ACTA ARITHMETICA
XCVI.3 (2001)

A note on the diophantine equation $a^2x^4 - By^2 = 1$

by

JIANHUA CHEN (Wuhan)

1. Introduction. Let A, B be coprime integers. The diophantine equation

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

has been studied extensively by many people, including Ljunggren [3] and Cohn [1]. Ljunggren proved that (1) has at most two solutions. In a recent paper in this journal, Le [2] proved some results on the diophantine equation

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

for example he proved that when $\max(a^2, B) > 2.374 \cdot 10^{10}$, the diophantine equation (2) has at most one integer solution. In fact, Ljunggren [4] proved this result without that restriction. (The author would like to express his gratitude to the referee for this reference.) The diophantine equation (2) includes many interesting special cases such as $x^4 - By^2 = 1$, $4x^4 - By^2 = 1$ and $9x^4 - By^2 = 1$.

In the present note we will prove the following two results:

(I) the equation (2) has at most one solution;

(II) the solution, when it exists, occurs in the "first possible place", i.e., comes from the least possible integer x for which $x^2 - By^2 = 1$ and x is divisible by a.

The result (I) is a new proof of Ljunggren's result, and the result (II) enables one to prove easily that many equations are not solvable. We will prove

THEOREM. *Let $a > 1$ and $B > 0$ be positive integers which are square-free. Suppose $\varepsilon = u + v\sqrt{B} > 1$ is the fundamental solution of Pell's equation $x^2 - By^2 = 1$. Define*

$$\varepsilon^n = u_n + v_n\sqrt{B}, \qquad n = 1, 2, \ldots$$

2000 *Mathematics Subject Classification*: Primary 11D09.

If (2) *is solvable then it has at most one solution* (x,y) *in positive integers, and then*

$$ax^2+v\sqrt{B}=\varepsilon^t$$

where t *is the least positive integer such that* $u_t\equiv 0 \pmod a$.

REMARK 1. It is easy to see that we can "effectively" determine if the equation (2) has an integer solution, because we can "effectively" determine whether there exists a positive integer t such that $u_t\equiv 0 \pmod a$ is solvable or not.

2. Preliminaries. In order to prove the Theorem we need some technical lemmas. First we consider Pell's equation

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

Let $\varepsilon=u+v\sqrt{B}$ be the fundamental solution of (3), define $\overline{\varepsilon}=u-v\sqrt{B}$, and for any integer n define

$$\varepsilon^n=x_n+y_n\sqrt{B}. \tag{4}$$

Throughout the paper we always assume that a is a given positive integer which is squarefree. If $a^2x^4-By^2=1$ has a solution then it is easy to see that there must exist an integer n such that $x_n\equiv 0 \pmod a$. The next lemma shows which n satisfy this congruence.

LEMMA 2.1. *Let* x_n *be defined as in* (4), *and let* $a>0$ *be an integer. If* $x_n\equiv 0 \pmod a$, *then there exists a positive integer* t *such that* $n=(2k+1)t$, $k=1,2,\ldots$

REMARK 2. From Lemma 2.1 we see that t is the least positive integer such that $x_t\equiv 0 \pmod a$.

Proof. Let t be the least positive integer such that $x_t\equiv 0 \pmod a$. Then for $0\le j<t$, we have

$$x_j\not\equiv 0 \pmod a. \tag{5}$$

Since $\varepsilon^t=x_t+y_t\sqrt{B}\equiv y_t\sqrt{B} \pmod a$, it is easy to verify that for an integer k we have

$$\varepsilon^{2kt}\equiv (y_t\sqrt{B})^{2k} \pmod a \equiv (y_t^2B)^k\equiv \pm 1 \pmod a. \tag{6}$$

Here we have made use of the relations

$$x_t^2-By_t^2=1 \tag{7}$$

and

$$x_t\equiv 0 \pmod a. \tag{8}$$

Similarly we have

$$\varepsilon^{(2k+1)t}\equiv (y_t\sqrt{B})^{2k+1}\equiv (y_t^2B)^k(y_t\sqrt{B})\equiv \pm y_t\sqrt{B} \pmod a. \tag{9}$$

From (9) we see that

$$x_{(2k+1)t} \equiv 0 \pmod{a}. \tag{10}$$

Let n be an arbitrary positive integer. We write n as $n = mt + r$, where $m \in \mathbb{Z}$ and $0 \le r < t$. We will prove that if $x_n \equiv 0 \pmod{a}$ then m is odd and $r = 0$. If m is an even integer then from (6) we get

$$\varepsilon^n = \varepsilon^{mt+r} \equiv \varepsilon^r \varepsilon^{mt} \equiv (x_r + y_r\sqrt{B})(\pm 1) \pmod{a}. \tag{11}$$

From (11) we see that $x_n \equiv \pm x_r \pmod{a} \equiv 0 \pmod{a}$. So we are left with odd m. For odd m we rewrite n as $n = mt + r = (m+1)t + r - t$; note that $m+1$ is even. Using a similar method we have

$$\varepsilon^n = \varepsilon^{(m+1)t+r-t} \equiv \pm\varepsilon^{r-t} \pmod{a}. \tag{12}$$

Note that

$$\varepsilon^{r-t} = x_{r-t} + y_{r-t}\sqrt{B}. \tag{13}$$

So if $x_n \equiv 0 \pmod{a}$ then from (11) and (12) we have $x_{t-r} \equiv 0 \pmod{a}$ and by (5) we must have $r = 0$. The lemma follows.

LEMMA 2.2. *Let $L > 0$, M be integers, $L - 4M > 0$, $(L, M) = 1$, and let α, β be two roots of $x^2 - \sqrt{L}x + M = 0$. If $M = -1$, $L \equiv 0 \pmod{4}$, put*

$$Q_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}$$

(n is an odd integer). Then for any odd prime p and integer z, we have

$$Q_p \ne pz^2.$$

Proof. See [6].

LEMMA 2.3. *Let t be the least integer such that $x_t \equiv 0 \pmod{a}$. Then $a^2x^4 - By^2 = 1$ is solvable if and only if $x_t = au^2$, $u \in \mathbb{Z}$.*

Proof. If $x_t = au^2$, then obviously $a^2x^4 - By^2 = 1$ and thus equation (2) is solvable. We now suppose $a^2x^4 - By^2 = 1$ is solvable. Then there exists an integer n such that

$$x_n = au^2 \tag{14}$$

and

$$x_n^2 - By^2 = 1. \tag{15}$$

Obviously $x_n \equiv 0 \pmod{a}$, hence by Lemma 2.1, $n = (2k+1)t$. Assume $n = (2k+1)t$ is the least solution of (14). If $2k+1 = 1$, the assertion follows. So we assume that $2k+1 > 1$. We write $2k+1 = ps$, where $p > 1$ is an odd prime number and s is an odd integer. From (14) we have

$$x_n = ax^2 = \frac{\varepsilon^{(2k+1)t} + \overline{\varepsilon}^{(2k+1)t}}{2} = \frac{\varepsilon^{pst} - \overline{\varepsilon}^{pst}}{2}. \tag{16}$$

Putting $\alpha = \varepsilon^{st}$ and $\beta = -\bar{\varepsilon}^{st}$, from (16) we get

$$ax^2 = \frac{\alpha^p - \beta^p}{2} = \frac{\alpha^p - \beta^p}{\alpha - \beta} \cdot \frac{\alpha - \beta}{2}. \tag{17}$$

By Lemma 2.1 it is obvious that $(\alpha - \beta)/2 \equiv 0 \pmod{a}$, hence from (17) we have

$$x^2 = \frac{\alpha^p - \beta^p}{\alpha - \beta} \cdot \frac{\alpha - \beta}{2a}. \tag{18}$$

Define

$$h = \left(\frac{\alpha^p - \beta^p}{\alpha - \beta}, \frac{\alpha - \beta}{2a}\right).$$

It is well known that $h = 1$ or $h = p$. If $h = 1$, from (18) we have $u^2 = (\alpha - \beta)/(2a)$ for some integer u, which contradicts the assumption that $n = (2k+1)t$ is the least solution of (14). So $h = p$. From (18) we find

$$pv^2 = \frac{\alpha^p - \beta^p}{\alpha - \beta} \tag{19}$$

for some integer v. Note that α, β are roots of the equation

$$x^2 - \sqrt{4By_t^2}x - 1 = 0.$$

By Lemma 2.2, (19) is impossible. This completes the proof.

We quote a result from Rickert [5] as our next lemma.

LEMMA 2.4. *For an integer N the numbers $\theta_1 = \sqrt{1 - 1/N}$, $\theta_2 = \sqrt{1 + 1/N}$ satisfy*

$$\max(|\theta_1 - p_1/q|, |\theta_2 - p_2/q|) > 1/(271Nq^{1+\lambda}),$$

for all integers p_1, p_2, $q > 0$, where

$$\lambda = \frac{\log(12N\sqrt{3} + 24)}{\log(27(N^2 - 1)/32)}. \tag{20}$$

Proof. See Rickert [5], p. 469.

LEMMA 2.5. *Let $u > 0$ be an integer, $au^2 > 25$. Consider the simultaneous Pell equations*

$$ax^2 - (au^2 - 1)z_1^2 = 1, \quad ax^2 - (au^2 + 1)z_2^2 = -1. \tag{21}$$

Then all its positive integer solutions satisfy

$$|\sqrt{a}x|^{1-\lambda} < 141.89(\sqrt{a}u)^{3+\lambda}, \tag{22}$$

where λ is as in (20) and $N = au^2$. Furthermore, if $au^2 > 99$ and $x > u$, then $\sqrt{a}x > (2\sqrt{a}u)^{569}$.

Proof. Let $x > 0$ be a solution of (21). The equations (21) have an obvious solution $x = u, z_1 = z_2 = 1$. So we assume $x > u$. Now we have

$$|\sqrt{a}x - z_1\sqrt{au^2-1}| = \frac{1}{|\sqrt{a}x + z_1\sqrt{au^2-1}|} < \frac{1}{1.99\sqrt{a}x}.$$

Hence

$$|\sqrt{a/(au^2-1)} - z_1/x| < \frac{1}{1.99\sqrt{a}x^2\sqrt{au^2-1}} < \frac{1}{1.95aux^2}.$$

Multiplying this inequality by u we get

$$|\sqrt{au^2/(au^2-1)} - z_1u/x| < \frac{1}{1.95ax^2}. \tag{23}$$

Multiplying both sides of (23) by $1 - 1/(au^2)$ we get

$$|\sqrt{1-1/N} - z_1(au^2-1)/(aux)| < \frac{1}{1.95ax^2}. \tag{24}$$

In a similar way from the second equation of (21) we get

$$|\sqrt{1+1/N} - z_2(au^2+1)/(aux)| < \frac{1}{1.95ax^2}. \tag{25}$$

Then by Lemma 2.4 we get

$$271au^2|aux|^{1+\lambda} > 1.91ax^2. \tag{26}$$

From (26) we easily deduce that

$$|x|^{1-\lambda} < 141.89u^{3+\lambda}a^{1+\lambda}.$$

Multiplying this inequality by $a^{(1-\lambda)/2}$ we get the conclusion.

We now prove $\sqrt{a}x > (2\sqrt{a}u)^{569}$. Put

$$\eta_1 = \sqrt{a}u + \sqrt{au^2-1}, \quad \overline{\eta}_1 = \sqrt{a}u - \sqrt{au^2-1}, \tag{27}$$

$$\eta_2 = \sqrt{a}u + \sqrt{au^2+1}, \quad \overline{\eta}_2 = \sqrt{a}u - \sqrt{au^2+1}. \tag{28}$$

Then all the solutions (x, z_1) of $ax^2 - (au^2-1)z_1^2 = 1$ are given by

$$\eta_1^m = \sqrt{a}x + z_1\sqrt{au^2-1} \tag{29}$$

for odd integers $m > 0$. All the solutions (x, z_2) of $ax^2 - (au^2+1)z_2^2 = -1$ are given by

$$\eta_2^n = \sqrt{a}x + z_2\sqrt{au^2+1} \tag{30}$$

for odd integers $n > 0$. Hence if (21) has another solution x, then

$$\eta_1^m + \overline{\eta}_1^m = \eta_2^n + \overline{\eta}_2^n. \tag{31}$$

From (31) we get

$$|n\log(\eta_2/\eta_1) + (n-m)\log\eta_1| < 1.1/\eta_1^{2m} + 1.1/\eta_1^{2n}. \tag{32}$$

Noting that $n\log(\eta_2/\eta_1) < n(\eta_2-\eta_1)/\eta_1$, from (32) we get

$$n\frac{\eta_2-\eta_1}{\eta_1} > |n-m|\log\eta_1 - 2.2/\eta_1^6 > 0.99\log\eta_1$$

so $n > 0.97\sqrt{a}u\eta_1\log\eta_1 > 570$, hence

$$\sqrt{a}x = (\eta_2^n+\overline{\eta}_2^n)/2 > (2\sqrt{a}u)^{569},$$

and the lemma follows at once.

Remark 3. From the above lemma we can "effectively" solve the simultaneous equations as in the lemma when $au^2 > 25$.

3. Proof of the Theorem. In this section, we will prove our main theorem and discuss some special cases of it. First from Lemmas 2.1 and 2.3 we see that if the equation

$$a^2x^4 - By^2 = 1 \tag{33}$$

is solvable, then

$$au^2 + y_t\sqrt{B} = \varepsilon^t. \tag{34}$$

Since $(\varepsilon\overline{\varepsilon})^t = 1$, we get $a^2u^4 - By_t^2 = 1$, thus we have

$$\sqrt{a^2u^4-1} = \sqrt{By_t^2},$$

so

$$au^2 + \sqrt{a^2u^4-1} = \varepsilon^t.$$

For brevity we write $D = a^2u^4-1$, $\varepsilon_1 = \varepsilon^t$, $\overline{\varepsilon}_1 = \overline{\varepsilon}^t$. If (33) has another solution (x,y), then by Lemma 2.3 we have

$$ax^2 = \frac{\varepsilon_1^{2k+1}+\overline{\varepsilon}_1^{2k+1}}{2}. \tag{35}$$

We write

$$\varepsilon_1^n = X_n + Y_n\sqrt{D} \tag{36}$$

for non-negative integers n. Notice that $X_1 = au^2$, $Y_1 = 1$. Then (35) can be written as

$$ax^2 = X_{2k+1}. \tag{37}$$

It is easy to verify that

$$X_{2n+1} = X_1X_{2n} + DY_{2n}, \tag{38}$$

$$X_{2n} = X_n^2 + DY_n^2, \qquad Y_{2n} = 2X_nY_n. \tag{39}$$

Combining (36) with (37) and (38), we get

$$ax^2 = X_1(X_k^2+DY_k^2) + 2DX_kY_k. \tag{40}$$

Since $X_k^2 - DY_k^2 = 1$, we have

$$\begin{aligned} ax^2 - 1 &= X_1(X_k^2 + DY_k^2) + 2DX_kY_k - (X_k^2 - DY_k^2) \\ &= (X_1 - 1)X_k^2 + D(X_1 + 1)Y_k^2 + 2DX_kY_k \\ &= (X_1 - 1)(X_k^2 + (X_1 + 1)^2Y_k^2 + 2(X_1 + 1)X_kY_k) \\ &= (X_1 - 1)(X_k + (X_1 + 1)Y_k)^2 = (X_1 - 1)Z_1^2. \end{aligned}$$

Here we have used the relation $D = X_1^2 - 1 = a^2X^4 - 1$. In a similar way we have

$$ax^2 + 1 = (X_1 + 1)Z_2^2. \tag{41}$$

By Lemma 2.5 a solution x of the simultaneous equations

$$ax^2 - 1 = (X_1 - 1)Z_1^2$$

and

$$ax^2 + 1 = (X_1 + 1)Z_2^2$$

satisfies

$$|\sqrt{a}x|^{1-\lambda} < 141.89(\sqrt{a}u)^{3+\lambda} \tag{42}$$

where λ is just as in Lemma 2.5.

Note that for $N = au^2 > 99$, we have $\lambda < 0.84630254$. From (42) we get

$$|\sqrt{a}x| < 141.89^{1/(1-\lambda)}(\sqrt{a}u)^{(3+\lambda)/(1-\lambda)} < 1.01 \cdot 10^{14}(\sqrt{a}u)^{25.026}. \tag{43}$$

But from Lemma 2.5 we have $\sqrt{a}x > (2\sqrt{a}u)^{569}$, a contradiction. This proves the lemma.

Remark 4. From the proof of the Theorem we see that $au^2 > 99$ can be relaxed.

Remark 5. By the same method, we can completely solve the equations $x^4 - By^2 = 1$, $4x^4 - By^2 = 1$ and $9x^4 - By^2 = 1$.

Note added in proof. M. Bennett and G. Walsh proved the same result using a different method (see Proc. Amer. Math. Soc. 127 (1999), 3481–3491). The author would like to express his thanks to Professor Schinzel as well as Professor Walsh for telling him about the above paper.

References

[1] J. H. E. Cohn, *The diophantine equation $x^4 + 1 = Dy^2$*, Math. Comp. 66 (1997), 1347–1351.

[2] M.-H. Le, *On the diophantine equation $D_1x^4 - D_2y^2 = 1$*, Acta Arith. 76 (1996), 1–9.

[3] W. Ljunggren, *Über die unbestimmte Gleichung $Ax^4 - By^2 = C$*, Arch. Math. Naturv. 41 (10) (1938).

[4] W. Ljunggren, *Einige Sätze über unbestimmte Gleichungen von der Form $Ax^4 + By^2 + C = Dy^2$*, Vid.-Akad. Skr. Norsk. Oslo 1942, no. 9.

[5] J. Rickert, *Simultaneous rational approximations and related Diophantine equations*, Math. Proc. Cambridge Philos. Soc. 113 (1993), 461–472.

[6] A. Rotkiewicz, *Applications of Jacobi's symbol to Lehmer's numbers*, Acta Arith. 42 (1983), 163–187.

Department of Mathematics
Wuhan University
Wuhan 430072, P.R. China
E-mail: jianh_chen@sina.com

Received on 4.5.1999
and in revised form 19.4.2000 (3594)