PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 98, Number 1, September 1986

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

$$x^{2n} - Dy^2 = 1 \tag{1}$$

$D > 0$ 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*

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

The proof of the above result is obtained by studying equations

$$x^p + 1 = 2y^2, \qquad p \text{ odd prime } > 3, \tag{2}$$

and

$$x^p - 1 = 2y^2, \qquad p \text{ odd prime } > 3, \tag{3}$$

with Ko Chao's elementary method (see Ko Chao [**4**]). The method is helpful to the research of Erdös' conjecture on combinatorial

Received by the editors October 24, 1984 and, in revised form, May 29, 1985.
1980 *Mathematics Subject Classification* (1985 *Revision*). Primary 11D15; Secondary 11B10.

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

$$x+1 = 2y_1^2, \qquad (x^p+1)/(x+1) = y_2^2, \qquad y = y_1 y_2, \tag{4}$$

or

$$x+1 = 2py_1^2, \qquad (x^p+1)/(x+1) = py_2^2, \qquad y = py_1 y_2. \tag{5}$$

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 $2\nmid y$, from (2), we have $x \equiv 1 \pmod 8$. Put

$$\mathcal{A}(t) = (x^t+1)/(x+1), \qquad t \geq 1 \text{ and } 2\nmid t,$$

and so $\mathcal{A}(t) \equiv 1 \pmod 8$. 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

$$\mathcal{A}(p) = \frac{((x+1)\mathcal{A}(l) - 1)^{2k} x^r + 1}{x+1} \equiv \frac{x^r+1}{x+1} \equiv \mathcal{A}(r) \pmod{\mathcal{A}(l)}, \tag{6}$$

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

$$(\mathcal{A}(p)/\mathcal{A}(l)) = (\mathcal{A}(r)/\mathcal{A}(l)).$$

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

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

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

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

For l, r, we have

$$\begin{aligned}
&l = 2k_1 r + \varepsilon_1 r_1, && 0 < r_1 < r,\\
&r = 2k_2 r_1 + \varepsilon_2 r_2, && 0 < r_2 < r_1,\\
&\cdots\\
&r_{s-1} = 2k_{s+1} r_s + \varepsilon_{s+1} r_{s+1}, && 0 < r_{s+1} < r_s,\\
&r_s = k_{s+2} r_{s+1},
\end{aligned}$$

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

$$\begin{aligned}
\left(\frac{\mathcal{A}(p)}{\mathcal{A}(l)}\right) &= \left(\frac{\mathcal{A}(r)}{\mathcal{A}(l)}\right) = \left(\frac{\mathcal{A}(l)}{\mathcal{A}(r)}\right) = \left(\frac{\mathcal{A}(r_1)}{\mathcal{A}(r)}\right) = \left(\frac{\mathcal{A}(r)}{\mathcal{A}(r_1)}\right) = \left(\frac{\mathcal{A}(r_2)}{\mathcal{A}(r_1)}\right)\\
&= \cdots = \left(\frac{\mathcal{A}(r_{s+1})}{\mathcal{A}(r_s)}\right) = \left(\frac{\mathcal{A}(1)}{\mathcal{A}(r_s)}\right) = \left(\frac{1}{\mathcal{A}(r_s)}\right) = 1.
\end{aligned}$$

Now, from $(x^p+1)/(x+1) = py_2^2$, we have

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

Thus

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

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

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

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

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

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

PROOF. From (3), we have

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

if $p \nmid y$. 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

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

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

$$x \equiv 1 \pmod 8. \tag{9}$$

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

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

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

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

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

and so $p|2$ which is impossible.

If $a = 1$, then we have

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

Since $2|b$ and $b \neq 0$, let $2^{s_k} \| \binom{p}{2k} \left(b\sqrt{-2}\right)^{2k}$ $(1 \le k \le (p-1)/2)$, 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 $u^2 - Dv^2 = -1$, $\overline{\Omega} = u_0 - v_0\sqrt{D}$, $\Omega\overline{\Omega} = -1$, and let $\eta = U_0 + V_0\sqrt{D}$ be the fundamental solution of the equation $U^2 - DV^2 = 1$, $\eta = U_0 - V_0\sqrt{D}$, $\eta\overline{\eta} = 1$. Then, we have $\eta = \Omega^2$.

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

$$x^n = \frac{\eta^m + \overline{\eta}^m}{2} = \frac{\Omega^{2m} + \overline{\Omega}^{2m}}{2}, \qquad m > 0. \tag{12}$$

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

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

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

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

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

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

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

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

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

and

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

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

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

is odd.

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

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

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

and so $x = 1$, $(\Omega^m + \overline{\Omega}^m)/2 = 0$ when $p = 3$ (see [**6**]). If $p > 3$, then (17) gives $x = 3$, $(\Omega^m + \overline{\Omega}^m)/2 = 11$ (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. □

PROOF OF THEOREM 2. If

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

then we have

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

By Lemma 1, (18) is impossible since $2\nmid(\eta^{2m} + \overline{\eta}^{2m})/2$ and $m > 0$. □

4. Applications. As applications of the result, we will discuss other problems in number theory in the following paragraphs.

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

$$\binom{n}{m} = y^k, \qquad n > m > 1, k \geq 3, \tag{19}$$

has no integer solution. In 1951, Erdös 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

$$n - 1 = 2y_1^{2k}, \quad n = y_2^{2k}, \quad y = y_1 y_2,$$

or

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

Hence

$$y_2^{2k} \mp 1 = 2y_1^{2k}. \tag{20}$$

If $2|k$, then (20) clearly gives $|y_1 y_2| \leq 1$; on the other hand, $n > 2$ and $\binom{n}{2} = y^{2k}$ imply $|y| = |y_1 y_2| > 1$. here we have a contradiction. If $2 \nmid k$, $k > 1$, we may conclude from Theorem 1 and Lemma 1 that (20) is impossible. □

4.2. For the Pell sequence

$$x_0 = 1, \quad x_1 = a, \quad x_{n+2} = 2ax_{n+1} - x_n, \tag{21}$$

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 $x_n = (\alpha^n + \overline{\alpha}^n)/2$, $n \geq 0$, where $\alpha = a + \sqrt{a^2 - 1}$ and $\overline{\alpha} = a - \sqrt{a^2 - 1}$ 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

$$\alpha = a + b\sqrt{D}, \quad \overline{\alpha} = a - b\sqrt{D} \quad \text{and} \quad \alpha\overline{\alpha} = 1.$$

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

$$x_n^2 - Dy_n^2 = 1. \tag{22}$$

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

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 $u^2 + 1 = Dv^2$, 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* $x_1 = 2 \cdot 11^2 + 1 = 3^5$. □

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

REFERENCES

1. Ko Chao and Sun Chi, *On the diophantine equation* $x^4 - Dy^2 = 1$. II, Chinese Ann. Math. Ser. A **1** (1980), 83–88.
2. Cao Zhenfu, *On the diophantine equations* $x^2 + 1 = 2y^2$ *and* $x^2 - 1 = 2Dz^2$, J. Math. (Wuhan) **3** (1983), 227–235.
3. L. J. Mordell, *Diophantine equations*, Academic Press, London and New York, 1969.
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* $(x^n - 1)/(x - 1) = y^q$, Norsk Mat. Tidsskr. **25** (1943), 17–20.
6. R. W. van der Waall, *On the diophantine equations* $x^2 + x + 1 = 3v^2$, $x^3 - 1 = 2y^2$, $x^3 + 1 = 2y^2$, Simon Stevin **46** (1972/73), 39–51.
7. P. Erdös, *On a diophantine equation*, J. London Math. Soc. **26** (1951), 176–178.
8. W. Ljunggren, *On the Diophantine equation* $Cx^2 + D = 2y^n$, Math. Scand. **18** (1966), 69–86.

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