

CLASS NUMBERS OF REAL QUADRATIC ORDERS, GENERALIZED FERMAT NUMBERS, AND EXPONENTIAL DIOPHANTINE EQUATIONS

R. A. MOLLIN

Department of Mathematics and Statistics
University of Calgary
Calgary, Alberta
Canada, T2N 1N4
e-mail: ramollin@math.ucalgary.ca

Abstract

We examine criteria for the existence of cyclic subgroups of the class groups of arbitrary real quadratic orders via the solvability of certain exponential Diophantine equations. This extends numerous results in the literature including past work by this author over the past 25 years.

1. Introduction

Numerous authors have looked at the notion of divisibility of the class numbers of real quadratic fields via the form of the underlying discriminant. This includes, Ankeny and Chowla, [1], Ankeny, Chowla, and Hasse [2], Cao and Dong [3], Chowla and Friedlander [4], Lang [5], Le [6], Lu [7], Takeuchi [20], Yamaguchi [21], Yuan [22], and this author [9]-[13], [16], [19], to name a few. Much of this is summarized and covered in detail in [14]. We propose to provide more general results that yield much of the above as consequences.

2000 Mathematics Subject Classification: Primary 11R29, 11D09, 11R11, 11R65.

Keywords and phrases: Diophantine equations, continued fractions, class numbers, Fermat numbers, Mersenne numbers, quadratic orders.

Received May 15, 2007

Initially, we examine the class groups of real quadratic orders, not necessarily squarefree, whose radicand is of the form $D = b^{2q^n} + 1$ for positive integers b, q, n — see Theorem 3.1. This form of D is a generalization of the renowned Fermat numbers, which are covered by the case $b = q = 2$. Indeed, the $n+1$ -th Fermat number is given by $\mathcal{F}_{n+1} = 2^{2^{n+1}} + 1$. Typically, in the literature, a generalized Fermat number is considered to be of the form $b^{2^n} + 1$ for a given positive integer b . However, our more general approach allows us to say a substantial amount about the existence of certain cyclic subgroups in the class group of the quadratic order. We also examine discriminants of the form $a^{2b} \pm 4$ and $a^{2b} - 1$, which covers all the possibilities since we are not assuming squarefreeness of the discriminants.

2. Notation and Preliminaries

Let $D = D_0 f_D^2 \equiv 0, 1 \pmod{4}$, where $D_0 \neq 1$ is a squarefree integer and f_D is the *conductor* of the *discriminant* D . Here D_0 is called the *fundamental* or *field* discriminant associated with the discriminant D . When $D \equiv 0 \pmod{4}$, then $D/4$ is called the *radicand* associated with D , and when $D \equiv 1 \pmod{4}$, then the discriminant D itself is also called the radicand. In simple terms, this says that the radicand is D/σ^2 , where

$$\sigma = \begin{cases} 1 & \text{if } D \equiv 1 \pmod{4} \\ 2 & \text{if } D \equiv 0 \pmod{4}. \end{cases}$$

The notation given for a \mathbb{Z} -module is

$$[\alpha, \beta] = \{\alpha x + \beta y : x, y \in \mathbb{Z}, \text{ and } \alpha, \beta \in \mathbb{Q}(\sqrt{D}) = \mathbb{Q}(\sqrt{D_0})\}.$$

In particular,

$$\mathcal{O}_D = \begin{cases} [1, \sqrt{D}] & \text{if } D \equiv 0 \pmod{4} \\ [1, (1 + \sqrt{D})/2] & \text{if } D \not\equiv 0 \pmod{4}. \end{cases}$$

is a quadratic *order* in $\mathbb{Q}(\sqrt{D})$. Also, the conductor, given above, is also defined by the index $f_D = |\mathcal{O}_D : \mathcal{O}_{D_0}|$. When $f_D = 1$, then \mathcal{O}_D is the ring of integers or *maximal order* of $\mathbb{Q}(\sqrt{D})$. The ideal *class group* for a given quadratic order of discriminant D is denoted by \mathcal{C}_D . The order of \mathcal{C}_D , or *class number* of \mathcal{O}_D , is denoted by $h_D = |\mathcal{O}_D|$. A class number formula that we shall use in the next section for a quadratic order is given as follows, where the reader may see [14] for more detail and background material.

$$h_D = h_{D_0} \psi_{D_0}(f_D)/u, \tag{2.1}$$

where

$$\psi_{D_0}(f_D) = f_D \prod_{p|f_D} \left(1 - \frac{(D_0/p)}{p}\right),$$

with (D_0/p) being the Kronecker symbol, and the product ranging over all distinct prime divisors of f_D . Moreover, u is the *unit index* of \mathcal{O}_{D_0} in \mathcal{O}_D , namely $\varepsilon_D = \varepsilon_{D_0}^u$, where ε_D is the fundamental unit of \mathcal{O}_D and ε_{D_0} is the fundamental unit of the maximal order \mathcal{O}_{D_0} , whose class number is h_{D_0} .

Furthermore, we need the following important observation. If I is a primitive \mathcal{O}_D ideal of order s in \mathcal{C}_D , with norm relatively prime to the conductor, namely $\gcd(N(I), f_D) = 1$, and with

$$\gcd(s, \psi_{D_0}(f_D)/u) = 1, \tag{2.2}$$

then $s|h_D$.

Now we present results achieved in earlier work that we can exploit in different fashion than previously employed. Note that the following four results cover all possible quadratic orders since we do not restrict to the field case.

Theorem 2.1. Let $D/\sigma^2 = t^2 + 1$, $t \in \mathbb{N}$, be a radicand with discriminant D , and assume that there exist integers $r > 1$, $s > 1$, $m \in \mathbb{N}$, with $t \notin \{2m, 2m - 2\}$, and

$$r^s = \begin{cases} 4mt - 4m^2 + 1 & \text{if } D \not\equiv 1 \pmod{4} \\ m(t+1) - m^2 - t/2 & \text{if } D \equiv 1 \pmod{4}. \end{cases}$$

Furthermore, assume that $\gcd(f_D, r) = 1$. Then \mathcal{C}_D has a cyclic subgroup of order s . Also, if Equation (2.2) holds, then $s \mid h_{D_0}$.

Proof. See [16, Theorem 2.1, p. 200]. □

Theorem 2.2. Let $D = t^2 - 1$, $t \in \mathbb{N}$, and assume that there exists a positive integer m such that

$$r^s = 4mt - 4m^2 - 1,$$

for some integers $r > 1$ and $s > 1$. Furthermore, assume that $\gcd(f_D, r) = 1$. Then \mathcal{C}_D has a cyclic subgroup of order s . Also, if Equation (2.2) holds, then $s \mid h_{D_0}$.

Proof. See [16, Theorem 2.3, p. 202]. □

Theorem 2.3. Let $D = t^2 + 4$, be a discriminant, where t is an odd natural number. Assume that there exists a positive integer m such that

$$r^s = mt - m^2 + 1,$$

for some integers $r > 1$ and $s > 1$. Furthermore, assume that $\gcd(f_D, r) = 1$. Then \mathcal{C}_D has a cyclic subgroup of order s . Also, if Equation (2.2) holds, then $s \mid h_{D_0}$.

Proof. See [16, Theorem 2.2, p. 202].

Theorem 2.4. Let $D = t^2 - 4$, be a discriminant, where t is an odd natural number, and assume that there exists a positive integer m such that

$$r^s = mt - m^2 - 1,$$

for some integers $r > 1$ and $s > 1$. Furthermore, assume that $\gcd(f_D, r) = 1$. Then \mathcal{C}_D has a cyclic subgroup of order s . Also, if Equation (2.2) holds, then $s | h_{D_0}$.

Proof. See [16, Theorem 2.4, p. 203]. □

3. Class Numbers

In what follows the notation from the previous section is in force.

Theorem 3.1. Class Numbers and Generalized Fermat Numbers

Let $b, q \in \mathbb{N}$, $b > 1$, $q > 1$, and let $D/\sigma^2 = (b^{q^n})^2 + 1$ be a radicand. If $\gcd(f_D, q) = 1$, then \mathcal{C}_D has a cyclic subgroup of order

$$s = \begin{cases} 2q^n & \text{if } b \text{ is odd} \\ aq^n - 1 & \text{if } b = 2^a \text{ for some } a \in \mathbb{N}, \text{ and } \sigma = 1. \end{cases}$$

Proof. If b is odd, then $\sigma = 2$, and we invoke Theorem 2.1 with $m = (b^{q^n} + 1)/2$, and $t = b^{q^n}$, to get

$$\begin{aligned} 4mt - 4m^2 + 1 &= 4 \left(\frac{b^{q^n} + 1}{2} \right) b^{q^n} - 4 \left(\frac{b^{q^n} + 1}{2} \right)^2 + 1 \\ &= 4 \left(\frac{b^{q^n} + 1}{2} \right) \left(\frac{b^{q^n} - 1}{2} \right) + 1 = b^{2q^n} = r^s, \end{aligned}$$

so since $\gcd(r, D) = \gcd(b, 4((b^{q^n})^2 + 1)) = 1$, then \mathcal{C}_D has a cyclic subgroup of order $s = 2q^n$.

If $b = 2^a$, and $\sigma = 1$, then set $m = 1$ and $t = b^{q^n}$ in Theorem 2.1. Then

$$m(t + 1) - m^2 - t/2 = b^{q^n} - b^{q^n}/q = b^{q^n}/2 = 2^{aq^n-1} = r^s.$$

Since $\gcd(D, 2) = 1$, \mathcal{C}_D has a cyclic subgroup of order $s = aq^n - 1$. □

Example 3.1. Let $b = 3$, $q = 2$, and $n = 3$, so $D/4 = 3^{16} + 1 = 2 \cdot 21523361$, and C_D has a cyclic subgroup of order 16. In fact, $h_D = h_{172186888} = 2^4 \cdot 5 \cdot 11$.

Example 3.2. Let $b = q = 3$ and $n = 2$ in Theorem 3.1, so

$$D/4 = 3^{2 \cdot 3^2} + 1 = 387420490 = 2 \cdot 5 \cdot 73 \cdot 530713.$$

Then \mathcal{C}_D has a cyclic subgroup of order 18 since $2q^n = 18$ and $D/4 = D_0/4$ is squarefree. In fact, $h_D = h_{1549681960} = 2520 = 2^3 \cdot 3^2 \cdot 5 \cdot 7$.

Corollary 3.1. *In Theorem 3.1, suppose that $b = 2$, and q is a quadratic residue modulo an odd prime $p \nmid q$, and $n = (p-1)/2$. Then for the discriminant $D = 2^{2q^{(p-1)/2}} + 1$, \mathcal{C}_D has a cyclic subgroup of order p .*

Proof. With the given values $s = q^{(p-1)/2} - 1$ so by Euler's criterion for quadratic residues, for instance, see [15, Corollary 4.1.1, p. 186], $p \mid s$, and we have the result. \square

Example 3.3. Let $2^a = b$, and $4^1 = q^n$, and $D = (4^4)^2 + 1 = 65537$. Then \mathcal{C}_D has a cyclic subgroup of order $7 = 4 \cdot 2 - 1 = 2^{an} \cdot a - 1$, by Theorem 3.1. In this case, $D = \mathcal{F}_4$ is the fourth Fermat number. In fact, $h_{\mathcal{F}_4} = 21$. Another way to look at this is via Corollary 3.1, where we have $q = b = 2$ and $n = 3 = (7-1)/2$, so $p = 7$ divides h_D .

Corollary 3.2. Fermat Numbers and Class Numbers

If $\mathcal{F}_{n+1} = (2^{2^n})^2 + 1$, for $n \in \mathbb{N}$, then $\mathcal{C}_{\mathcal{F}_{n+1}}$ has a cyclic subgroup of order $2^n - 1$.

Proof. Take $q = 2 = b$ in Theorem 3.1 and we have the result. \square

Example 3.4. Since $\mathcal{F}_3 = 257$, $\mathcal{C}_{\mathcal{F}_3}$ has a cyclic subgroup of order 3. Indeed, $\mathcal{C}_{\mathcal{F}_3}$ is a cyclic group of order 3.

Remark 3.1. It is an open question as to whether Fermat numbers are squarefree. No such numbers have been found that are *not* squarefree and the consensus is that they are all squarefree. However, in the absence of a proof, the above is the most general result possible. On the other hand, we might hope to use Theorem 2.2 for Mersenne numbers, but problems arise with the conductor that prevent this. Mersenne numbers are not necessarily squarefree. For instance, $\mathcal{M}_6 = 2^6 - 1 = 3^2 \cdot 7 = f_{\mathcal{M}_6}^2 D_0$. Moreover, $3^3 = 4 \cdot 2^3 - 4 - 1$, so with $m = 1$, $r = 3 = s$, we have an exponential equation that seems to satisfy Theorem 2.2. However, the problem is that $\gcd(f_{\mathcal{M}_6}, 3) = 3$, so Theorem 2.2 does not apply. Indeed, we have that $h_{\mathcal{M}_6} = 2$.

Corollary 3.3. *If $n = 2^s$ for some $s \in \mathbb{N}$ in Theorem 3.1 and $\mathcal{F}_0 = 3$, then*

$$\prod_{j=0}^{s-1} \mathcal{F}_j \mid h_{\mathcal{F}_{2^s+1}}.$$

Proof. This follows from Theorem 3.1, and the elementary number theory fact that

$$\prod_{j=0}^{s-1} \mathcal{F}_j = \mathcal{F}_s - 2 = 2^{2^s} - 1,$$

(for instance, see [15, Exercise 2.2.8(d), pp. 88-89].) □

Example 3.5. For $\mathcal{F}_5 = 641 \cdot 6700417$, we have that $h_{\mathcal{F}_5} = 4320 = 2^5 \cdot 3^3 \cdot 5$, and $\prod_{j=0}^1 \mathcal{F}_j = \mathcal{F}_0 \mathcal{F}_1 = 3 \cdot 5$, which is a divisor of $h_{\mathcal{F}_5}$.

The following is an illustration of the even case in Theorem 3.1 where D is *not* a Fermat number.

Example 3.6. Let $q = 8 = b = 2^a$, and $n = 1$ in Theorem 3.1. Then $D = 8^{16} + 1 = 193 \cdot 65537 \cdot 22253377$ and $s = 2^3 3 - 1 = 23$ so \mathcal{C}_D has a cyclic subgroup of order 23.

Other results similar to Theorem 3.1, but not of generalized Fermat type are as follows, which are easily obtained via our methods.

Theorem 3.2 (Lu [7]). *Let $a, b \in \mathbb{N}$ with $a > 1$ and $b > 1$. Then for a discriminant $D = (2a^b)^2 + 1$, \mathcal{C}_D has a cyclic subgroup of order b .*

Proof. Let $m = 1$ and $t = 2a^b$ in Theorem 2.1. Then

$$m(t+1) - m^2 - t/2 = a^b,$$

and the result follows. \square

Integers of the form $b^n \pm 1$ are of interest since they play a role in generating pseudorandom numbers, as well as their significance in abstract algebra, and number theory. Indeed, finding such factorizations is the Cunningham project, which has relationship to some cryptographic applications (see [17] or [18] for instance). We have shown how the orders generated by such numbers have class numbers whose divisors may be found in certain cases. Now we look at analogues using Theorems 2.3-2.4.

Theorem 3.3. *Let $D = a^{2b} + 4$, where $a, b \in \mathbb{N}$ with a odd be a discriminant. Then \mathcal{C}_D has a cyclic subgroup of order b .*

Proof. Let $m = 1$, $r = a$, $s = b$, and $t = a^b$ in Theorem 2.3 to get the result. \square

Example 3.7. Let $D = 3^8 + 4 = 5 \cdot 13 \cdot 101$. Then $h_D = 8$ and \mathcal{C}_D is a cyclic group of order 8. Also, if $D = 5^6 + 4 = 15629$, a prime, then $h_D = 9$, and \mathcal{C}_D has a cyclic subgroup of order 3.

The following looks at more cases where the form of the radicand affects the class number.

Theorem 3.4. *Let $a > 1$ be an odd integer, with $\gcd(a, 3) = 1$, and let $b > 1$ such that $a^b \equiv 1 \pmod{4}$. Then $D = ((a^b + 5)/2)^2 - 4$ is a discriminant, and \mathcal{C}_D has a cyclic subgroup of order b .*

Proof. Let $m = 2$, $r = a$, $s = b$, and $t = (a^b + 5)/2$ in Theorem 2.4 to get the result. Notice that $\gcd(D, a) = 1$, since if an odd prime p divides $\gcd(D, a)$, then $p = 3$, contradicting the hypothesis. Thus, $\gcd(f_D, a) = 1$. \square

Example 3.8. Let $a = 7$ and $b = 6$, so

$$D = \left(\frac{7^6 + 5}{2} \right)^2 - 4 = 3460615925 = 5^2 \cdot 13 \cdot 89 \cdot 181 \cdot 661.$$

By Theorem \mathcal{C}_D has a cyclic subgroup of order 6. In fact, $h_D = 1152 = 2^7 \cdot 3^2$.

Acknowledgement

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

References

- [1] N. C. Ankeny and S. Chowla, On the divisibility of the class number of quadratic fields, *Pacific J. Math.* 5 (1955), 321-324.
- [2] N. C. Ankeny, S. Chowla and H. Hasse, On the class number of the maximal real subfield of a cyclotomic field, *J. Reine Angew. Math.* 217 (1965), 217-220.
- [3] Z. Cao and X. Dong, Diophantine equations and class numbers of real quadratic fields, *Acta Arith.* 47 (2001), 313-328.
- [4] S. Chowla and J. Friedlander, Class numbers and quadratic residues, *Glasgow Math. J.* 17 (1976), 47-52.
- [5] S. D. Lang, Note on the class-number of the maximal real subfield of a cyclotomic field, *J. Reine Angew. Math.* 290 (1977), 70-72.
- [6] M. H. Le, Divisibility of the class number of the real quadratic field $\mathbb{Q}(\sqrt{(1 + 4k^{2n})/a^2})$, *Acta Math. Sinica* 33 (1990), 565-574.

- [7] H. W. Lu, The divisibility of the class number of some real quadratic fields, *Acta Math. Sinica* 28 (1985), 756-762.
- [8] R. A. Mollin, Class numbers and a generalized Fermat theorem, *J. Number Theory* 16 (1983), 420-429.
- [9] R. A. Mollin, Diophantine equations and class numbers, *J. Number Theory* 24 (1986), 7-19.
- [10] R. A. Mollin, Class numbers of quadratic fields determined by Diophantine equations, *Math. Comp.* 48 (1987), 233-242.
- [11] R. A. Mollin, 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 (1987), 39-47.
- [12] R. A. Mollin, Ambiguous classes in quadratic fields, *Math. Comp.* 61 (1993), 355-360.
- [13] R. A. Mollin, Quadratic residue covers for certain real quadratic fields, *Math. Comp.* 62 (1994), 885-897.
- [14] R. A. Mollin, *Quadratics*, CRC Press, Boca Raton, New York, London, Tokyo, 1996.
- [15] R. A. Mollin, *Fundamental Number Theory with Applications*, CRC Press, Boca Raton, New York, London, Tokyo, 1998.
- [16] R. A. Mollin, Cyclic subgroups of ideal class groups in real quadratic orders, *Glasgow Math. J.* (1999) 197-206.
- [17] R. A. Mollin, *Codes — The Guide to Secrecy from Ancient to Modern Times*, CRC Press, Boca Raton, New York, London, Tokyo, 2005.
- [18] R. A. Mollin, *An Introduction to Cryptography, Second Edition*, CRC Press, Boca Raton, New York, London, Tokyo, 2006.
- [19] R. A. Mollin and H. C. Williams, Lower bounds for class numbers of real quadratic and biquadratic fields, *Proc. Amer. Math. Soc.* 101 (1987), 179-187.
- [20] H. Takeuchi, On the class number of the maximal real subfield of a cyclotomic field, *Canad. J. Math.* 33 (1981), 55-58.
- [21] I. Yamaguchi, On the class-number of the maximal real subfield of a cyclotomic field, *J. Reine Angew. Math.* 272 (1975), 217-220.
- [22] P. Z. Yuan, The divisibility of the class numbers of real quadratic fields, *Acta Math. Sinica* 41 (1998), 525-530.