4m^2 - 4mt + r$, and $|2m - t| \neq \lfloor N^{n/2} \rfloor$ when n is odd given the restriction on b .

In a similar fashion, we get the following criterion.

Theorem 7. *If $D = t^2 - 4r \equiv 1 \pmod{4}$ is a squarefree negative integer with $t \geq 1$, $r \geq 1$, and let $n > 1$ be an integer. Then the following are equivalent.*

(1) C_D has a cyclic subgroup of order n generated by $I = [N, (b + \sqrt{D})/2]$,

where $|b| < \lfloor 2N^{n/2} \rfloor$ when n is odd and $|b| < \lfloor 2N^{n/2} \rfloor - 1$ when n is even.

(2) There exist integers $m \geq 0$, and $N > 1$ with $N^n = m^2 + mt + r$, where $|2m + t| \neq \lfloor 2N^{n/2} \rfloor$ when n is odd, and $2m + t \neq 2N^{n/2} - 1$ when n is even.

We conclude with the observation that we may achieve analogous criteria for real quadratic orders using the ideas in [7].

Acknowledgement

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

References

- [1] Y. Bugeaud and N. Shorey, On the number of solutions of the generalized Ramanujan-Nagell equation, *J. Reine Angew. Math.* 539 (2001), 55-74.
- [2] M. J. Cowles, On the divisibility of the class number of imaginary quadratic fields, *J. Number Theory* 12 (1980), 113-115.
- [3] B. H. Gross and D. E. Rohrlich, Some results on the Mordell-Weil group of the Jacobian of a Fermat curve, *Invent. Math.* 44 (1978), 201-224.
- [4] R. A. Mollin, Diophantine equations and class numbers, *J. Number Theory* 24 (1986), 7-19.
- [5] R. A. Mollin, *Quadratics*, CRC Press, Boca Raton, New York, London, Tokyo, 1995.
- [6] R. A. Mollin, *Fundamental Number Theory with Applications*, CRC Press, Boca Raton, New York, London, Tokyo, 1997.
- [7] R. A. Mollin, Cyclic subgroups of ideal class groups in real quadratic orders, *Glasgow Math. J.* 41 (1999), 197-206.
- [8] R. A. Mollin, A note on the Diophantine equation $D_1x^2 + D_2 = ak^n$, *Acta Math. Acad., Paedagogicae Nyiregyháziensis*, to appear.
- [9] M. R. Murty, The ABC conjecture and exponents of class quadratic fields, *Contemporary Math.* 210 (1998), 85-95.

