Publ. Math. Debrecen
80/3-4 (2012), 327–331
DOI: 10.5486/PMD.2012.5004

On the diophantine equation $(a^n - 1)(b^n - 1) = x^2$

By PINGZHI YUAN (Guangzhou) and ZHONGFENG ZHANG (Zhaoqing)

Abstract. Let a and b be distinct positive integers. In this paper, we will present some new results on the positive integer solutions (n, x) of the equation of the title.

1. Introduction

Let $\mathbb{N}^+$ denote the set of all positive integers, and let $a, b \in \mathbb{N}^+$. There are some results on the following equation

$$(a^n - 1)(b^n - 1) = x^2. \tag{1.1}$$

Szalay [7] has shown that equation (1.1) has no solution for $(a, b) = (2, 3)$, only the solution $n = 1$ for $(2, 5)$, and for $(2, 2^k)$ has no solutions with $k \geq 2$ except for $n = 3$ and $k = 2$. Hajdu and Szalay [3] proved that (1.1) has no solution for $(2, 6)$ and for (a, a^k), there are no solutions with $k \geq 2$ and $kn > 2$ except for the three cases $(a, n, k) = (2, 3, 2), (3, 1, 5)$ and $(7, 1, 4)$. Walsh [9] proved that equation $(2^n - 1)(3^m - 1) = z^2$ has no positive integer solutions (n, m, x). Cohn [2] obtained some general results for equation (1.1). He proved that there is no solution to (1.1) when $n = 4$, except for $(a, b) = (13, 239)$.

Luca and Walsh [6] have shown that the equation

$$(a^k - 1)(b^k - 1) = x^n \tag{1.2}$$

Mathematics Subject Classification: 11D31.
Key words and phrases: exponential diophantine equations, Pell equations.
The corresponding author and he is supported by the Guangdong Provincial Natural Science Foundation (No. 8151027501000114) and NSF of China (No. 10971072).

has finitely many solutions in positive integers (k, x, n) with $n > 1$. Moreover, they showed how one can determine all solutions of the equation (1.1) with $n > 1$, for almost all pairs (a, b) with $2 \le b < a \le 100$. Recently, Le [5] proved that if $3|b$, then the equation

$$(2^n - 1)(b^n - 1) = x^2 \tag{1.3}$$

has no solutions in positive integers n and x. Tang [8] showed that (1.1) has no solutions for (a, b) with $a \equiv 0 \pmod 2$ and $b \equiv 15 \pmod{20}$ or $a \equiv 2 \pmod 6$ and $b \equiv 0 \pmod 3$. Li and Szalay [4] proved that (1.1) has no solution if $a \equiv 2 \pmod 6$ and $b \equiv 0 \pmod 3$.

In this paper we prove the following result. This theorem generalizes the results in [7] (Theorem 1), in [3], in [5] and in [4] (Theorem 1).

Theorem. $a, b \in \mathbb{N}^+$. *Suppose that one of the following properties is satisfied:*

i) $a \equiv 2 \pmod 3$ *and* $b \equiv 0 \pmod 3$,

ii) $a \equiv 3 \pmod 4$ *and* $b \equiv 0 \pmod 2$,

iii) $a \equiv -1 \pmod 5$ *and* $b \equiv 0 \pmod 5$.

Then equation (1.1) *has no positive integer solutions* (n, x) *with* $n > 2$.

To prove our result, beside combining some known tools from [2], [4], [6], we introduce a new one as well: a result of Bennett and Skinner concerning ternary equations of signature $(n, n, 2)$.

2. Lemmas and the proof of the Theorem

To prove the Theorem, we need some results on divisibility properties of the solutions of Pell equation and some known results.

Let D be a non-square positive integer. It is well-known that the Pell equation

$$u^2 - Dv^2 = 1, \quad u, v \in \mathbb{N}^+ \tag{2.1}$$

has infinitely many solutions (u, v). If $(u, v) = (u_1, v_1)$ denotes the fundamental solution to equation (2.1), then every positive solution $(u_k, v_k)\,(k \in \mathbb{N}^+)$ can be represented by

$$u_k + v_k\sqrt{D} = \left(u_1 + v_1\sqrt{D}\,\right)^k, \quad k = 1, 2, \dots . \tag{2.2}$$

First, we need the following simple lemma.

Lemma 1. (i) $u_1|u_k$ *if and only if* $2\nmid k$.

(ii) *If* $q\in\{2,3,5\}$, *then* $q|u_k$ *implies that* k *is odd and* $q|u_1$.

(iii) $u_{2k}=2u_k^2-1$.

For the proof of the above lemma, we refer to [4] Lemma 1 or the more general result of the first author [10].

The following lemma is Theorem 1.1 in [1]. It plays a key role in the proof of our Theorem.

Lemma 2. *If* $n\geq 3$, *then the diophantine equation*

$$x^n=2y^2-1 \tag{2.3}$$

has no solution (x,y) *with* $x>1$.

The following lemma is an immediate consequence of Result 2 of [2].

Lemma 3. *The diophantine equation*

$$(a^{4m}-1)(b^{4n}-1)=z^2 \tag{2.4}$$

has the only positive integer solution $(a,b,m,n,z)=(13,239,1,1,9653280)$.

Proof of the Theorem. We prove only part i) of the statement, the proof of the other parts are similar. Let $a\equiv 2 \pmod 3$ and $b\equiv 0 \pmod 3$, and suppose that (n,x) is a solution to equation (1.1). Put $D=\gcd(a^n-1,b^n-1)$. By (1.1), we get

$$a^n-1=Dy^2,\ b^n-1=Dz^2,\ x=Dyz,\quad D,y,z\in\mathbb{N}^+. \tag{2.5}$$

Since $3|b$, by $b^n-1=Dz^2$, it follows that

$$D\equiv -1 \pmod 3 \quad\text{and}\quad 3\nmid z. \tag{2.6}$$

Now we distinguish two cases. Firstly, if $3\nmid y$, then $y^2\equiv 1 \pmod 3$, and (2.5), together with (2.6) implies

$$a^n=Dy^2+1\equiv D+1\equiv 0 \pmod 3, \tag{2.7}$$

which contradicts $a\equiv 2 \pmod 3$.

Assume now that $3|y$. Since $a\equiv 2 \pmod 3$, by $a^n-1=Dy^2$ we obtain

$$2^n\equiv a^n\equiv Dy^2+1\equiv 1 \pmod 3, \tag{2.8}$$

which implies that n is even.

Put $n = 2m$. Therefore, by (2.5), D cannot be a square, and the corresponding Pell equation $u^2 - Dv^2 = 1$ has two solutions

$$(x, y) = (a^m, y),\ (b^m, z). \tag{2.9}$$

Since $a \neq b$, there exist distinct positive integers r and s such that

$$(a^m, y) = (u_r, v_r) \quad \text{and} \quad (b^m, z) = (u_s, v_s) \tag{2.10}$$

hold.

By Lemma 1 (ii) and $3|b$, we obtain that $2 \nmid s$ and $3|u_1$. On the other hand, $a \equiv 2 \pmod 3$, which together with $3|u_1$ and Lemma 1 (i), shows that $2|r$.

Put $r = 2t$, then by Lemma 1 (iii),

$$u_{2t} = 2u_t^2 - 1 = a^m. \tag{2.11}$$

Now we distinguish two cases. Firstly, if $2|m$, then $4|n$, and so Lemma 2.3 implies that $(a, b) = (13, 239)$, which contradicts $3|b$. Now we assume that $2 \nmid m$ and $m > 1$, then Lemma 2 implies that (2.11) has no positive integer solutions, a contradiction. $\square$

Remark. By [2] Result 4 and the above proof, it is easy to see equation

$$(a^2 - 1)(b^2 - 1) = z^2, \quad a, b, z \in \mathbb{N}^+$$

has infinitely many solutions (a, b, x) with $a \equiv 5 \pmod 6$ and $b \equiv 0 \pmod 3$.

ACKNOWLEDGMENTS. The authors are grateful to the referee for his valuable suggestions.

References

[1] M. A. BENNETT and C. SKINNER, Ternary Diophantine equations via Galois representations and modular forms, *Canad. J. Math.* **56** (2004), 23–54.

[2] J. H. E. COHN, The diophantine equation $(a^n - 1)(b^n - 1) = x^2$, *Period. Math. Hungar.* **44**(2) (2002), 169–175.

[3] L. HAJDU and L. SZALAY, On the diophantine equation $(2^n - 1)(6^n - 1) = x^2$ and $(a^n - 1)(a^{kn} - 1) = x^2$, *Period. Math. Hungar.* **40**(2) (2000), 141–145.

[4] L. LAN and L. SZALAY, On the exponential diophantine equation $(a^n - 1)(b^n - 1) = x^2$, *Publ. Math. Debrecen* **77** (2010), 465–470.

[5] M. LE, A note on the exponential diophantine equation $(2^n - 1)(b^n - 1) = x^2$, *Publ. Math. Debrecen* **3-4** (2009), 453–455.

[6] F. Luca and P. G. Walsh, The product of like-indexed terms in binary recurrences, *J. Number Theory* **96**(1) (2002), 152–173.

[7] L. Szalay, On the diophantine equation $(2^n-1)(3^n-1)=x^2$, *Publ. Math. Debrecen* **57** (2000), 1–9.

[8] M. Tang, A note on the exponential diophantine equation $(a^m-1)(b^n-1)=x^2$, *J. Math. Res. & Expo.* **31** (2011), 1064–1066.

[9] P. G. Walsh, On Diophantine equations of the form $(x^n-1)(y^m-1)=z^2$, *Tatra Mt. Math. Publ.* **20** (2000), 87–89.

[10] P. Yuan, A note on the divisibility of the generalized Lucas sequences, *Fibonacci Quart.* **40** (2002), 153–156.

PINGZHI YUAN
SCHOOL OF MATHEMATICS
SOUTH CHINA NORMAL UNIVERSITY
GUANGZHOU 510631
P.R. CHINA

E-mail: yuanpz@scnu.edu.cn

ZHONGFENG ZHANG
COLLEGE OF MATHEMATICS
AND INFORMATION SCIENCE
ZHAOQING UNIVERSITY
ZHAOQING,526061
P.R. CHINA

E-mail: zh12zh31f@yahoo.com.cn

(Received September 15, 2010; revised November 29, 2011)