ON THE DIOPHANTINE EQUATION \( x^{2n} - Dy^2 = 1 \)

CAO ZHENFU

ABSTRACT. In this paper, it has been proved that if \( n > 2 \) and Pell's equation \( u^2 - Dv^2 = -1 \) has integer solution, then the equation \( x^{2n} - Dy^2 = 1 \) has only solution in positive integers \( x = 3, y = 22 \) (when \( n = 5, D = 122 \)). That is proved by studying the equations \( x^p + 1 = 2y^2 \) and \( x^p - 1 = 2y^2 \) (\( p \) is an odd prime). In addition, some applications of the above result are given.

1. Introduction. For the Diophantine equation

\[
 x^{2n} - Dy^2 = 1
\]

\( D > 0 \) and is not a perfect square, and \( n > 1 \) is an integer number. When \( n = 2 \), its solvability was discussed by Ljunggren, Cohn, Ko Chao and Sun Chi [1], and the author [2], etc. In this paper, we discuss the solvability of equation (1) in the case \( n > 2 \).

THEOREM 1. If \( n > 2 \) and Pell's equation \( u^2 - Dv^2 = -1 \) has integer solution, then the Diophantine equation (1) has only solution in positive integers \( x = 3, y = 22 \) (when \( n = 5, D = 122 \)).

Tartakowski [3] has proved that if \( n > 2 \) and the equation \( u^2 - Dv^2 = -1 \) has solution, then the equation \( x^{2n} - Dy^{2n} = 1 \) has no solution in positive integers. Clearly, the result of Tartakowski is included in Theorem 1.

THEOREM 2. If \( \eta = U_0 + V_0\sqrt{D} \) is the fundamental solution of Pell's equation \( U^2 - DV^2 = 1 \), then positive integer solutions of equation (1) do not satisfy

\[
 x^n + y\sqrt{D} = \eta^{4m}, \quad n > 2, \ m > 0.
\]

The proof of the above result is obtained by studying equations

\[
 x^p + 1 = 2y^2, \quad p \text{ odd prime} > 3,
\]

and

\[
 x^p - 1 = 2y^2, \quad p \text{ odd prime} > 3,
\]

with Ko Chao's elementary method (see Ko Chao [4]). The method is helpful to the research of Erdös' conjecture on combinatorial
2. Two lemmas on equations (2) and (3).

**Lemma 1.** If equation (2) has positive integer solution, then $2p|y$ except $x = y = 1$.

**Proof.** Suppose $(x, y)$ is any positive integer solution of (2). Then

$$
(x + 1)/((x^p + 1)/(x + 1)) = 2y^2.
$$

Since $(x + 1, (x^p + 1)/(x + 1)) = 1$ or $p$, we have

$$
x + 1 = 2y_1^2, \quad (x^p + 1)/(x + 1) = y_2^2, \quad y = y_1y_2,
$$

or

$$
x + 1 = 2py_1^2, \quad (x^p + 1)/(x + 1) = py_2^2, \quad y = py_1y_2.
$$

By the result of Ljunggren [5], $(x^p + 1)/(x + 1) = y_2^2$, therefore $x = 1$. Thus (4) gives $x = y = 1$.

For (5), clearly $p|y$. We will prove $2|y$ with Ko Chao's elementary method. If $2|y$, from (2), we have $x \equiv 1 \pmod{8}$. Put

$$
A(t) = (x^t + 1)/(x + 1), \quad t \geq 1 \text{ and } 2|t,
$$

and so $A(t) \equiv 1 \pmod{8}$. Let $1 < l < p$ be a positive odd integer. Then there exist an integer $r$, odd, $0 < r < l$, and $2k$ such that $p = 2kl + r$ or $p = 2kl - r$.

If $p = 2kl + r$, then

$$
A(p) = ((x^lA(l) - 1)2^{kl}x^r + 1)/(x + 1) \equiv A(r) \pmod{A(l)},
$$

since $x^l = (x + 1)A(l) - 1$. Now $(A(p), A(l)) = (A(p, l)) = A(1) = 1$. Thus, (6) gives

$$
(A(p)/A(l)) = (A(r)/A(l)).
$$

If $p = 2kl - r$, then $l - r$ is even. Thus

$$
(A(p)/A(l)) = (-x^{l-r}A(r)/A(l)) = (A(r)/A(l)),
$$

since $A(l) \equiv 1 \pmod{8}$ and

$$
A(p) = x^{l-r}A(l(2k - 1)) + A(l) - x^{l-r}A(r).
$$

For $l$, $r$, we have

$$
l = 2k_1r + \varepsilon_1r_1, \quad 0 < r_1 < r,
$$

$$
r = 2k_2r_1 + \varepsilon_2r_2, \quad 0 < r_2 < r_1,
$$

$$
\ldots
$$

$$
r_{s-1} = 2k_{s+1}r_s + \varepsilon_{s+1}r_{s+1}, \quad 0 < r_{s+1} < r_s,
$$

$$
r_s = k_{s+2}r_{s+1},
$$

where $\varepsilon_i = \pm 1$ ($i = 1, \ldots, s + 1$) and $r_i$ ($i = 1, \ldots, s + 1$) are odd integers. Since $(l, p) = 1$, we have $r_{s+1} = 1$. Hence

$$
\left(\begin{array}{c}
A(p)/A(l)
\end{array}\right) = \left(\begin{array}{c}
A(r)/A(l)
\end{array}\right) = \left(\begin{array}{c}
A(r_1)/A(l)
\end{array}\right) = \left(\begin{array}{c}
A(r)/A(r_1)
\end{array}\right) = \left(\begin{array}{c}
A(r_2)/A(r_1)
\end{array}\right) = \ldots = \left(\begin{array}{c}
A(r_{s+1}+1)/A(r_s)
\end{array}\right) = \left(\begin{array}{c}
A(1)/A(r_s)
\end{array}\right) = \left(\begin{array}{c}
1/A(r_s)
\end{array}\right) = 1.
$$
ON THE DIOPHANTINE EQUATION $x^{2n} - Dy^2 = 1$

Now, from $(x^{p} + 1)/(x + 1) = p\bar{y}_2$, we have

$$(py_2)^2 \equiv p\bar{A}(p) \pmod{A(l)}.$$ 

Thus

$$\left(\frac{p\bar{A}(p)}{\bar{A}(l)}\right) = \left(\frac{p}{\bar{A}(l)}\right) = \left(\frac{l}{p}\right) = 1,$$

since $x \equiv -1 \pmod{p}$ and so $A(l) \equiv l \pmod{p}$. We have a contradiction if $l$ is taken as an odd quadratic nonresidue of $p$. This proves the result. \hfill \Box

**Remark 1.** Using the above method, we can prove that the equations

$$x^p \pm y^p = 2z^2, \quad (x, y) = 1, p \text{ prime } > 3,$$

have no positive integer solution when $2|z, p|z$.

**Lemma 2.** Equation (3) has only positive integer solution $x = 3, y = 11$ (when $p = 5$).

**Proof.** From (3), we have

$$(7) \quad \frac{(x^p - 1)/(x - 1)}{a^2},$$

if $p|y$. By the result of Ljunggren [5], the solution of (7) is $x = 3$ (when $p = 5$). Thus (3) has positive integer solution $x = 3, y = 11$ (when $p = 5$).

If $p|y$, then $2|y$ by Remark 1. From (3), $(1 + \sqrt{-2}y)(1 - \sqrt{-2}y) = x^p$. With $(1 + \sqrt{-2}y, 1 - \sqrt{-2}y) = 1$, we have

$$(8) \quad 1 + \sqrt{-2}y = (a + b\sqrt{-2})^p, \quad x = a^2 + 2b^2,$$

where $a, b$ are rational integers. Since $2|y$, from (3), it follows that

$$(9) \quad x \equiv 1 \pmod{8}.$$ 

From (8) and (9), we have $2|b$ and $b \neq 0$. Now, (8) gives

$$(10) \quad 1 = a^p + \left(\frac{p}{2}\right) a^{p-2} (b\sqrt{-2})^2 + \cdots + \left(\frac{p}{p-1}\right) a (b\sqrt{-2})^{p-1}.$$ 

Thus $a|1$ and so $a = \pm 1$.

If $a = -1$, then (10) gives

$$-2 = \left(\frac{p}{2}\right) (b\sqrt{-2})^2 + \cdots + \left(\frac{p}{p-1}\right) (b\sqrt{-2})^{p-1},$$

and so $p|2$ which is impossible.

If $a = 1$, then we have

$$(11) \quad 0 = \left(\frac{p}{2}\right) (b\sqrt{-2})^2 + \cdots + \left(\frac{p}{p-1}\right) (b\sqrt{-2})^{p-1}.$$ 

Since $2|b$ and $b \neq 0$, let $2^s \| (\frac{p}{2k}) (b\sqrt{-2})^{2k} \ (1 \leq k \leq (p-1)/2)$, clearly $s_k > s_j \ (k > j)$. Thus (11) is impossible.

**Remark 2.** Nagell [8] also proved Lemma 2, but the above proof is a new method.
3. Proof of the theorems.

Proof of Theorem 1. Let $\Omega = u_0 + v_0\sqrt{D}$ be the fundamental solution of the equation $u^2 - Dv^2 = -1$, $\bar{\Omega} = u_0 - v_0\sqrt{D}$, $\Omega\bar{\Omega} = -1$, and let $\eta = U_0 + V_0\sqrt{D}$ be the fundamental solution of the equation $U^2 - DV^2 = 1$, $\eta = U_0 - V_0\sqrt{D}$, $\eta\bar{\eta} = 1$. Then, we have $\eta = \Omega^2$.

Suppose $(x, y)$ is any positive integer solution of (1). Then

$$x^m = \frac{\eta^m + \bar{\eta}^m}{2} = \frac{\Omega^{2m} + \bar{\Omega}^{2m}}{2}, \quad m > 0. \tag{12}$$

Clearly, without loss of generality, we may assume that $n = 4$ or $n = p$ ($p$ is odd prime).

(a) If $n = 4$, then (12) gives

$$x^4 = 2((\Omega^m + \bar{\Omega}^m)/2)^2 - (-1)^m,$$

and so $x = 1$, $m = 0$ which is impossible since $m > 0$.

(b) If $n = p$ ($p$ is odd prime), then (12) gives

$$x^p = 2((\Omega^m + \bar{\Omega}^m)/2)^2 - (-1)^m, \tag{13}$$

(b.1) When $2|m$, let $m = 2s$, $s > 0$; then (13) gives

$$x^p + 1 = 2((\Omega^{2s} + \bar{\Omega}^{2s})/2)^2. \tag{14}$$

Suppose $p = 3$. Then by (14), we have (see [6])

$$x = (\Omega^{2s} + \bar{\Omega}^{2s})/2 = 1, \tag{15}$$

and

$$x = 23, \quad (\Omega^{2s} + \bar{\Omega}^{2s})/2 = 78. \tag{16}$$

Clearly (15) is impossible since $s > 0$, and (16) is also impossible since

$$\frac{\Omega^{2s} + \bar{\Omega}^{2s}}{2} = 2 \left( \frac{\Omega^s + \bar{\Omega}^s}{2} \right)^2 - (-1)^s$$

is odd.

Thus $p > 3$. For (14), we have $2p|((\Omega^{2s} + \bar{\Omega}^{2s})/2)$ by Lemma 1. However, $2|((\Omega^{2s} + \bar{\Omega}^{2s})/2)$ is impossible.

(b.2) When $2 \nmid m$, we have

$$x^p - 1 = 2((\Omega^m + \bar{\Omega}^m)/2)^2, \tag{17}$$

and so $x = 1$, $(\Omega^m + \bar{\Omega}^m)/2 = 0$ when $p = 3$ (see [6]). If $p > 3$, then (17) gives $x = 3$, $(\Omega^m + \bar{\Omega}^m)/2 = 11$ (when $p = 5$) by Lemma 2. Thus (1) has only positive integer solution $x = 3, y = 22$ (when $n = 5, D = 122$).

This completes the proof of Theorem 1. \hfill \Box

Proof of Theorem 2. If

$$x^n + y\sqrt{D} = \eta^{4m}, \quad n > 2, m > 0,$$

then we have

$$x^n = \frac{\eta^{4m} + \bar{\eta}^{4m}}{2} = 2 \left( \frac{\eta^{2m} + \bar{\eta}^{2m}}{2} \right)^2 - 1. \tag{18}$$

By Lemma 1, (18) is impossible since $2 \nmid (\eta^{2m} + \bar{\eta}^{2m})/2$ and $m > 0$. \hfill \Box
4. Applications. As applications of the result, we will discuss other problems in number theory in the following paragraphs.

4.1. In 1939, Erdős [7] conjectured that the equation

\[ \binom{n}{m} = y^k, \quad n > m > 1, k \geq 3, \]

has no integer solution. In 1951, Erdős himself proved that the conjecture is right when \( m > 3 \), leaving the cases \( m = 2 \) and \( m = 3 \) unsolved. Now, we can deduce the following corollary from Theorem 1 and Lemma 1.

COROLLARY 1. The equation \( \binom{n}{2} = y^{2k} \) has no positive integer solution \( n, y \) with \( n > 2 \) and \( k > 1 \).

**Proof.** From \( \binom{n}{2} = n(n-1)/2 = y^{2k} \), we have

\[ n - 1 = 2y_1^{2k}, \quad n = y_2^{2k}, \quad y = y_1y_2, \]

or

\[ n - 1 = y_2^{2k}, \quad n = y_1^{2k}, \quad y = y_1y_2. \]

Hence

\[ y_2^{2k} + 1 = 2y_1^{2k}. \]

If \( 2|k \), then (20) clearly gives \( |y_1y_2| \leq 1 \); on the other hand, \( n > 2 \) and \( \binom{n}{2} = y^{2k} \) imply \( |y| = |y_1y_2| > 1 \). Here we have a contradiction. If \( 2 \nmid k, k > 1 \), we may conclude from Theorem 1 and Lemma 1 that (20) is impossible. \( \Box \)

4.2. For the Pell sequence

\[ x_0 = 1, \quad x_1 = a, \quad x_{n+2} = 2ax_{n+1} - x_n, \]

where \( a \) is an integer \( > 1 \), we have

COROLLARY 2. The equation \( x_{4n} = y^m \) has no positive integer solution \( n, y \) when \( m > 2 \).

**Proof.** From (21), we have \( x_n = (\alpha^n + \bar{\alpha}^n)/2, n \geq 0 \), where \( \alpha = a + \sqrt{a^2 - 1} \) and \( \bar{\alpha} = a - \sqrt{a^2 - 1} \) are roots of the trinomial \( z^2 - 2az + 1 \). Let \( a^2 - 1 = Db^2 \), where \( D > 0 \) is squarefree and \( b \) is positive integer. Then

\[ \alpha = a + b\sqrt{D}, \quad \bar{\alpha} = a - b\sqrt{D} \quad \text{and} \quad \alpha\bar{\alpha} = 1. \]

Thus \( y_n = (\alpha^n - \bar{\alpha}^n)/2\sqrt{D} \) satisfies

\[ x_n^2 - Dy_n^2 = 1. \]

By Theorem 2, (22) is impossible when \( 4|n, x_n = y^m \) and \( m > 2 \). \( \Box \)

Clearly, if \( a = 2u^2 + 1 \) \( (u > 0) \), then \( Db^2 = a^2 - 1 = 4u^2(u^2 + 1) \). Thus \( 2u|b \). Let \( b = 2uv \), we have \( u^2 + 1 = Du^2 \). Hence, using Theorem 1, we have

COROLLARY 3. For the Pell sequence

\[ x_0 = 1, \quad x_1 = 2u^2 + 1, \quad x_{n+2} = 2(2u^2 + 1)x_{n+1} - x_n, \]

where \( u \) is positive integer, \( x_n \) is never an \( m \)th power if \( m > 2 \) and except \( x_1 = 2 \cdot 11^2 + 1 = 3^5. \) \( \Box \)

ACKNOWLEDGMENT. The author would like to thank Professor Sun Chi for his helpful suggestions.
REFERENCES

4. Ko Chao, *On the diophantine equation* $x^2 = y^n + 1, xy \neq 0$, Sichun Daxue Xuebao 1 (1962), 1–6.
5. W. Ljunggren; *Some theorems on indeterminate equations of the form* $(x^n - 1)/(x - 1) = y^2$, Norsk Mat. Tidsskr. 25 (1943), 17–20.
6. R. W. van der Waall, *On the diophantine equations* $x^2 + x + 1 = 3y^2$, $x^3 - 1 = 2y^2$, $x^3 + 1 = 2y^2$, Simon Stevin 46 (1972/73), 39–51.

DEPARTMENT OF MATHEMATICS, HARBIN INSTITUTE OF TECHNOLOGY, HARBIN, CHINA