Annali di Matematica (2010) 189:679–687
DOI 10.1007/s10231-010-0131-8

On Diophantine equation $3a^2x^4 - By^2 = 1$

Debiao He · Jianhua Chen · Yu Wang

Received: 26 August 2009 / Accepted: 1 February 2010 / Published online: 19 February 2010

Abstract Bumby proved that the only positive solutions to the quartic Diophantine equation $3x^4 - 2y^2 = 1$ are $(x, y) = (1, 1), (3, 11)$. In this paper, we extend this result and prove that if the class number of the field $\mathrm{Q}(\sqrt{1-3a^2})$ is not divisible by 2, the equation $3a^2x^4 - By^2 = 1$ has at most two solutions. However, both solutions occur in only one case, $a = 1, b = 2$, as solved by Bumby. The proof utilizes the law of quadratic reciprocity that seems very rare in solving Diophantine equations, and the solution will be also obtained effectively through the proof when it exists.

Keywords Diophantine equation · Quadratic reciprocity law

Mathematics Subject Classification (2000) 11D72

1 Introduction

Let A, B be integers, the Diophantine equation

$$Ax^4 - By^2 = 1 \tag{1}$$

has been studied in great detail by many people. For the general case, there is a long-standing conjecture that (1) has at most two integer solutions. Ljuggren [1] proved that (1) has at most two solutions in some cases by the method of algebraic number theory. From then on, there are many other special cases discussed [3–9]. In 1967, Bumby solved the Diophantine equation $3x^4 - 2y^2 = 1$ [2]. His method applies a clever argument involving arithmetic in the quartic number field $\mathrm{Q}(\sqrt{-2}, \sqrt{-3})$ and has been regarded to be very difficult to extend to other equations in a long period [5]. The purpose of this paper is to extend Bumby's method

D. He (✉) · J. Chen · Y. Wang
School of Mathematics and Statistics, Wuhan University,
430072 Wuhan, Hubei, China
e-mail: hedebiao@163.com

to the family of the Diophantine equations of type

$$3a^2x^4 - By^2 = 1 \tag{2}$$

here, we assume the class number of the field $\mathrm{Q}(\sqrt{1-3a^2})$ is not divisible by 2. (2) includes many interesting special cases such as $12x^4 - 11y^2 = 1$ and $300x^4 - 299y^2 = 1$, which were studied by Bennentt and Walsh [5] through elliptic curve with a mass of complicated computations. In [5], the equation $12x^4 - 11y^2 = 1$ was used to find the integer points on the elliptic curve $dy^2 = x(4x^2 - 3)$ for some d and this result will be extended in this paper. We also observe an interesting phenomenon about the class number of imaginary quadratic fields which suggests that the result in this paper is best possible. The main result of this paper is:

Theorem *Let a, B be positive integers and $\rho = \sqrt{3a^2}u_0 + \sqrt{B}v_0 > 1$ be the least positive solution of equation $3a^2u^2 - Bv^2 = 1$, h be the class number of the field $\mathrm{Q}(\sqrt{1-3a^2})$. Suppose that h is not divisible by 2, then Eq. (2) has at most one solution when $a \geq 1$, $B > 2$, moreover the possible solution is given by $u_0 = x^2$, where x is a rational integer. For $a = 1$, $B = 2$, Eq. (2) has two solutions $(x, y) = (1, 1), (3, 11)$.*

Remark The latter result of the theorem has been proved by Bumby [2]. In this paper, a slightly different approach is presented.

2 Some lemmas and the proof of the theorem

Throughout the paper, we assume $a \geq 1$, $B \geq 2$ are square-free positive integers. At first, we quote an important result from Chen [3] to reduce Eq. (2) to its special case.

Lemma 1 (Chen Jianhua [3]) *Let $\mu = \sqrt{3a^2}u_0 + \sqrt{B}v_0 > 1$ be the least solution of the Pell equation*

$$3a^2u^2 - Bv^2 = 1 \tag{3}$$

If (2) is solvable, then $u_0 = x_0^2$.

Since all the solutions of (3) are given by $u_k\sqrt{3a^2} + v_k\sqrt{B} = (u_0\sqrt{3a^2} + v_0\sqrt{B})^{2k+1} = (\sqrt{3a^2u_0^2} + \sqrt{3a^2u_0^2 - 1})^{2k+1}$. Assume (x_k, y_k) is another solution of (2), then $u_k = x_k^2$ and $u = \frac{u_k}{u_0}$ is a solution of the equation $3a^2u_0^2u^2 - (3a^2u_0^2 - 1)v^2 = 1$. Note that u_0 is a square, then we reduce (2) to its special case:

$$3a^2x^4 - (3a^2 - 1)y^2 = 1. \tag{4}$$

In order to solve the equation of the title, we only need to study Eq.(4) instead.

Throughout this paper, we let $\rho = \sqrt{3a^2} + \sqrt{3a^2 - 1} > 1$ be the least solution of the Pell equation $3a^2u^2 - (3a^2 - 1)v^2 = 1$, and $\theta = \sqrt{-3a^2} + \sqrt{1 - 3a^2}$. Clearly $\theta^2 = -\rho^2$. We have all the solutions of the Pell equation $3a^2u^2 - (3a^2 - 1)v^2 = 1$ are given by

$$U_{2k+1}\sqrt{3a^2} + V_{2k+1}\sqrt{3a^2 - 1} = \rho^{2k+1}, \quad k = 0, \pm1, \pm2, \ldots.$$

thus

$$x^2 = U_{2n-1} = \frac{\rho^{2n} + \rho^{2-2n}}{\rho^2 + 1} = (-1)^n\frac{\theta^{2n} - \theta^{2-2n}}{1 - \theta^2} = (-1)^n\frac{\theta^n - \theta^{1-n}}{1 - \theta}\frac{\theta^n + \theta^{1-n}}{1 + \theta} \tag{5}$$

Table 1 Other calculations about Y_n

Modulo	Y_{6k}	Y_{6k+1}	Y_{6k+2}	Y_{6k+3}	Y_{6k+4}	Y_{6k+5}
$2\sqrt{1-3a^2}-1$	1	1	0	-1	-1	0
$2\sqrt{1-3a^2}+1$	1	1	-2	1	1	-2

The two factors of x^2 we have separated in (5) are both algebraic. Let $Y_n = \frac{\theta^n+\theta^{1-n}}{1+\theta}$ and Y_n' be the conjugate of Y_n in $\mathrm{Z}(\sqrt{1-3a^2})$, a slightly less obvious fact is

Lemma 2 *Y_n is in $\mathrm{Z}(\sqrt{1-3a^2})$ and its conjugate in $\mathrm{Z}(\sqrt{1-3a^2})$ is $Y_n' = (-1)^n\frac{\theta^n-\theta^{1-n}}{1-\theta}$. Moreover, Y_n and Y_n' are coprime.*

Proof From definition of Y_n, and noting that $\theta^{n+2}+\theta^n = \theta^{n+1}(\theta+1/\theta)$ we have

$$Y_0 = Y_1 = 1, \quad Y_{n+2} = 2\sqrt{1-3a^2}Y_{n+1} - Y_n. \tag{6}$$

Thus, it follows that Y_n is in $\mathrm{Z}(\sqrt{1-3a^2})$. It's a also routine matter to verify that the conjugate of Y_n in $\mathrm{Z}(\sqrt{1-3a^2})$ is $Y_n' = (-1)^n\frac{\theta^n-\theta^{1-n}}{1-\theta}$.

Furthermore, since $Y_{n+2}Y_{n+1}' + Y_{n+2}'Y_{n+1} = -(Y_n'Y_{n+1} + Y_nY_{n+1}') = \cdots = \pm(Y_0'Y_1 + Y_1'Y_0) = \pm 2$ and $Norm(Y_n)$ is odd, we get Y_n and Y_n' are coprime.

Other calculations about Y_n which will be required are listed below:

Let h denote the class number of $\mathrm{Q}(\sqrt{1-3a^2})$. If $h \neq 0 (\mathrm{mod}\, 2)$, it follows from (5) $Y_n = \pm\xi^2$, where $\xi = c + d\sqrt{1-3a^2}$ with $c, d \in \mathrm{Z}$. Next, we will prove the main theorem of the paper by determining when $\pm Y_n$ can be a square in $\mathrm{Q}(\sqrt{1-3a^2})$.

Since $Y_n = Y_{1-n}$, we only need to consider even n. We divide the even n into three cases: $n = 6k, 6k+2, 6k+4$. The proof is organized as follows: Lemma 3 proves $-Y_n$cannot be a square for all even n; $Y_{6k+4} = \xi^2$ can be disproved in a similar way as $-Y_n = \xi^2$, which is omitted for brevity; $Y_{6k+2} = \xi^2$ is discussed in Lemma 4; in terms of even a and odd a, $Y_{6k} = \xi^2$ will be dealt with in Lemmas 6 and 7, respectively.

Lemma 3 *If n is even, then $-Y_n$ cannot be a square in the field $\mathrm{Q}(\sqrt{1-3a^2})$.*

Proof Assume that $-Y_n = \xi^2 = (c + d\sqrt{1-3a^2})^2$, where $c, d \in Z$.

(i) $n = 6k$. From Table (1), we have $4(c + d\sqrt{1-3a^2})^2 = -4(\mathrm{mod}\, 2\sqrt{1-3a^2}-1)$, By the fact that $2\sqrt{1-3a^2} \equiv 1(\mathrm{mod}\, 2\sqrt{1-3a^2}-1)$, which implies $(2c+d)^2 = -4(\mathrm{mod}\, 3(1-4a^2))$, we get $1 = (\frac{-4}{3}) = -1$, a contradiction.

(ii) $n = 6k+2$. From Table 1 we have $4(c + d\sqrt{1-3a^2})^2 = 8(\mathrm{mod}\, 2\sqrt{1-3a^2}+1)$, which implies $(2c+d)^2 = 8(\mathrm{mod} 3(1-4a^2))$. So we have $1 = (\frac{8}{3}) = -1$, a contradiction.

(iii) $n = 6k+4$. We have $4(c + d\sqrt{1-3a^2})^2 = -4(\mathrm{mod}\, 2\sqrt{1-3a^2}-1)$ which implies $1 = (\frac{-4}{3}) = -1$, thus it is impossible.

By (i–iii), we prove $-Y_n$ cannot be a square for all even n.

In a similar way, we prove that Y_{6k+4} cannot be a square by taking mod $2\sqrt{1-3a^2}-1$.

Lemma 4 *If Y_{6k+2} is a square in the field $\mathrm{Q}(\sqrt{1-3a^2})$, then a in the Eq. (3) must be 1, and the only two solutions of (2) in this case are (1, 1) and (3, 11).*

Proof Assume $Y_{6k+2} = \xi^2$ where $\xi \in \mathrm{Z}(\sqrt{1-3a^2})$, then we have $Y'_{6k+2} = \xi'^2$ and therefore $Y_{6k+2}Y'_{6k+2} = A^2$ where $A \in \mathrm{Z}$.

Writing $\rho^{4k+1} = u\sqrt{3a^2} + v\sqrt{3a^2-1}$ for brevity, we have

$$\begin{aligned} A^2 &= \frac{\rho^{2(6k+2)-1} + \rho^{1-2(6k+2)}}{\rho + \rho^{-1}} = \frac{\rho^{3(4k+1)} + \rho^{-3(4k+1)}}{\rho + \rho^{-1}} \\ &= \frac{2(3a^2u^3\sqrt{3a^2} + 3(3a^2-1)uv^2\sqrt{3a^2})}{2\sqrt{3a^2}} = 3u(4a^2u^2 - 1) \end{aligned} \tag{7}$$

by the fact that u, v satisfies $3a^2u^2 - (3a^2-1)v^2 = 1$.

Since $(3u, 4a^2u^2 - 1) = 1$ or 3, (7) implies either

$$3u = S^2, \quad 4a^2u^2 - 1 = T^2 \quad \text{when } (3u, 4a^2u^2 - 1) = 1 \tag{8}$$

or

$$3u = 3S^2, \quad 4a^2u^2 - 1 = 3T^2 \quad \text{when } (3u, 4a^2u^2 - 1) = 3 \tag{9}$$

It is obvious that (8) is impossible.

From (9), we have

$$4a^2S^4 - 3T^2 = 1. \tag{10}$$

Applying the result in [3], we get that (10) has one solution only when $2a|2$, thus $a = 1$, and the only solution in this case is $(S, T) = (1, 1)$. Consequently, we find the nontrivial solution of (2) when $a = 1$, $B = 2$.

In order to deal with the case of $Y_{6k} = \xi^2$, we develop some useful sequences in $\mathrm{Z}(\sqrt{1-3a^2})$. Write $\theta^n = f_n + wg_n$, here $w = (-1+\sqrt{-3})/2$ and $f_n, g_n \in \mathrm{Q}(\sqrt{1-3a^2})$. Consequently, we write $f_n = r_n - s_n\sqrt{1-3a^2}$.

Lemma 5 *Let f_n, r_n, s_n be defined as above, then $r_n, s_n \in \mathrm{Z}$ and $(r_n, s_n) = 1$.*

Proof It is easily verified that f_n satisfies:

$$f_0 = 1, \quad f_1 = \sqrt{1-3a^2} + a, \quad f_{n+2} = 2\sqrt{1-3a^2}f_{n+1} - f_n,$$

therefore, f_n is in $\mathrm{Z}(\sqrt{1-3a^2})$ and $r_n, s_n \in \mathrm{Z}$. Since θ is an unit, then $(r_n, s_n) = 1$.

Let $N_n = r_n^2 + (3a^2-1)s_n^2$ be the norm of f_n in $\mathrm{Z}(\sqrt{1-3a^2})$, note that $f_n = \frac{w\theta^n - \theta^{-n}}{w-1}$ and $f'_n = (-1)^n \frac{w\theta^{-n} - \theta^n}{w-1}$ from the definition of f_n, then we have the recurrence of N_m:

$$N_0 = 1; \quad N_1 = 4a^2 - 1; \quad N_{n+2} = 2(6a^2-1)N_{n+1} - N_n + (-1)^n 4a^2; \tag{11}$$

It is also obvious that

$$\begin{aligned} &r_0 = 1; \quad r_1 = a; \quad r_{n+2} = 2(3a^2-1)s_{n+1} - r_n; \\ &s_0 = 0; \quad s_1 = -1; \quad s_{n+2} = -2r_{n+1} - s_n; \end{aligned} \tag{12}$$

Some other calculations about N_n, r_n, s_n will be necessary in the following proof, which are listed as follows:

$$N_{2t+1} \equiv -1 (\mathrm{mod}\ a);$$
$$r_{2t+1} \equiv 0 (\mathrm{mod}\ a); \quad s_{2t+1} \equiv -1 (\mathrm{mod}\ a); \quad M_n \equiv 1 (\mathrm{mod}\ a); \quad P_n \equiv -1 (\mathrm{mod}\ a); \tag{13}$$
$$r_{6t+3} \equiv 0 (\mathrm{mod}\ 2a-1); \quad s_{6t+3} \equiv 2 (\mathrm{mod}\ 2a-1); \quad M_{6t+3} \equiv -1 (\mathrm{mod}\ 2a-1) \tag{14}$$
$$r_{6t+3} \equiv 0 (\mathrm{mod}\ 2a+1); \quad s_{6t+3} \equiv 2 (\mathrm{mod}\ 2a+1); \quad P_{6t+3} \equiv 1 (\mathrm{mod}\ 2a+1) \tag{15}$$

where $M_n = (a-1)s_n + r_n$ and $P_n = (a+1)s_n - r_n$.

Lemma 6 *Suppose $a \equiv 0 (\mathrm{mod}\ 2)$ and $n = 6k$, we have $n = 0$ if Y_n is a square.*

Proof Assume that $n = 6k \neq 0$, then write $n = 2 \cdot 3^b(3k \pm 1)$ with $b > 0$. Let $m = 3^b$, whereby $m \equiv 3 (\mathrm{mod}\ 6)$ and $m \equiv 1 \mathrm{or}\, 3 (\mathrm{mod}\ 4)$.

Moreover for even a, we have

$$\begin{aligned} &N_{2t+1} \equiv -1 (\mathrm{mod}\ 8); \\ &r_{4t+1} \equiv a; \quad r_{4t+3} \equiv -a (\mathrm{mod}\ 8); \quad s_{4t+1} \equiv -1; \quad s_{4t+3} \equiv -1 (\mathrm{mod}\ 8); \\ &M_t \equiv 1 (\mathrm{mod}\ 4); \quad P_t \equiv -1 (\mathrm{mod}\ 4) \end{aligned} \tag{16}$$

By the definition of f_n, we have $\theta^{2n} \equiv w^2 (\mathrm{mod}\ f_n)$, which follows

$$Y_{2m(3k-1)} = \frac{\theta^{2m(3k-1)} + \theta^{1-2m(3k-1)}}{1+\theta} \equiv \frac{w + w^2\theta}{1+\theta} (\mathrm{mod}\ f_m)$$

and

$$Y_{2m(3k+1)} = \frac{\theta^{2m(3k+1)} + \theta^{1-2m(3k+1)}}{1+\theta} \equiv \frac{w^2 + w\theta}{1+\theta} (\mathrm{mod}\ f_m).$$

Write $Y_n = (c + d\sqrt{1-3a^2})^2$ with $c, d \in \mathrm{Z}$, combined with Lemma 5 and that the class number of $\mathrm{Q}(\sqrt{1-3a^2})$ is not divisible by 2, the above two congruences imply respectively:

$$\begin{aligned} &(-2a^2)(cs_m + dr_m)^2 \\ &\quad \equiv (-2a)s_m((a-1)s_m + r_m) (\mathrm{mod}\ (r_m^2 + (3a^2-1)s_m^2) \overset{\Delta}{=} (-2a)s_m M_m (\mathrm{mod}\ N_m) \end{aligned}$$

and

$$\begin{aligned} &(-2a^2)(cs_m - dr_m)^2 \\ &\quad \equiv (-2a)s_m((a+1)s_m - r_m) (\mathrm{mod}\ (r_m^2 + (3a^2-1)s_m^2) \overset{\Delta}{=} (-2a)s_m P_m (\mathrm{mod}\ N_m) \end{aligned}.$$

thus we have

$$\left(\frac{-2as_m M_m}{N_m}\right) = 1 \mathrm{or}\, 0 \tag{17}$$

and

$$\left(\frac{-2as_m P_m}{N_m}\right) = 1 \mathrm{or}\, 0. \tag{18}$$

In order to compute $(\frac{-2as_m M_m}{N_m})$ and $(\frac{-2as_m P_m}{N_m})$, we will repeatedly use the formula $(\frac{m}{|n|})(\frac{n}{|m|}) = (-1)^{\frac{m-1}{2}\frac{n-1}{2}}$ where at least one of m, n is positive and $(m, n) = 1$ [8].

Writing $a = 2^h a_1$, where $h \geq 1$ and a_1 is odd, then we have

$$\left(\frac{-2as_m}{N_m}\right) = \left(\frac{-1}{N_m}\right)\left(\frac{2^{h+1}}{N_m}\right)\left(\frac{a_1}{N_m}\right)\left(\frac{s_m}{N_m}\right) = (-1)^{\frac{a_1-1}{2}}\left(\frac{-1}{a_1}\right)\left(\frac{N_m}{|s_m|}\right) = 1,$$

and

$$\left(\frac{M_m}{N_m}\right) = \left(\frac{2a(2a-1)s_m^2}{|M_m|}\right) = \left(\frac{2^{h+1}}{|M_m|}\right)\left(\frac{a_1}{|M_m|}\right)\left(\frac{2a-1}{|M_m|}\right) = \left(\frac{1}{a_1}\right)\left(\frac{-1}{2a-1}\right) = -1$$

$$\left(\frac{P_m}{N_m}\right) = -\left(\frac{2a(2a+1)s_m^2}{|P_m|}\right) = -\left(\frac{2^{h+1}}{|P_m|}\right)\left(\frac{a_1}{|P_m|}\right)\left(\frac{2a+1}{|P_m|}\right)$$
$$= -(-1)^{\frac{a_1-1}{2}}\left(\frac{-1}{a_1}\right)\left(\frac{1}{2a+1}\right) = -1.$$

It follows at once that $(\frac{-2as_mM_m}{N_m}) = -1$ and $(\frac{-2as_mP_m}{N_m}) = -1$ which imply that neither (17) nor (18) can be established. Thus we proved Lemma 6.

Now we turn to deal with $n = 6k$ for odd a.

Lemma 7 *Suppose $a \equiv 1 (\mathrm{mod}\ 2)$ and $n = 6k$, we have $n = 0$ if Y_n is a square.*

Proof Suppose that $n \neq 0$ We divide $n = 6k$ into $n = 12k + 6$ and $n = 12k$ to complete the proof. We assume that $Y_n = \xi^2 = (c + d\sqrt{1-3a^2})^2$ where $c, d \in \mathrm{Z}$.

(i) $n = 12k + 6$.
From direct calculations, we have $\theta^3 \equiv 2\sqrt{-3a^2} (\mathrm{mod}\ 12a^2 - 1)$, $\theta^6 \equiv -12a^2 \equiv -1 (\mathrm{mod}\ 12a^2 - 1)$ and $\theta^{12} \equiv 1 (\mathrm{mod}\ 12a^2 - 1)$, hence $Y_{n+12} = Y_n (\mathrm{mod}\ (3a + \sqrt{1-3a^2})$ and $Y_{6+12k} \equiv Y_6 \equiv -1 (\mathrm{mod}\ (3a + \sqrt{1-3a^2})$.
Since $Y_{12k+6} = \xi^2 = (c + d\sqrt{1-3a^2})^2$, from above we get $A^2 \equiv -1 (\mathrm{mod}\ 12a^2 - 1)$, for some rational integer A, which is impossible.

(ii) $n = 12k$
Write $n = 4 \cdot 3^b(3k \pm 1)$, $m = 3^b$ whereby $m \equiv 3 (\mathrm{mod}\ 6)$ and $m \equiv 1 \mathrm{or}\ 3 (\mathrm{mod}\ 4)$, then $Y_{4m(3k-1)} = \frac{\theta^{4m(3k-1)} + \theta^{1-4m(3k-1)}}{1+\theta} \equiv \frac{w + w^2\theta}{1+\theta} (\mathrm{mod}\ f_{2m})$
or

$$Y_{4m(3k+1)} = \frac{\theta^{4m(3k+1)} + \theta^{1-4m(3k+1)}}{1+\theta} \equiv \frac{w^2 + w\theta}{1+\theta} (\mathrm{mod}\ f_{2m})$$

and the similar argument shows $(\frac{-2as_{2m}((a-1)s_{2m}+r_{2m})}{N_{2m}}) = 1 \mathrm{or}\ 0$
or $(\frac{-2as_{2m}((a+1)s_{2m}-r_{2m})}{N_{2m}}) = 1 \mathrm{or}\ 0$

Now we calculate the above Jacobi symbols to get a contradiction.
By (11) and (12), for $a \equiv 1 (\mathrm{mod}\ 2)$, we have

$$N_{2t+1} \equiv 3 (\mathrm{mod}\ 8);$$
$$r_{8t+2} \equiv 3;\ r_{8t+6} \equiv 3 (\mathrm{mod}\ 8)$$
$$s_{8t+2} \equiv -2a; \quad s_{8t+6} \equiv -2a - 4 (\mathrm{mod}\ 8)$$
$$M_{4t+2} \equiv -2a + 5 (\mathrm{mod}\ 8); \quad P_{4t+2} \equiv -2a + 3 (\mathrm{mod}\ 8),$$

thus we have $(\frac{-2a}{N_{2m}}) = (\frac{a}{N_{2m}}) = (\frac{N_{2m}}{a}) = (\frac{1}{a}) = 1$, $(\frac{s_{2m}}{N_{2m}}) = (\frac{N_{2m}}{|s_{2m}|}) = 1$

$$\begin{aligned}\left(\frac{M_{2m}}{N_{2m}}\right) &= \left(\frac{N_{2m}}{|M_{2m}|}\right) = \left(\frac{2a}{|M_{2m}|}\right)\left(\frac{2a-1}{|M_{2m}|}\right)\left(\frac{s_m^2}{|M_{2m}|}\right)\\ &= (-1)^{(M_{2m}^2-1)/8}\left(\frac{M_{2m}}{a}\right)\left(\frac{M_{2m}}{2a-1}\right)(-1)^{(a-1)/2}\\ &= (-1)^{(M_{2m}^2-1)/8}\left(\frac{1}{a}\right)\left(\frac{1}{2a-1}\right)(-1)^{(a-1)/2}\\ &= (-1)^{(M_{2m}^2-1)/8+(a-1)/2} = -1,\end{aligned}$$

and

$$\begin{aligned}\left(\frac{P_{2m}}{N_{2m}}\right) &= \left(\frac{N_{2m}}{|P_{2m}|}\right) = \left(\frac{2a}{|P_{2m}|}\right)\left(\frac{2a+1}{|P_{2m}|}\right)\left(\frac{s_m^2}{|P_{2m}|}\right)\\ &= (-1)^{(P_{2m}^2-1)/8}\left(\frac{P_{2m}}{a}\right)\left(\frac{P_{2m}}{2a+1}\right)(-1)^{(a-1)/2}\\ &= (-1)^{(P_{2m}^2-1)/8}\left(\frac{1}{a}\right)\left(\frac{1}{2a+1}\right)(-1)^{(a-1)/2}\\ &= (-1)^{(P_{2m}^2-1)/8+(a-1)/2} = -1,\end{aligned}$$

for $2m \equiv 2 \cdot 3^b \equiv 2 (\mathrm{mod}\ 4)$. So we have both

$$\left(\frac{-2as_{2m}M_m}{N_{2m}}\right) = \left(\frac{-2a}{N_{2m}}\right)\left(\frac{s_{2m}}{N_{2m}}\right)\left(\frac{M_m}{N_{2m}}\right) = -1$$

and

$$\left(\frac{-2as_{2m}P_m}{N_{2m}}\right) = \left(\frac{-2a}{N_{2m}}\right)\left(\frac{s_{2m}}{N_{2m}}\right)\left(\frac{P_m}{N_{2m}}\right) = -1$$

which is a contradiction.

From (i) and (ii), Lemma 7 is proved.

By the result of Lemmas 6 and 7, we see that if $n = 6k \neq 0$, Y_n cannot be a square in $Z(\sqrt{1-3a^2})$.

Collect all the results above, the theorem follows at once.

3 Some corollaries

In this section, we deduce some interesting corollaries from the theorem.

Corollary 1 (i) *The only solution in positive integers to the equation* $T(4T^2-3) = 11x^2$ *is given by* $T = 3$ *and* $x = 3$.

(ii) *The only solution in positive integers to the equation* $T(4T^2-3) = 55x^2$ *is given by* $T = 135$ *and* $x = 423$.

The two equations above have been proposed by Bennett and Walsh [5] and solved involving complicated computations in elliptic curve. Here, we give a much simpler proof.

Proof (i) It's a routine matter to verify if $T(4T^2-3) = 11x^2$ is solvable, then $T = 3u^2$, $4T^2 - 3 = 33v^2$, thus $12u^4 - 11v^2 = 1$. By our main theorem, we see that the

only solution of $12u^4 - 11v^2 = 1$ is given by $(u, v) = (1, 1)$.Thus, we prove that the only solution of equation $T(4T^2 - 3) = 11x^2$ is $(T, x) = (3, 3)$.

(ii) With the similar method, we obtain the only solution to the equation $T(4T^2 - 3) = 55x^2$ is given by$(T, x) = (135, 432)$. Here, the leading equation is $300u^4 - 11v^2 = 1$, where $T = 15u^2, 4T^2 - 3 = 33v^2$.

In fact, we can prove a more general result about Diophantine equation $T(4T^2-3) = dx^2$.

Corollary 2 (i) *Let p be prime positive integer and $p \equiv 3 (\mathrm{mod}\ 4)$, then we can find the integer solutions of Diophantine equation $T(4T^2 - 3) = px^2$ effectively if they exist.*

(ii) *Let p, q be prime positive integers with $p \equiv 1 (\mathrm{mod}\ 4)$ and $q \equiv -1 (\mathrm{mod}\ 4)$, then we can find the solutions of Diophantine equation $T(4T^2 - 3) = pqx^2$ if they exist.*

Proof (i) Since $(T, 4T^2 - 3) = 1 \mathrm{or}\ 3$, it is a routine matter to find that the Diophantine equation $T(4T^2 - 3) = px^2$ leads to

$$T = 3A^2, \quad 4T^2 - 3 = 3pB^2. \tag{19}$$

When $p \equiv 3 (\mathrm{mod}\ 4)$, (19) leads to the equation $12A^4 - pB^2 = 1$ which has at most one solution, and the solution can be obtained by the theorem if it exists. Then, we get the soluti on of equation in (i).

(ii) By disposing the obviously impossible equations, we conclude that $T(4T^2 - 3) = pqx^2$ leads to $T = 3pA^2, 4T^2 - 3 = 3qB^2$, thus we have $3(2p)^2A^4 - qB^2 = 1$ which has at most one solution, and the solution can be obtained by the theorem if it exists.

From the theorem, suppose $a \geq 1$ and the class number of field $\mathrm{Q}(\sqrt{1 - 3a^2})$ is not divisible by 2, we have Diophantine equation $3a^2x^4 - By^2 = 1$ which has at most one solution. Consequently, if we have already obtained at least two solutions of equation $3a^2x^4 - By^2 = 1$, we can determine that the class number of field $\mathrm{Q}(\sqrt{1 - 3a^2})$ is divisible by 2.

Corollary 3 *Let $m_0 = 1, m_1 = 22, m_{k+2} = 14m_{k+1} - m_k + 6$, where $k = 0, 1, 2, \ldots$, then the class number of the imaginary quadratic field $\mathrm{Q}(\sqrt{-m_k^2 - m_k})$ is divisible by 2.*

Proof Since $\alpha = 2 + \sqrt{3}$ is the least solution of Pell equation $u^2 - 3v^2 = 1$, then all the solutions of $u^2 - 3v^2 = 1$ are given by $u_t + v_t\sqrt{3} = \alpha^t, t = 0, 1, 2 \ldots$ and all the solutions for even u and odd v are given by $u_k + v_k\sqrt{3} = \alpha^{2k+1}, k = 0, 1, 2 \ldots$. Thus $v_k = \frac{\alpha^{2k+1} - \alpha^{-(2k+1)}}{2\sqrt{3}}, k = 0, 1, 2 \ldots$ and we have the following recurrence for v_k:

$$v_0 = 1, \quad v_1 = 15, \quad v_{k+2} = 14v_{k+1} - v_k.$$

Put $u_k = 2a_k, v_k = \frac{2m_k+1}{3}$, then from the recurrence above for v_k,we have the recurrence for m_k:

$$m_0 = 1, \quad m_1 = 22, \quad m_{k+2} = 14m_{k+1} - m_k + 6$$

Noting the fact that $u_k^2 - 3v_k^2 = 1$, we have $3a_k^2 = m_k^2 + m_k + 1$.

It can be easily verified that the Diophantine equation $(m_k^2 + m_k + 1)x^4 - (m_k^2 + m_k)y^2 = 1$ has two solutions $(1, 1)$ and $(2m_k + 1, 4m_k^2 + 4m_k + 3)$. In fact, it has been proved $(m^2 + m + 1)x^4 - (m^2 + m)y^2 = 1$ has only two solutions in [9]. Then, from the discussion above, the corollary follows.

For example, when $m = 22$, $m^2 + m + 1 = 3 \cdot 13^2$, the class number of $\mathrm{Q}(\sqrt{-506})$ is 28, which is divisible by 2.

Corollary 3 also shows that the result of the main theorem is best possible for the equation $3a^2x^4 - By^2 = 1$ in a certain sense.

References

1. Ljunggren, W.: On the Diophantine equation $Ax^4 - By^2 = C (C = 1, 4)$. Math. Scand. **21**, 149–158 (1967)
2. Bumby, R.T.: The Diophantine equation $3x^4 - 2y^2 = 1$. Math. Scand. **21**, 144–148 (1967)
3. Chen, J.H., Voutier, P.M.: A complete solution of the Diophantine equation $x^2 + 1 = dy^4$ and a related family of quadratic Thue equations. J. Number Theory **62**, 71–99 (1997)
4. Chen, J.H.: A note on the Diophantine equation. Acta. Arith. **96**(3), 205–212 (2001)
5. Bennett, M.A., Walsh, P.G.: The Diophantine equation $b^2x^4 - dy^2 = 1$. Proc. A.M.S **127**, 3481–3491 (1999)
6. Chen, J.H.: Rational approximations to some algebraic numbers and their applications to solve Diophantine equations. J. Math. (PRC) **20**(2), 121–132 (2000)
7. Le, M.H.: On the Diophantine equation $D_1x^4 - D_2y^2 = 1$. Acta. Arith. **76**, 1–9 (1996)
8. Hua, L.K.: Introduction to Number Theory. Springer, New York (1987)
9. Bennett, M.A., Togbe, A., Walsh, P.G.: A generalization of a theorem of Bumby on quartic Diophantine equations. Int. J. Number Theory **2**(2), 195–206 (2006)