ON THE DIOPHANTINE EQUATION $x^p + 2^{2m} = py^2$

ZHENFU CAO

(Communicated by David E. Rohrlich)

ABSTRACT. Let p be an odd prime. In this paper, using some theorems of Adachi and the author, we prove that if $p \equiv 1 \pmod{4}$ and $p \nmid B_{(p-1)/2}$, then the equation $x^p + 1 = py^2$, $y \neq 0$, and the equation $x^p + 2^{2m} = py^2$, $m \in \mathbb{N}$, $\gcd(x, y) = 1$, $p \nmid y$, have no integral solutions respectively. Here $B_{(p-1)/2}$ is $(p-1)/2$ th Bernoulli number.

§1. INTRODUCTION

Let $\mathbb{Z}, \mathbb{N}, \mathbb{Q}$ be the sets of integers, positive integers and rational numbers respectively, and let p be an odd prime. In [1], Nagell proved that if $D \in \mathbb{N}$ with $D > 2$ square-free, and $p \nmid h(-D)$, where $h(-D)$ is the class number of $\mathbb{Q}(\sqrt{-D})$, then the equation

$$x^p - 1 = Dy^2, \quad x, y \in \mathbb{Z}, \quad xy \neq 0,$$

has no solutions with $2 \nmid x$. In [2], we proved that if $p > 3$, $D \in \mathbb{N}$ is a square-free integer which is not divisible by primes of the form $2mp + 1$, then the equation

$$x^p + C = Dy^2, \quad C \in \{-1, 1\}, \quad x, y \in \mathbb{Z}, \quad xy \neq 0,$$

has no solutions with $2p \nmid y$, except $1^p + 1 = 2 \cdot (\pm 1)^2$ and $3^5 - 1 = 2 \cdot (\pm 11)^2$. In 1995, Le [3] proved that if $p > 3$, then the equation

$$x^p - 2^n = py^2, \quad x, y, n \in \mathbb{N}, \quad \gcd(x, y) = 1,$$

has no solutions. Rabinowitz [4] found all solutions of the equations

$$x^3 \pm 2^n = 3y^2, \quad x, y, n \in \mathbb{Z}.$$

Now, from [1] and [2] we have that the equation

$$x^p - 1 = py^2, \quad x, y \in \mathbb{Z},$$

has no solutions since the class number $h(-p)$ of $\mathbb{Q}(\sqrt{-p})$ is less than p .

In this paper, we will discuss the solvability of the equations

$$(1) \quad x^p + 1 = py^2, \quad x, y \in \mathbb{Z}, \quad y \neq 0,$$

and

$$(2) \quad x^p + 2^{2m} = py^2, \quad x, y \in \mathbb{Z}, \quad m \in \mathbb{N}, \quad \gcd(x, y) = 1,$$

Received by the editors September 8, 1998.

2000 *Mathematics Subject Classification*. Primary 11D61, 11D41.

Key words and phrases. Exponential Diophantine equation, higher degree Diophantine equation, Adachi's theorem, Pell's equation, Bernoulli number.

by using a theorem of Adachi [5] and a result of the author [6], [7] on Pell's equation. Let B_n denote n th Bernoulli number. We prove the following:

Theorem. *If $p \equiv 1 \pmod{4}$ and $p \nmid B_{(p-1)/2}$, then we have that*

- (A) *equation (1) has no solutions;*
- (B) *equation (2) has no solutions with $p \mid y$.*

§2. PRELIMINARIES

We use the following lemmas to prove our theorem.

Lemma 1 (Adachi [5]). *If $p \equiv 1 \pmod{4}$, $p \nmid B_{(p-1)/2}$ and $p \mid y$, then all solutions of the equation*

$$x^2 - py^2 = z^p, \quad x, y, z \in \mathbb{Z}, \quad \gcd(x, y) = 1, \quad 2 \nmid x + y,$$

are given by $z = a^2 - pb^2$,

$$x + y\sqrt{p} = (a + b\sqrt{p})^p,$$

where $a, b \in \mathbb{Z}$, $\gcd(a, b) = 1$.

Lemma 2 (Cao [6], [7]). *Let $a, b \in \mathbb{N}$ with ab not a square. If $c \in \{1, 2, 4\}$, $1 < a \neq c$ and there exist $x, y \in \mathbb{N}$ such that*

$$ax^2 - by^2 = c, \quad x \mid^* a \text{ or } y \mid^* b,$$

where symbol $x \mid^ a$ means that each prime factor of x divides a , then*

$$\frac{ax^2 + by^2}{2} + xy\sqrt{ab} = \begin{cases} \frac{1}{2}\varepsilon & \text{or } \frac{1}{2}\varepsilon^3, & \text{for } c = 1, \\ \varepsilon & \text{or } \varepsilon^3, & \text{for } c = 2, \\ \Omega & \text{or } \frac{1}{4}\Omega^3, & \text{for } c = 4, \end{cases}$$

except $(a, b, c, x, y) = (5, 1, 4, 5, 11)$. Here $\varepsilon = u_0 + v_0\sqrt{ab}$ and $\Omega = U_0 + V_0\sqrt{ab}$ is the least positive integer solution of Pell's equation $u^2 - abv^2 = 1$ and $U^2 - abV^2 = 4$, respectively.

Lemma 3. *Let $p \equiv 1 \pmod{4}$, and $D_1, D_2 \in \mathbb{Z}$. If $m \in \mathbb{N}$ and $2 \nmid D_1x^2 - D_2y^2$, then the equation*

$$(3) \quad 2^{m+1}\sqrt{D_1} = (x\sqrt{D_1} + y\sqrt{D_2})^p + (x\sqrt{D_1} - y\sqrt{D_2})^p, \quad x, y \in \mathbb{Z},$$

has no solutions.

Proof. From the binomial formula and (3), we obtain that

$$\begin{aligned} 2^{m+1}\sqrt{D_1} &= \sum_{j=0}^p \binom{p}{j} (x\sqrt{D_1})^{p-j} (y\sqrt{D_2})^j + \sum_{j=0}^p \binom{p}{j} (x\sqrt{D_1})^{p-j} (-y\sqrt{D_2})^j \\ &= 2 \sum_{j=0}^{(p-1)/2} \binom{p}{2j} (x\sqrt{D_1})^{p-2j} (y\sqrt{D_2})^{2j} \\ &= 2x\sqrt{D_1} \sum_{j=0}^{(p-1)/2} \binom{p}{2j} (D_1x^2)^{(p-1)/2-j} (D_2y^2)^j. \end{aligned}$$

Hence, we have $x = \pm 2^m$, $2 \nmid D_2 y^2$, and

$$\begin{aligned}
 (4) \quad \pm 1 &= \sum_{j=0}^{(p-1)/2} \binom{p}{2j} (2^{2m} D_1)^{(p-1)/2-j} (D_2 y^2)^j \\
 &= \sum_{j=0}^{(p-1)/2} \binom{p}{p-1-2j} (2^{2m} D_1)^j (D_2 y^2)^{(p-1)/2-j} \\
 &= \sum_{j=0}^{(p-1)/2} \binom{p}{2j+1} (2^{2m} D_1)^j (D_2 y^2)^{(p-1)/2-j}.
 \end{aligned}$$

Let $2^a \parallel p-1$. Then $a \geq 2$ since $p \equiv 1 \pmod{4}$. Since $2 \nmid D_2 y^2$, we have

$$(5) \quad (D_2 y^2)^{(p-1)/2} = ((D_2 y^2)^{(p-1)/2^a})^{2^{a-1}} \equiv 1 \pmod{2^{a+1}}.$$

Also, let $2^b \parallel 2j$, $b \geq 1$. Then we have $2j \geq b+1$ for $j \geq 1$. So if $j \geq 1$, then

$$\begin{aligned}
 (6) \quad \binom{p}{2j+1} 2^{2mj} &= \frac{p(p-1)}{(2j+1)(2j)} \binom{p-2}{2j-1} 2^{2mj} \\
 &\equiv 0 \pmod{2^{a+1}}.
 \end{aligned}$$

Thus, from (4), (5) and (6) we have

$$\begin{aligned}
 \pm 1 &= p(D_2 y^2)^{(p-1)/2} \\
 &\quad + \sum_{j=1}^{(p-1)/2} \binom{p}{2j+1} (2^{2mj} D_1^j) (D_2 y^2)^{(p-1)/2-j} \\
 &\equiv p \equiv 2^a + 1 \pmod{2^{a+1}},
 \end{aligned}$$

which is impossible since $a \geq 2$.

This completes the proof of Lemma 3.

§3. PROOF OF THE THEOREM

Proof of (A). Suppose (x, y, p) is a solution of equation (1). Then

$$(7) \quad 1 - py^2 = (-x)^p, \quad x, y \in \mathbb{Z}, \quad y \neq 0.$$

From [2] and (1), we see that $2p \mid y$. Hence, by Lemma 1, we get from (7) that

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

where $a, b \in \mathbb{Z}$, $\gcd(a, b) = 1$ and $2 \nmid a^2 - pb^2$. Clearly, (8) gives $a \mid 1$ and so $a = \pm 1$. So $-x = 1 - pb^2$, and from (7) we have

$$(9) \quad py^2 - (pb^2 - 1) \left((pb^2 - 1)^{(p-1)/2} \right)^2 = 1.$$

If $b = 0$, then $y = 0$ by (9). If $b \neq 0$, by Lemma 2, then we have from (9) that

$$(10) \quad py^2 + (pb^2 - 1) \left((pb^2 - 1)^{(p-1)/2} \right)^2 + 2y(pb^2 - 1)^{(p-1)/2} \sqrt{p(pb^2 - 1)} = \varepsilon \text{ or } \varepsilon^3,$$

where $\varepsilon = u_0 + v_0 \sqrt{p(pb^2 - 1)}$ is the least positive integer solution of Pell's equation

$$(11) \quad u^2 - p(pb^2 - 1)v^2 = 1.$$

Clearly, $(u, v) = (2pb^2 - 1, 2|b|)$ is a positive integer solution of Pell's equation (11). It is well known [8] that if (u_1, v_1) is a positive integer solution of equation (11) and $u_1 > \frac{1}{2}v_1^2 - 1$, then $u_1 + v_1\sqrt{p(pb^2 - 1)}$ is the least positive integer solution of equation (11). So $\varepsilon = 2pb^2 - 1 + 2|b|\sqrt{p(pb^2 - 1)}$. Since

$$\begin{aligned}\varepsilon^3 = & (2pb^2 - 1) \left((2pb^2 - 1)^2 + 12pb^2(pb^2 - 1) \right) \\ & + 2|b| \left(3(2pb^2 - 1)^2 + 4pb^2(pb^2 - 1) \right) \sqrt{p(pb^2 - 1)},\end{aligned}$$

we get from (10) that

$$(12) \quad \begin{aligned}py^2 + (pb^2 - 1) \left((pb^2 - 1)^{(p-1)/2} \right)^2 &= 2pb^2 - 1, \\ y(pb^2 - 1)^{(p-1)/2} &= |b|,\end{aligned}$$

or

$$(13) \quad \begin{aligned}py^2 + (pb^2 - 1) \left((pb^2 - 1)^{(p-1)/2} \right)^2 &= (2pb^2 - 1) \left((2pb^2 - 1)^2 + 12pb^2(pb^2 - 1) \right), \\ y(pb^2 - 1)^{(p-1)/2} &= |b| \left(3(2pb^2 - 1)^2 + 4pb^2(pb^2 - 1) \right).\end{aligned}$$

Clearly, (12) is impossible. For (13), by (9) we have

$$2(pb^2 - 1) \left((pb^2 - 1)^{(p-1)/2} \right)^2 + 1 = (2pb^2 - 1) (16pb^2(pb^2 - 1) + 1),$$

i.e.

$$(pb^2 - 1)^{(p-1)/2} = 4pb^2 - 1,$$

which also is impossible. (A) of the Theorem is proved.

Proof of (B). Suppose (x, y, p, m) is a solution of equation (2) with $p \mid y$. By Lemma 1, we get from (2) that

$$(14) \quad 2^m + y\sqrt{p} = (a + b\sqrt{p})^p, \quad -x = a^2 - pb^2,$$

where $a, b \in \mathbb{Z}$, $\gcd(a, b) = 1$ and $2 \nmid a^2 - pb^2$. By Lemma 3, (14) is impossible since (14) implies that

$$2^{m+1} = (a + b\sqrt{p})^p + (a - b\sqrt{p})^p.$$

Hence, (B) of the Theorem is proved.

ACKNOWLEDGEMENTS

The author would like to thank the referee for his valuable suggestions.

REFERENCES

1. T. Nagell, *Sur l'impossibilité de quelques équations à deux indéterminées*, Norsk Mat. Forenings Skriffter (1) **13** (1921), 65-82.
2. Zhenfu Cao, *On the Diophantine equation $x^p - y^p = Dz^2$ (Chinese)*, Northeast Math. J. **2** (1986), 219-227. MR **88b**:11013
3. Maohua Le, *On the Diophantine equation $2^n + px^2 = y^p$* , Proc. Amer. Math. Soc. **123** (1995), 321-326. MR **95c**:11038
4. S. Rabinowitz, *The solutions of $3y^2 \pm 2^n = x^3$* , Proc. Amer. Math. Soc. **69** (1978), 213-218. MR **58**:499
5. Norio Adachi, *The Diophantine equation $x^2 \pm ly^2 = z^l$ connected with Fermat's last theorem*, Tokyo J. Math. **11** (1988), 85-94. MR **89g**:11023
6. Zhenfu Cao, *On the equation $ax^m - by^n = 2$ (Chinese)*, Chinese Sci. Bull. **35** (1990), 558-559.

7. Zhenfu Cao, *On the Diophantine equation $(ax^m - 4c)/(abx - 4c) = by^2$ (Chinese)*, J. Harbin Inst. Tech. (1991), suppl. 110-112. MR **95f**:11021
8. Zhenfu Cao, *Introduction to Diophantine equations (Chinese)*, Harbin Inst. Tech. Press, 1989; (pp.154-155). MR **92e**:11018

DEPARTMENT OF MATHEMATICS, HARBIN INSTITUTE OF TECHNOLOGY, HARBIN 150001, PEOPLE'S REPUBLIC OF CHINA

E-mail address: `zfcao@hope.hit.edu.cn`