Publ. Math. Debrecen
77/3-4 (2010), 465–470

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

By LI LAN (Xi'an) and LÁSZLÓ SZALAY (Sopron)

Abstract. Let a and b be fixed positive integers such that $a \neq b$ and $\min(a, b) > 1$. In this paper, we combine some divisibility properties of the solutions of Pell equations with elementary arguments to prove that if $a \equiv 2 \pmod 6$ and $b \equiv 0 \pmod 3$, then the title equation $(a^n - 1)(b^n - 1) = x^2$ has no positive integer solution (n, x). Moreover, we show that in case of $a \equiv 2 \pmod{20}$ and $b \equiv 5 \pmod{20}$, where $b - 1$ is a full square, the only possible solution belongs to $n = 1$.

1. Introduction

Let $\mathbb{N}^+$ denote the set of all positive integers, further let a and b be distinct fixed positive integers such that $\min(a, b) > 1$. In this paper, we discuss the problem of the solution to the exponential diophantine equation

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

in some particular cases.

The literature of this equation and its alternations is very rich, see e.g. the papers [6], [2], [1], [5], [4]and the references given there. First, SZALAY [6], using a relatively complicated method, proved that if $(a, b) = (2, 3)$ then equation (1) has no solution. He also showed that only $(n, x) = (1, 2)$ satisfies $(2^n - 1)(5^n - 1) = x^2$. Then, HAJDU and SZALAY [2] justified the insolubility of (1) when $(a, b) = (2, 6)$,

Mathematics Subject Classification: 11D61.
Key words and phrases: exponential diophantine equation, Pell equation, divisibility.
Supported by the Shaanxi Provincial Department of Education Natural Science Foundation (No. 09Jk708).
The research is supported by Hungarian National Foundation for Scientific Research Grant No. T 61800 FT.

further they determined all the solutions if $a > 1$ is an arbitrary integer and $b = a^k$. This result was extended by Cohn [1] to the case $a^k = b^l$. He also proved that there is no solution to (1) when $4 \mid n$, except for $(a, b) = (13, 239)$. Luca and Walsh [5] described a computational method for solving (1), and their approach was used to solve completely the equations for almost all pairs (a, b) in the range $1 < a < b \leq 100$. Recently, Le [4] showed that equation (1) is insoluble if $a = 2$ and $3 \mid b$.

Several problems and conjectures linked to the title equation have already been posed (see [1], [5], [4]).

The main purpose of this paper is to prove the following general results by combining certain divisibility properties of the solutions of Pell equations, and partially applying the techniques described in [4] and [5].

Theorem 1. *If* $a \equiv 2 \pmod 6$ *and* $b \equiv 0 \pmod 3$ *then the equation* $(a^n - 1)(b^n - 1) = x^2$ *has no positive integer solution* (n, x).

Theorem 2. *Suppose that* $b - 1 = t^2$ *is a full square. If* $a \equiv 2 \pmod{20}$ *and* $b \equiv 5 \pmod{20}$ *then the only possible solution to the equation* $(a^n - 1)(b^n - 1) = x^2$ *is*

$$(n, x) = (1, t\sqrt{a - 1}\,).$$

Theorem 1 states that there is no solution in at least $\frac{1}{18}$ part of the possible integer pairs (a, b). At the same time, this theorem generalizes the results appearing in [6] (Theorem 1), in [2] (Theorem 1), and in [4], while Theorem 2 extends Theorem 2 of [6].

It is worthwhile noting that if one replaces the condition $b \equiv 5 \pmod{20}$ in Theorem 2 by the weaker relation $b \equiv 0 \pmod 5$ then our approach does not work. Although, the cases $b \equiv -5 \pmod{20}$ and $b \equiv 0(\pmod{20}$ can be handled trivially by applying modulo 20 arithmetic, in case of $b \equiv 10 \pmod{20}$ the method fails.

Obviously, there are infinitely many pairs (a, b) satisfying the conditions of Theorem 2. In particular, by choosing a such that $a - 1$ is a perfect square, we get equations (1) having unique solutions.

2. Divisibility properties of the solutions of Pell equation

Let D be a positive integer which is not a square. It is well known (see, for example, [3] (Theorems 10.9.1 and 10.9.2)) that the Pell equation

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

has infinitely many solutions (u,v). If $(u,v)=(u_1,v_1)$ denotes the smallest non-trivial positive solution to equation (2) then every positive solution (u_k,v_k) $(k\in\mathbb{N}^+)$ can be generated by

$$u_k+v_k\sqrt{D}=\left(u_1+v_1\sqrt{D}\,\right)^k. \tag{3}$$

The trivial solution $(u,v)=(1,0)$ is denoted by (u_0,v_0).

The proof of the Theorems 1 and 2 partially relies on

Lemma 1. (i) *If $2\mid k$ then $2\nmid u_k$.*

(ii) *If $2\mid k$ then each prime factor p of u_k satisfies $p\equiv\pm1 \pmod 8$.*

(iii) *If $2\nmid k$ then $u_1\mid u_k$.*

(iv) *If q is a prime in the set $\{2,3,5\}$ then $q\mid u_k$ implies $q\mid u_1$.*

We remark that the feature (iv) is not valid longer in its form for $p\geq 7$ since, for instance, the fundamental solution to $u^2-3v^2=1$ is $(u_1,v_1)=(2,1)$, $7\mid u_2=7$ but $7\nmid u_1$.

Proof of Lemma 1. (i) Let $k=2t$, where t is positive integer. By (3), we have

$$\begin{aligned} u_k+v_k\sqrt{D}&=\left(u_1+v_1\sqrt{D}\,\right)^{2t}=\left(\left(u_1+v_1\sqrt{D}\,\right)^t\right)^2\\ &=\left(u_t+v_t\sqrt{D}\,\right)^2=(u_t^2+Dv_t^2)+2u_tv_t\sqrt{D}. \end{aligned} \tag{4}$$

Further, $u_t^2-Dv_t^2=1$ holds since $(u,v)=(u_t,v_t)$ is the solution to equation (2). Consequently,

$$u_k=u_t^2+Dv_t^2=2u_t^2-1 \tag{5}$$

implies that u_k is an odd number. In other words, if u_k is an even number then the subscript k must be odd.

(ii) From part (i) of Lemma 1 it follows, that if k is even then all prime factors p of u_k are odd. For such a p, by (5), the Legendre symbol $\left(\frac{2}{p}\right)$ equals 1. Thus $p\equiv\pm1 \pmod 8$.

(iii) If $2\nmid k$, then by (3), together with the binomial theorem, we obtain immediately

$$u_k=u_1\sum_{i=0}^{(k-1)/2}\binom{k}{2i}u_1^{k-2i-1}(Dv_1^2)^i, \tag{6}$$

which implies $u_1\mid u_k$.

(iv) It is easy to see, that the terms of the sequence of u_k satisfy the recurrence relation $u_{k+1}=2u_1u_k-u_{k-1}$. Since the sequence u_k is periodic modulo any

positive integer, so if $p = 2, 3, 5$, we have to eliminate those cases where $p \mid u_k$ occurs. Recall, that $u_0 = 1$ and note that the recurrence $u_{k+1} = 2u_1u_k - u_{k-1}$ is valid modulo p, too. We find that by any of the three possibilities for p,

$$p \mid u_k \text{ if and only if } k \equiv 1 \pmod 2 \text{ and } u_1 \equiv 0 \pmod p. \qquad \square$$

3. Proof of the theorems

Proof of Theorem 1. Let $a \equiv 2 \pmod 6$ and $b \equiv 0 \pmod 3$, and suppose that the pair (n, x) is a solution to equation (1). Put $D = \gcd(a^n - 1, b^n - 1)$. By (1), we get

$$a^n - 1 = Dy^2, \quad b^n - 1 = Dz^2, \quad x = Dyz, \qquad D, y, z \in \mathbb{N}^+. \tag{7}$$

Since $3 \mid b$, by $b^n - 1 = Dz^2$ it follows that $3 \nmid D$ and $3 \nmid z$. Hence $z^2 \equiv 1 \pmod 3$. Consequently,

$$D \equiv Dz^2 = b^n - 1 \equiv 2 \pmod 3. \tag{8}$$

Now we distinguish two cases. Firstly, if $3 \nmid y$, then $y^2 \equiv 1 \pmod 3$, and (7), together with (8) implies

$$a^n = Dy^2 + 1 \equiv D + 1 \equiv 0 \pmod 3. \tag{9}$$

However, it contradicts $a \equiv 2 \pmod 3$. Thus we can exclude $3 \nmid y$.

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

$$2^n \equiv a^n = Dy^2 + 1 \equiv 1 \pmod 3. \tag{10}$$

Clearly, $2^n \equiv \pm 1 \pmod 3$, and $+1$ is occurring exactly when n is even.

Put $n = 2m$. Therefore, by (7), D cannot be a square, and the corresponding Pell equation $u^2 - Dv^2 = 1$ has two solutions

$$(u, v) = (a^m, y), \ (b^m, z). \tag{11}$$

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

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

hold.

If s is even , by (ii) of Lemma 1 we know that any prime factor p of b satisfies $p \equiv \pm 1 \pmod 8$. But it is impossible since $3 \mid b$. Therefore, s must be odd.

Hence, by (iv) of Lemma 1 and $3 \mid b$ we obtain $3 \mid u_1$. On the other hand, $2 \mid a$ which, together with (i) of Lemma 1 and $(a^m, y) = (u_r, v_r)$ shows that r is odd. However, by the statement (iii) of Lemma 1 and $3 \mid u_1$ we have $3 \mid a^m$, which leads to a contradiction, since $a \equiv 2 \pmod 6$. This completes the proof of Theorem 1. □

Proof of Theorem 2. Now let $a \equiv 2 \pmod{20}$ and $b \equiv 5 \pmod{20}$, where $b-1$ is a square of a nonzero integer t. First, we deal with even exponents n in the proof of Theorem 2. Replace the prime 3 by 5 in the proof of Theorem 1, and repeat step by step arguments handling the case $n = 2m$ to obtain the statement in this case.

Assume now that n is odd. Suppose that there is a non-negative integer m such that $n = 4m+3$. Consider the equation $(a^n-1)(b^n-1) = x^2$ modulo 10. Obviously,

$$x^2 = (a^{4m+3}-1)(b^{4m+3}-1) \equiv (2^{4m+3}-1)(5^{4m+3}-1) \equiv 7 \cdot 4 \equiv 8 \pmod{10},$$

which is impossible since 8 is not a quadratic residue modulo 10.

Finally, let $n = 4m+1$ for some non-negative integer m. Recall, that $b-1 = t^2$. Thus, if (n, x) is a solution to (1) then

$$(a^{4m+1}-1)(b^{4m}+b^{4m-1}+\cdots+b+1) = \left(\frac{x}{t}\right)^2 \in \mathbb{N}. \tag{12}$$

Suppose that $m>0$ and consider (12) modulo 4 to obtain $(2^{4m+1}-1)(4m+1) \equiv 3 \cdot 1 = 3$, which is not a quadratic residue modulo 4. Thus we arrive at a contradiction. If $m = 0$, equation (12) simplifies

$$\left(\frac{x}{t}\right)^2 = a-1.$$

That is, if $a-1$ is a full square then there is exactly one solution $(n, x) = (1, t\sqrt{a-1}\,)$. The proof of Theorem 2 is complete. □

References

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

[2] 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.

[3] L. G. Lua, Introduction to Number Theory, *Science Press, Beijing*, 1979 (in *Chinese*).

[4] M. H. Le, A note on the exponential diophantine equation $(2^n - 1)(b^n - 1) = x^2$, *Publ. Math. Debrecen* **74**(3–4) (2009), 453–455.

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

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

LI LAN
DEPARTMENT OF MATHEMATICS
XI'AN UNIVERSITY OF ARTS & SCIENCE
XI'AN 710065
P.R. CHINA

E-mail: lanli98@126.com

LÁSZLÓ SZALAY
INSTITUTE OF MATHEMATICS AND STATISTICS
UNIVERSITY OF WEST HUNGARY
SOPRON
HUNGARY

E-mail: laszalay@ktk.nyme.hu

(Received August3, 2009; revised April 22, 2010)