

A note on the exponential Diophantine equation $(a^n - 1)(b^n - 1) = x^2$

Armand Noubissie^a, Alain Togbé^b

^aInstitut de Mathématiques et de Sciences Physiques, Dangbo, Bénin
armand.noubissie@imsp-uac.org

^bDepartment of Mathematics, Statistics and Computer Science
Purdue University Northwest, Westville, USA
atogbe@pnw.edu

Submitted: June 13, 2019
Accepted: November 19, 2019
Published online: December 1, 2019

Abstract

Let a and b be two distinct fixed positive integers such that $\min\{a, b\} > 1$. We show that the equation in the title with $b \equiv 3 \pmod{12}$ and a even has no solution in positive integers (n, x) . This generalizes a result of Szalay [9]. Moreover, we show that this equation in the title with $(a \equiv 4 \pmod{10}$ and $b \equiv 0 \pmod{5})$ has no solution in positive integer (n, x) . We give a necessary and sufficient condition for Diophantine equation $(a^n - 1)(b^n - 1) = x^2$ with $(a \equiv 4 \pmod{5}$ and $b \equiv 0 \pmod{5})$ or $(a \equiv 3 \pmod{4}$ and $b \equiv 0 \pmod{2})$ to have positive integer solutions. Finally, we prove that the equation with a even, $\vartheta_2(b - 1) = 1$ and $5 \mid b$ has no solution in positive integer (n, x) , where ϑ_2 is the 2-adic valuation.

Keywords: Pell equation, exponential Diophantine equation.

MSC: 11D41, 11D61

1. Introduction

Let \mathbb{N}^+ be the set of all positive integers. Let $a > 1$ and $b > 1$ be different fixed integers. The exponential Diophantine equation

$$(a^n - 1)(b^n - 1) = x^2, \quad x, n \in \mathbb{N}^+ \tag{1.1}$$

has been studied by many authors in the literature since 2000. First, Szalay [9] studied equation (1.1) for $(a, b) = (2, 3)$ and showed that this equation has no positive integer solutions. He also proved that equation (1.1) has only the positive integer solution $(n, x) = (1, 2)$, for $(a, b) = (2, 5)$ and there is no solution, for $(a, b) = (2, 2^k)$ with $k \geq 2$ except when $n = 3$ and $k = 2$. Hajdu and Szalay [3] proved that equation (1.1) has no solution for $(a, b) = (2, 6)$ and for $(a, b) = (a, a^k)$, there is no solution with $k \geq 2$ and $kn > 2$ except for the three cases $(a, n, k) = (2, 3, 2), (3, 1, 5), (7, 1, 4)$. So their result generalized Theorem 3 of [9]. This result was extended by Cohn [2] to the case $a^k = b^l$ (see RESULT 1). Cohn also proved that there are no solutions to (1.1) when $4 \mid n$, except for $\{a, b\} = \{13, 239\}$ with $n = 4$. Walsh and Luca [7] proved equation (1.1) has finitely positive solutions for fixed (a, b) and showed that the equation has no solution with $n > 2$ for some pairs (a, b) in the range $1 < a < b \leq 100$. Theorem 1.1 completes this result ([7, Theorem 3.1]) for some special cases. Since then, many authors studied equation (1.1) by introducing some special constraints to a or b (see for examples [4, 6, 8, 10, 11]). Yuan and Zhang [11] showed that equation (1.1) has no solution with $n > 2$ if $(a \equiv 2 \pmod{3} \text{ and } b \equiv 0 \pmod{3})$ or $(a \equiv 4 \pmod{5} \text{ and } b \equiv 0 \pmod{5})$ or $(a \equiv 3 \pmod{4} \text{ and } b \equiv 0 \pmod{2})$. But this proof was not complete because Lemma 2 in their paper is not correct. The authors and Z. Zhang completed the proof of this theorem (see [8]). In 2013, Xiaoyan [10] showed that equation (1.1) has no solution with $n > 2$ and $2 \mid n$ when $\vartheta_2(a-1)$ and $\vartheta_2(b-1)$ have the opposite parity. In 2016, Ishii [4] gave a necessary and sufficient condition for equation (1.1) with the conditions $(a \equiv 5 \pmod{6} \text{ and } b \equiv 0 \pmod{3})$ to have positive integer solutions. Theorem 1.4 and Theorem 1.5 give a necessary sufficient condition for Diophantine equation (1.1) with $(a \equiv 4 \pmod{5} \text{ and } b \equiv 0 \pmod{5})$ or $(a \equiv 3 \pmod{4} \text{ and } b \equiv 0 \pmod{2})$ to have positive integer solutions with $n \geq 2$. In 2018, Keskin [5] showed that equation (1.1) has no solution in positive integer with $2 \mid n$ when a and b have the opposite parity. Recently, the authors of [8] showed that equation (1.1) has no solution in positive integer when a is even and $b \equiv 3 \pmod{8}$ with b a prime number.

In this paper, we will show that equation (1.1) has no positive solution (n, x) under some constraints on a and b . Our main results are the following.

Theorem 1.1. *Let $a, b \in \mathbb{N}$ such that $a, b > 1$. Suppose that one of the following conditions is satisfied:*

- $a \equiv 0 \pmod{2}$ and $b \equiv 3 \pmod{12}$;
- a is even, $\vartheta_2(b-1) = 1$ and $5 \mid b$.

Then, equation (1.1) has no solution in positive integers (n, x) .

This result generalizes the main result of Szalay [9]. A consequence of the above theorem is the following result.

Corollary 1.2. *Let $b \in \{15, 35, 55, 75, 95, 3, 27, 39, 51, 63, 87, 99\}$. Then the equation*

$$((2k)^n - 1)(b^n - 1) = x^2$$

has no solution in positive integers (k, n, x) .

Theorem 1.3. *Let $a, b \in \mathbb{N}$ such that $a, b > 1$. Suppose that $a \equiv 4 \pmod{10}$ and $b \equiv 0 \pmod{5}$. Then, equation (1.1) has no solution in positive integers (n, x) .*

Theorem 1.4. *Suppose that $a \equiv 4 \pmod{5}$ and $b \equiv 0 \pmod{5}$. Then equation (1.1) has a positive integer solution (n, x) if and only if $(a, b) = (u_r, u_s)$ with non-square $d \equiv \pm 1 \pmod{5}$ satisfying $u_1 \equiv 0 \pmod{5}, r \equiv 2 \pmod{4}$ and s is odd. In this case, the solution is $(x, n) = (dv_r v_s, 2)$.*

Theorem 1.5. *Suppose that $a \equiv 3 \pmod{4}$ and $b \equiv 0 \pmod{2}$. Then equation (1.1) has positive integer solutions (n, x) if and only if $(a, b) = (u_r, u_s)$ with non-square $d \equiv 3 \pmod{4}$ satisfying $u_1 \equiv 0 \pmod{2}, r \equiv 2 \pmod{4}$ and s is odd. In this case, the solution is $(x, n) = (dv_r v_s, 2)$.*

Remark 1.6. Using the Theorem 1.4 and the fact that there exist $d \equiv \pm 1 \pmod{5}$ with $u_1 \equiv 0 \pmod{5}$. For example, $u_1 = 2543295$ for $d = 94$. We deduce that

$$(a^2 - 1)(b^2 - 1) = x^2$$

has infinitely many solutions (a, b, x) with $a \equiv 4 \pmod{5}$ and $b \equiv 0 \pmod{5}$.

The proof of the first theorem using the method in [8]. We organize this paper as follows. To prove the above results, we need some results on divisibility properties of the solutions of Pell equations and some known results. See Section 2. The proof of Theorem 1.1 is done in Section 3. We prove Theorem 1.3 in Section 4 and the proof of Theorem 1.4 in Section 5. For similar reason, the proof of Theorem 1.5 is also left to the reader.

2. Preliminaries

In this section, we recall some results which will be very useful for the proofs.

Let d be a positive integer which is not a square. Then, by the theory of Pell equations, one knows that the equation

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

has infinitely many solutions and all its positive solutions (u, v) are given by

$$u_n + v_n \sqrt{d} = (u_1 + v_1 \sqrt{d})^n,$$

for some positive integer n , where (u_1, v_1) is the smallest positive solution.

The following result is well-known. As a reference (see [6, Lemma 1]).

Lemma 2.1. *Let d be a positive which is not square.*

1. *If k is even, then each prime factor p of u_k satisfies $p \equiv \pm 1 \pmod{8}$.*

2. If k is odd, then $u_1 \mid u_k$ and u_k/u_1 is odd.

3. If $q \in \{2, 3, 5\}$, then $q \mid u_k$ implies $q \mid u_1$.

The following lemma can be deduced from [1, Proposition 1].

Lemma 2.2. *Let $p > 3$ be a prime. Then, the equation*

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

has the only solution $(x, y) = (1, 1)$ in positive integers and the equation

$$x^3 = 2y^2 - 1, \quad x, y \in \mathbb{N}$$

has the only solutions $(x, y) = (1, 1), (23, 78)$ in positive integers.

The last result to recall is [10, Lemma 2.1].

Lemma 2.3. *For a fixed d , if $2 \mid u_r$ and $2 \nmid u_s$, then $2 \nmid r$ and $2 \mid s$.*

3. Proof of Theorem 1.1

We prove only the first part of the statement, the proofs of the other part is similar and left to the reader. Suppose that equation (1.1) has a solution in positive integer n, x with $a \equiv 0 \pmod{2}$ and $b \equiv 3 \pmod{12}$. Then we have

$$a^n - 1 = Dy^2 \quad \text{and} \quad b^n - 1 = Dz^2,$$

where $D = (a^n - 1, b^n - 1)$. D can be written as $D = dw^2$, with a square-free integer d . If $d = 1$, then n must be odd. Indeed, if n is even, then we obtain $(a^m)^2 - (yw)^2 = 1$ with $n = 2m$ and yw integers. This is impossible. So n is odd. As

$$b^n - 1 = (b - 1)(b^{n-1} + \dots + b + 1) \tag{3.1}$$

and $2 \mid (b^n - 1)$, it follows that $2 \mid z^2$. This implies that $2 \mid z$. Hence, $4 \mid (b^n - 1)$, which is a contradiction to equation (3.1) (as $\nu_2(b - 1) = 1$). So $d \geq 2$ and D is not square. Using the equation $a^n - 1 = Dy^2$ and the fact that a is even, we deduce that D is odd. Moreover, $2 \mid z^2$ by the equation $b^n - 1 = Dz^2$. This implies that $4 \mid (b^n - 1)$ and by equation (3.1) we conclude that n is even. Put now $n = 2m$, we obtain

$$(a^m)^2 - Dy^2 = 1 \quad \text{and} \quad (b^m)^2 - Dz^2 = 1.$$

The pairs

$$\{(a^m, y), (b^m, z)\}$$

are two solutions of the corresponding Pell equation $u^2 - Dv^2 = 1$. So there exist distinct positive integers r and s such that

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

where (u_1, v_1) is the fundamental solution of this Pell equation. Since $3 \mid b$ and 3 not congruent to ± 1 modulo 8. Lemma 2.1 tells us that s is odd. As $2 \mid a$ and $2 \nmid b$, it follows (by Lemma 2.3) that r is odd and s is even. This contradicts the fact that s is odd and thus completes the proof of Theorem 1.1.

4. Proof of Theorem 1.3

The aim of this section is to prove Theorem 1.3. Thus, let $a \equiv 4 \pmod{10}$ and $b \equiv 0 \pmod{5}$. Suppose that (n, x) is a solution to equation (1.1). Put $D = (a^n - 1, b^n - 1)$. By this equation, we have

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

Since $5 \mid b$, by $b^n - 1 = Dz^2$, it follows that

$$D \equiv \pm 1 \pmod{5} \text{ and } 5 \nmid z.$$

Now, we consider two cases according to the fact that 5 divides y or not.

Case 1: Suppose that $5 \nmid y$. Then $y^2 \equiv \pm 1 \pmod{5}$ and we get

$$a^n \equiv Dy^2 + 1 \equiv \pm D + 1 \equiv 0, 2 \pmod{5}.$$

This contradicts the fact that $a \equiv 4 \pmod{5}$.

Case 2: Assume now that $5 \mid y$. Since $a \equiv 4 \pmod{5}$, by $a^n - 1 = Dy^2$, we obtain

$$4^n \equiv a^n \equiv Dy^2 + 1 \equiv 1 \pmod{5}.$$

We deduce that n is even. Put $n = 2m$. Therefore, D cannot be a square and the pairs

$$\{(a^m, y), (b^m, z)\}$$

are two solutions of the corresponding Pell equation $u^2 - Dv^2 = 1$. Since $a \neq b$, there exist distinct positive integers r and s such that

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

where (u_1, v_1) is the fundamental solution of this Pell equation. By Lemma 2.1 and as $5 \mid b$ and $b^m = u_s$, one can see that $2 \nmid s$ and $5 \mid u_1$. Therefore, $2 \mid a$ and $a^m = u_r$ implies that $2 \mid u_r$ and so r is odd. By Lemma 2.1 (2), it follows that $u_1 \mid u_r$. For above, we deduce that $5 \mid u_r$ and thus $5 \mid a$, which contradicts the fact that $a \equiv 4 \pmod{5}$. This completes our proof.

5. Proof of Theorem 1.4

In this section, we will prove Theorem 1.4. Let $a \equiv 4 \pmod{5}$ and $b \equiv 0 \pmod{5}$ and suppose that (n, x) is a solution to equation (1.1). Put $D = (a^n - 1, b^n - 1)$. By this equation, we have

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

We similarly proceed as in the proof of Theorem 1.3 and obtain that n is even. Put $n = 2m$. Therefore, D cannot be a square and the corresponding Pell equation $u^2 - Dv^2 = 1$ has two solutions

$$(u, v) = (a^m, y), (b^m, z).$$

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

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

where (u_1, u_1) is the fundamental solution of this Pell equation. By Lemma 8 (1) and $5 \mid b$, we obtain that $2 \nmid s$ and $5 \mid u_1$. On the other hand, $a \equiv 4 \pmod{5}$, which together with $5 \mid u_1$ and Lemma 8 (2), shows that $2 \mid r$. Put $r = 2t$, we get

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

Now we distinguish two cases. Firstly, if $2 \mid m$, then $4 \mid n$ and so RESULT 2 in [2] implies that $(a, b) = (13, 239)$, with contradicts $5 \mid b$. Now, we assume that $2 \nmid m$ and $m > 3$, Lemma 9 shows that we have a contradiction since $a > 1$. If $m = 3$, then we get $a^3 = 2u_t^2 - 1$ and by Lemma 9, we obtain $a = 23$ and $u_t = 78$, which contradicts the fact that $a \equiv 4 \pmod{5}$. So $m = 1$, then $n = 2m = 2$. Now suppose that $r \equiv 0 \pmod{4}$. Then t is even and hence u_t not congruent to 0 modulo 5 by Lemma 8 (1). Then $a = u_r = 2u_t^2 - 1 \equiv 1, 2 \pmod{5}$, which contradicts that $a \equiv 4 \pmod{5}$. Conversely, suppose that $(a, b) = (u_r, u_s)$ with $d \equiv \pm 1 \pmod{5}$, $u_1 \equiv 0 \pmod{5}$, $r \equiv 2 \pmod{4}$ and s is odd. Therefore, equation (1.1) has the solution $(x, n) = (dv_r v_s, 2)$. Notice that $b \equiv u_t \equiv 0 \pmod{5}$ by Lemma 8 (2) and hence $a = u_r = 2u_t^2 - 1 \equiv 4 \pmod{5}$. This completes the proof of Theorem 1.4.

Acknowledgements. The authors are grateful to the anonymous referee's comments that lead to a more precise version of this paper.

References

- [1] M. A. BENNETT, C. M. SKINNER: *Ternary Diophantine equation via Galois representations and modular forms*, *Canad. J. Math* 56 (2004), pp. 23–54, DOI: 10.4153/cjm-2004-002-2.
- [2] J. H. E. COHN: *The Diophantine equation $(a^n - 1)(b^n - 1) = x^2$* , *Period. Math. Hungar.* 44.2 (2002), pp. 169–175, DOI: 10.1023/a:1019688312555.
- [3] L. HAJDU, 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), pp. 141–145, DOI: 10.1023/a:1010335509489.
- [4] K. ISHII: *On the exponential Diophantine equation $(a^n - 1)(b^n - 1) = x^2$* , *Publ. Math. Debrecen* 89.1-2 (2016), pp. 253–256, DOI: 10.5486/pmd.2016.7578.
- [5] R. KESKIN: *A Note On the Exponential Diophantine equation $(a^n - 1)(b^n - 1) = x^2$* , arXiv: 1801.04717v1.
- [6] L. LAN, L. SZALAY: *On the exponential Diophantine equation $(a^n - 1)(b^n - 1) = x^2$* , *Publ. Math. Debrecen* 77 (2010), pp. 1–6.
- [7] F. LUCA, P. G. WALSH: *The product of like-indexed terms in binary recurrences*, *J. Number Theory* 96.1 (2002), pp. 152–173, DOI: 10.1016/s0022-314x(02)92794-0.
- [8] A. NOUBISSIE, A. TOGBÉ, Z. ZHANG: *On the Exponential Diophantine equation $(a^n - 1)(b^n - 1) = x^2$* , to appear in the *Bulletin of the Belgian Mathematical Society – Simon Stevin*.
- [9] L. SZALAY: *On the Diophantine equation $(2^n - 1)(3^n - 1) = x^2$* , *Publ. Math. Debrecen* 57 (2000), pp. 1–9.

- [10] G. XIOYAN: *A Note on the Diophantine equation $(a^n - 1)(b^n - 1) = x^2$* , Period. Math. Hungar. 66 (2013), pp. 87–93.
- [11] P. YUAN, Z. ZHANG: *On the Diophantine equation $(a^n - 1)(b^n - 1) = x^2$* , Publ. Math. Debrecen 80 (2012), pp. 327–331.