Discussiones Mathematicae
General Algebra and Applications 20 (2000) 199–206

DIOPHANTINE EQUATIONS AND CLASS NUMBERS OF IMAGINARY QUADRATIC FIELDS

Zhenfu Cao and Xiaolei Dong*
Department of Mathematics, Harbin Institute of Technology
Harbin 150001, P. R. China
e-mail: zfcao@hope.hit.edu.cn

Abstract

Let $A, D, K, k \in \mathbb{N}$ with D square free and $2 \nmid k, B = 1, 2$ or 4 and $\mu_i \in \{-1, 1\} (i = 1, 2)$, and let $h(-2^{1-e}D) (e = 0$ or $1)$ denote the class number of the imaginary quadratic field $\mathbb{Q}(\sqrt{-2^{1-e}D})$. In this paper, we give the all-positive integer solutions of the Diophantine equation $Ax^2 + \mu_1 B = K\big((Ay^2 + \mu_2 B)/K\big)^n, 2 \nmid n, n > 1$ and we prove that if $D > 1$, then $h(-2^{1-e}D) \equiv 0 (\mathrm{mod}\ n)$, where D, and n satisfy $k^n - 2^{e+1} = Dx^2, x \in \mathbb{N}, 2 \nmid n, n > 1$. The results are valuable for the realization of quadratic field cryptosystem.

Keywords: Diophantine equation, imaginary quadratic field, class number, cryptographic problem.

1991 Mathematics Subject Classification: 11D41, 11R11, 11R29, 94A60.

1. Introduction

Let $\mathbb{Z}$, $\mathbb{N}$, $\mathbb{Q}$ be the sets of integers, positive integers and rational numbers, respectively. Let $A, K \in \mathbb{N}, B = 1, 2$ or 4, $\mu_i \in \{-1, 1\} (i = 1, 2)$ and throughout this paper, we assume that if $p^a \| K$ for each prime divisor $p \mid K$, then $a < n$. We study the positive integer solutions of the Diophantine equation

$$Ax^2 + \mu_1 B = K((Ay^2 + \mu_2 B)/K)^n, \text{ where } 2 \nmid n, \ n > 1. \tag{1.1}$$

*Supported by the National Natural Science Foundation of China and the Heilongjiang Provincial Natural Science Foundation

In 1979, K. Inkeri in [9] proved that if $k > 2$, then the equation $2y^2 = 7^k + 1$ has no positive integer solution. In 1987, we proved in [2] and [3] that the equation $Dy^2 = (Dx^2 + 1)^k - 1$, for $k > 2, D \in \mathbb{N}$, has only positive integer solutions $(x, y, D, k) = (1, 11, 2, 5)$ and $(1, 20, 6, 4)$, and the equation $Dy^2 = (Dx^2 - 1)^k + 1, k > 1, D \in \mathbb{N}$ has only positive integer solutions $(x, y, D, k) = (1, 1, 2, k)$ and $(2, 5, 2, 2)$.

Clearly, the equations $Dy^2 = (Dx^2 + 1)^k - 1$ and $Dy^2 = (Dx^2 - 1)^k + 1$ is a special case of (1.1) when $A = D, \mu_1 = \mu_2, B = 1, K = 1$ respectively.

In this paper, we first prove a general result on equation (1.1). Next using the general result, we provide results on the divisibility of the class number of imaginary quadratic fields. Let $D \in \mathbb{N}$ be square free, and let $h(-2^{1-e}D)(e = 0 \text{ or } 1)$ denote the class number of the imaginary quadratic field $\mathbb{Q}(\sqrt{-2^{1-e}D})$. Furthermore, let $k, n \in \mathbb{N}$ with $2 \nmid kn, k > 1, n > 1$, and

$$k^n - 2^{e+1} = Dx^2, \ x \in \mathbb{N}.$$

We prove that if $D > 1$, then

$$h(-2^{1-e}D) \equiv 0 (\text{mod } n). \tag{1.2}$$

In 1996, a result of R.A. Mollin shows in [12] only that if $x = 1$ then (1.2) holds.

Let $s = 0, 1, 2$ and $y \in \mathbb{N}$ with $2 \nmid y$ when $s = 0$ or 1. If $x, n \in \mathbb{N}$ satisfy

$$2^s y^n - 1 = Dx^2 (s = 0, 1, 2), \ y > 1, 2 \nmid n, n > 1, \tag{1.3}$$

then $h(-D) \equiv 0 (\text{mod } n)$, where $h(-D)$ is the class number of imaginary quadratic field $\mathbb{Q}(\sqrt{-D})$. These are a well-known results of Stǿrmer [15] (for $D = 1, s = 1$), Lebesgue [10] (for $D = 1, s = 0$), Nagell [13] (for $s = 0$) and Ljunggren [11] (for $s = 1, 2$) on equation (1.3). We also obtain a general method to proof of the well-known results.

By the way, the results of this paper are also valuable for the realization of quadratic field cryptosystem (see [1]).

2. A kind of Diophantine equations

In this section, we give all positive integer solutions of (1.1) by using some recent results of the generalized Pell's equation. We have

Theorem 2.1. *The Diophantine equation*

$$Ax^2 + \mu_1 = K((Ay^2 + \mu_2)/K)^n, \ 2 \nmid n, \ n > 1 \tag{2.1}$$

has a positive integer solution if and only if $\mu_1 = \mu_2$, *and all positive integer solutions of* (2.1) *satisfy*

(A) $x = y, K = Ay^2 + \mu_2$; *or*

(B) $Ay^2 = 3K - \mu_2,\ K = (3^{(n-3)/2} + \mu_2)/4,$
$x = y(48K^2 - 16\mu_2 K + 1) \cdot 3^{-(n-3)/2},$

where $n > 3, n \equiv \mu_2 (\mathrm{mod}\ 4)$.

Theorem 2.2. *If* $A \neq 2$, *then the Diophantine equation*

$$Ax^2 + 2\mu_1 = K((Ay^2 + 2\mu_2)/K)^n,\ 2 \nmid n,\ n > 1 \tag{2.2}$$

has a positive integer solution if and only if $\mu_1 = \mu_2$, *and all positive integer solutions of* (2.2) *satisfy*

(C) $x = y, K = Ay^2 + 2\mu_2$; *or*

(D) $Ay^2 = 3K - 2\mu_2,\ K = (3^{(n-3)/2} + \mu_2)/2,$
$x = y(12K^2 - 8\mu_2 K + 1) \cdot 3^{-(n-3)/2}$, *where* $n \geq 3$, *and* $n > 3$ *if* $\mu_2 = -1$.

Theorem 2.3. *If* $A \neq 4$, *then all positive integer solutions of the Diophantine equation*

$$Ax^2 + 4\mu_1 = K((Ay^2 + 4\mu_2)/K)^n,\ 2 \nmid n, n > 1 \tag{2.3}$$

satisfy $\mu_1 = 1, \mu_2 = -1, x = 11, y = 3, K = 1, n = 3, A = 1$; *or* $\mu_1 = \mu_2 = 1, x = 11, y = 1, K = 1, n = 3, A = 1$; *or* $\mu_1 = \mu_2$ *and*

(E) $x = y, K = Ay^2 + 4\mu_2$; *or*

(F) $Ay^2 = 3K - 4\mu_2, K = 3^{(n-3)/2} + \mu_2, x = y(3K^2 - 4\mu_2 K + 1) \cdot 3^{-(n-3)/2}$,

where $n \geq 3$, *and* $n > 3$ *if* $\mu_2 = -1$.

From Theorem 2.3, we know that

(I) the equation $Ax^2 + 4\mu = K((Ay^2 - 4\mu)/K)^n (\mu \in \{-1, 1\}, n \text{ odd} > 1)$ has only positive integer solution $\mu = 1, x = 11, y = 3, K = 1, n = 3, A = 1$, and

(II) the equation $Ax^2 + 4 = K((Ay^2 + 4)/K)^n (n \text{ odd} > 1)$ has only positive integer solutions $x = 11, y = 1, K = 1, n = 3, A = 1$; $x = y, K = Ay^2 + 4$, and $x = y(3K^2 - 4K + 1) \cdot 3^{-(n-3)/2}, K = 3^{(n-3)/2} + 1, Ay^2 = 3K - 4$, where $n \geq 3$.

For example, the equation $Ax^2 + 4 = (Ay^2 + 4)^n (n \text{ odd} > 1)$ has only positive integer solution $x = 11, y = 1, n = 3, A = 1$, and the equation $Ax^2 + 4 = 2((Ay^2 + 4)/2)^n (n \text{ odd} > 1)$ has only positive integer solution

$x = 5, y = 1, n = 3, A = 2$, and the equation $Ax^2 + 4 = 3((Ay^2 + 4)/3)^n$ (n odd > 1) has no positive integer solutions, etc.
We need some lemmas to prove our theorems.

Lemma 2.4. *Let ε and Ω be the fundamental solution of Pell's equation $x^2 - Dy^2 = 1$ and $x^2 - Dy^2 = 4$ respectively. Then*

$$\varepsilon = 2st^2 + \mu + 2t\sqrt{D} \text{ if } D = s(st^2 + \mu), s, t \in \mathbb{N}, \mu \in \{-1, 1\};$$

$$\varepsilon = st^2 + \mu + t\sqrt{D} \text{ if } D = s(st^2 + 2\mu), s, t \in \mathbb{N}, \mu \in \{-1, 1\};$$
$$\Omega = st^2 + 2\mu + t\sqrt{D} \text{ 'if } D = s(st^2 + 4\mu), s, t \in \mathbb{N}, \mu \in \{-1, 1\}.$$

Proof. See Z. Cao and A. Grytczuk [7]. The part results of Lemma 2.4 first appeared in the papers by C. Richaud [14] and G. Degert [8]. ∎

Lemma 2.5. *Let $a, b \in \mathbb{N}$. If $u, v \in \mathbb{N}$ satisfy $au^2 - bv^2 = 1$, and $u \mid^* a$ or $v \mid^* b$, where symbol $u \mid^* a$ means that every prime factor of u divides a, then*

$$au^2 + bv^2 + 2uv\sqrt{ab} = \varepsilon \text{ or } \varepsilon^3,$$

where ε is the fundamental solution of Pell's equation $x^2 - aby^2 = 1$.

Proof. See also [16], for an equivalent result by D.T. Walker. Also, Lemma 2.5 follows directly from a general result by Z. Cao in [4]. ∎

Lemma 2.6. *Let $a, b \in \mathbb{N}$ with $a \neq 2$. If $u, v \in \mathbb{N}$ satisfy $au^2 - bv^2 = 2$, and $u \mid^* a$ or $v \mid^* b$, then*

$$\frac{1}{2}(au^2 + bv^2) + uv\sqrt{ab} = \varepsilon \text{ or } \varepsilon^3,$$

where ε is the fundamental solution of Pell's equation $x^2 - aby^2 = 1$.

Proof. See Z. Cao [4]. ∎

Lemma 2.7. *Let $a, b \in \mathbb{N}$ with $a \neq 4$. If $u, v \in \mathbb{N}$ satisfy $au^2 - bv^2 = 4$, and $u \mid^* a$ or $v \mid^* b$, then*

$$\frac{1}{2}(au^2 + bv^2) + uv\sqrt{ab} = \Omega \text{ or } \frac{1}{4}\Omega^3,$$

except $a = 5, b = 1, u = 5, v = 11$, *where* Ω *is the fundamental solution of Pell's equation* $x^2 - aby^2 = 4$.

Proof. See Z. Cao [5]. ∎

Proof of Theorem 2.1. The sufficiency of the theorem is clear. Thus, we prove the necessity. Now we assume that (2.1) has a solution. From (2.1), we know that $K \mid Ay^2 + \mu_2$. Put $(X, Y) = (x, ((Ay^2 + \mu_2)/K)^{(n-1)/2})$. Then (2.1) gives

$$AX^2 - (Ay^2 + \mu_2)Y^2 = -\mu_1. \tag{2.4}$$

Since $Y \mid^* (Ay^2 + \mu_2)$, by (2.4) from Lemma 2.4 and Lemma 2.5, we have

$$AX^2 + (Ay^2 + \mu_2)Y^2 + 2XY\sqrt{A(Ay^2 + \mu_2)} = \varepsilon \quad \text{or} \quad \varepsilon^3, \tag{2.5}$$

$$\varepsilon = 2Ay^2 + \mu_2 + 2y\sqrt{A(Ay^2 + \mu_2)}.$$

We see that (2.5) gives

$$AX^2 + (Ay^2 + \mu_2)Y^2 = 2Ay^2 + \mu_2,\ XY = y, \tag{2.6}$$

or

$$AX^2 + (Ay^2 + \mu_2)Y^2 = (2Ay^2 + \mu_2)((2Ay^2 + \mu_2)^2 + 12Ay^2(Ay^2 + \mu_2)), \tag{2.7}$$

$$XY = y(3(2Ay^2 + \mu_2)^2 + 4Ay^2(Ay^2 + \mu_2)). \tag{2.8}$$

From (2.6) and (2.4), we get

$$2(Ay^2 + \mu_2)Y^2 = 2Ay^2 + \mu_2 + \mu_1,\ XY = y,$$

and so $\mu_1 = \mu_2, Y = 1, X = y$ i.e. $x = y, K = Ay^2 + \mu_2$.
From (2.7) and (2.4), we have

$$\begin{aligned} 2(Ay^2 + \mu_2)Y^2 &= \mu_1 + (2Ay^2 + \mu_2)((2Ay^2 + \mu_2)^2 + 12Ay^2(Ay^2 + \mu_2)) \\ &= \mu_1 + (2Ay^2 + \mu_2)(16A^2y^4 + 16\mu_2 Ay^2 + 1) \\ &= \mu_1 + (2Ay^2 + \mu_2) \cdot 16Ay^2(Ay^2 + \mu_2) + (2Ay^2 + \mu_2) \\ &= (2Ay^2 + \mu_2) \cdot 16Ay^2(Ay^2 + \mu_2) + (2Ay^2 + \mu_2 + \mu_1), \end{aligned}$$

and so $\mu_1 = \mu_2, Y = 4Ay^2 + \mu_2$. Hence

$$((Ay^2 + \mu_2)/K)^{(n-1)/2} = Y = 4Ay^2 + \mu_2 = 4(Ay^2 + \mu_2) - 3\mu_2, \tag{2.9}$$

and so $(Ay^2 + \mu_2)/K \mid 3, (Ay^2 + \mu_2)/K = 3$ since $(Ay^2 + \mu_2)/K = 1$ is impossible. So $Ay^2 = 3K - \mu_2$ and $K = (3^{(n-3)/2} + \mu_2)/4$ by (2.9), and $x = y(48K^2 - 16\mu_2 K + 1) \cdot 3^{-(n-3)/2}$ by (2.8). The theorem is proved. ∎

A proof of Theorem 2.2 and Theorem 2.3 is similar to the process of the proof of Theorem 2.1 by using Lemma 2.6 and Lemma 2.7 respectively, and so the proof is omitted.

3. The class number of imaginary quadratic fields

Let D be a positive integer which is square free, and let $h(-2^{1-e}D)$ ($e = 0$ or 1) denote the class number of the imaginary quadratic field $\mathbb{Q}(\sqrt{-2^{1-e}D})$. Furthermore, let $k, n \in \mathbb{N}$ with $2 \nmid kn, k > 1, n > 1$, and

$$k^n - 2^{e+1} = Dx^2,\ x \in \mathbb{N}. \tag{3.1}$$

We prove the following result.

Theorem 3.1. *If $D > 1$, then $h(-2^{1-e}D) \equiv 0 (\mathrm{mod} n)$.*

From Theorem 3.1, we get that if $D = 3, 5, 7, 11, 15, 17, 21, 33, 35, 39$, or 41, then equation (3.1) has no positive integer solutions.

For the Diophantine equations

$$1 + Dx^2 = 2^s y^n\ (s = 0, 1, 2),\ 2 \nmid n,\ n > 1, \tag{3.2}$$

using the above method, we can give a general new proof of a well-known results by Stømer [15], Lebesgue [10], Nagell [13] and Ljunggren [11] on equation (3.2).

Now, we only give the proof of Theorem 3.1. We need a lemma.

Lemma 3.2. *Let c, d be two square-free positive integers such that $(c, d) = 1$ and let $h(-cd)$ be the class number of the imaginary quadratic field $\mathbb{Q}(\sqrt{-cd})$. Then every integer solution (x, y, z, n) of the equation*

$$cx^2 + dy^2 = z^n,\ (x, y) = 1$$

can be expressed as $z^t = (ca^2 + db^2)/\lambda^2,\ n = n_1 t$,

$$x\sqrt{c} + y\sqrt{-d} = ((a\sqrt{c} + b\sqrt{-d})/\lambda)^{n_1},$$

where

$$t = (n, h(-cd)),\ (a,b) = \begin{cases} 1, & \\ 1 \quad \text{or} \quad 2, & \end{cases} \qquad \lambda = \begin{cases} 1, & \text{if } 3 \nmid n_1, \\ 2, & \text{if } 3 \mid n_1. \end{cases}$$

Proof. It is easy to see from the proof of lemma in [6]. ∎

Proof of Theorem 3.1. Let $(n, h(-2^{1-e}D)) = t$, and let $n = n_1 t$. If $n_1 = 1$, then the theorem is proved. Otherwise, $n_1 > 1$. By Lemma 3.2, we have that all integer solutions of (3.1) satisfy

$$x\sqrt{D} + 2^e\sqrt{-2^{1-e}} = ((a\sqrt{D} + b\sqrt{-2^{1-e}})/\lambda)^{n_1},\ 2 \nmid n_1, \tag{3.3}$$

$$k^t = (Da^2 + 2^{1-e}b^2)/\lambda^2, \tag{3.4}$$

where a, b, t, n_1 and λ are defined in Lemma 3.2. If $3 \mid n_1$, then $\lambda = 2, (a,b) = 1$ or 2. Hence, there exist $a', b' \in \mathbb{Z}$ such that

$$(a'\sqrt{D} + b'\sqrt{-2^{1-e}})/2 = ((a\sqrt{D} + b\sqrt{-2^{1-e}})/2)^{n_1/3},$$

where $(a', b') = 1$ or 2. So (3.3) gives

$$x\sqrt{D} + 2^e\sqrt{-2^{1-e}} = ((a'\sqrt{D} + b'\sqrt{-2^{1-e}})/2)^3, \tag{3.5}$$

and so

$$8x = a'(Da'^2 - 3 \cdot 2^{1-e}b'^2),\ 2^{e+3} = b'(3Da'^2 - 2^{1-e}b'^2). \tag{3.6}$$

Clearly, if $e = 0$, then $2 \mid a',\ 2 \mid b'$, and if $e = 1$ and $2 \nmid b'$, then the second equality of (3.6) is impossible. Therefore, we have $2 \mid a', 2 \mid b'$. Let $a' = 2a'', b' = 2b'', a'', b'' \in \mathbb{Z}$. Then the second equality of (3.6) gives $2^e = b''(3Da''^2 - 2^{1-e}b''^2)$ and so $Da''^2 = 1$, which is a contradiction since $D > 1$.

If $3 \nmid n_1$, then $\lambda = 1$ and $(a,b) = 1$. From (3.3), we get $b \mid 2^e$, and so $b = \pm 2^e$. Therefore, $k^t = Da^2 + 2^{1+e}$ by (3.4). Then by (3.1) we have

$$(Da^2 + 2^{1+e})^{n_1} = Dx^2 + 2^{1+e}. \tag{3.7}$$

By Theorem 2.2 and Theorem 2.3, we easily see that (3.7) gives $D = 1$ and $n_1 = 3$. This contradicts our assumption. The theorem is proved. ∎

References

[1] J. Buchmann and H.C. Williams, *Quadratic fields and cryptography*, p. 9–25 in: "*Number Theory and Cryptography*", University Press, Cambridge 1990.

[2] Z. Cao, *An Erdös conjecture, Pell sequences and Diophantine equations* (Chinese), J. Harbin Inst. Tech. **2** (1987), 122–124.

[3] Z. Cao, *On the equation* $Dx^2 \pm 1 = y^p, xy \neq 0$ (Chinese), J. Math. Res. & Exposition **7** (1987), no. 3, p. 414.

[4] Z. Cao, *On the equation* $ax^m - by^n = 2$ (Chinese), Chinese Sci. Bull. **35** (1990), 558–559.

[5] Z. Cao, *On the Diophantine equation* $(ax^m - 4c)/(abx - 4c) = by^2$ (Chinese), J. Harbin Inst. Tech. **23** (1991), Special Issue, 110–112.

[6] Z. Cao, *The Diophantine equation* $cx^4 + dy^4 = z^p$, C.R. Math. Rep. Acad. Sci. Canada **14** (1992), 231–234.

[7] Z. Cao and A. Grytczuk, *Some classes of Diophantine equations connected with McFarland's and Ma's conjectures*, Discuss. Math. – Algebra and Applications **2** (2000), 193–198.

[8] G. Degert, *Über die Bestimung der Grundeinheit gewisser reell-quadratischer Zahlkorper*, Abh. Math. Sem. Univ. Hamburg **22** (1958), 92–97.

[9] K. Inkeri, *On the diophantine equations* $2y^2 = 7^k + 1$ *and* $x^2 + 11 = 3^n$, Elem. Math. **34** (1979), 119–121.

[10] V.A. Lebesgue, *Sur l'impossibilitéon nombres entiers de l'équation* $x^m = y^2 + 1$, Nouv. Ann. Math. **9** (1850), no. 1, p. 178–181.

[11] W. Ljunggren, *Über die Gleichungen* $1 + Dx^2 = 2y^n$ *und* $1 + Dx^2 = 4y^n$, Norske Vid. Selsk. Forhandl. **15** (30) (1942), 115–118.

[12] R.A. Mollin, *Solutions of Diophantine equations and divisibility of class numbers of complex quadratic fields*, Glasgow Math. J. **38** (1996), 195–197.

[13] T. Nagell, *Sur l'impossibilité de quelques équations à deux indéterminées*, Norsk Matem. Forenings Skr. Serie I **13** (1923), 65–82.

[14] C. Richaud, *Sur la résolution des équations* $x^2 - Ay^2 = \pm 1$, Atti Acad. Pontif. Nuovi Lincei (1866), 177–182.

[15] C. Stφrmer, *Solution compléte en nombres entiers* m, n, x, y, k *de l'équation* $m\text{arctg}1/x + n\text{arctg}1/y = k\pi/4$, Christiania Vid. Selsk. Skr. I, **11** (1895).

[16] D.T. Walker, *On the Diophantina equation* $mx^2 - ny^2 = \pm 1$, Amer. Math. Monthly **74** (1967), 504–513.

Received 20 July 1998
Revised 30 October 2000