Proc. Indian Acad. Sci. (Math. Sci.) (2019) 129:69
https://doi.org/10.1007/s12044-019-0520-x

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

REFİK KESKİN

Department of Mathematics, Faculty of Arts and Science, Sakarya University, Sakarya, Turkey
E-mail: rkeskin@sakarya.edu.tr

MS received 7 February 2018; revised 21 June 2018; accepted 13 April 2019; published online 27 July 2019

Abstract. In 2002, Luca and Walsh (*J. Number Theory* **96** (2002) 152–173) solved the diophantine equation for all pairs (a, b) such that $2 \leq a < b \leq 100$ with some exceptions. There are sixty nine exceptions. In this paper, we give some new results concerning the equation $(a^n - 1)(b^n - 1) = x^2$. It is also proved that this equation has no solutions if a, b have opposite parity and $n > 4$ with $2|n$. Here, the equation is also solved for the pairs $(a, b) = (2, 50), (4, 49), (12, 45), (13, 76), (20, 77), (28, 49), (45, 100)$. Lastly, we show that when b is even, the equation $(a^n - 1)(b^{2n}a^n - 1) = x^2$ has no solutions n, x.

Keywords. Pell equation; exponential diophantine equation; Lucas sequence.

Mathematics Subject Classification. 11D61, 11D31, 11B39.

1. Introduction

Let $a > 1$ and $b > 1$ be fixed integers with $a < b$. The exponential diophantine equation

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

has been studied by many authors in the literature since 2000. Firstly, Szalay [13] studied the equation (1) for $(a, b) = (2, 3)$ and showed that this equation has no solutions x and n. He also showed that equation (1) has only the solution $(n, x) = (1, 2)$ for $(a, b) = (2, 5)$. After that, many authors studied (1) by introducing special constraints to a or b (see [2,4,5,7–10,13,15,18–20]). In [10], Luca and Walsh proved that equation (1) has finitely many solutions n, x for fixed (a, b) and gave the following remarkable theorem.

Theorem 1. *Let $2 \leq a < b \leq 100$ be integers, and assume that (a, b) is not in one of the following three sets*:

$$A_1 = \{(2, 22), (4, 22)\},$$
$$A_2 = \{(a, b);\ (a - 1)(b - 1) \textit{ is a square},\ a \equiv b (\bmod 2) \textit{ and } (a, b) \neq (9, 3), (64, 8)\},$$

$$A_3 = \{(a, b);\ (a-1)(b-1) \textit{ is a square}, a+b \equiv 1 (\mathrm{mod}\, 2) \textit{ and } ab \equiv 0 (\mathrm{mod}\, 4)\}.$$

If

$$(a^k - 1)(b^k - 1) = x^2, \tag{2}$$

then $k = 2$, *except for the pair* $(a, b) = (2, 4)$, *in which case the only solution to* (2) *occurs at* $k = 3$.

There are 69 exceptions for (a, b) with $1 < a < b \leq 100$. Some of these pairs are $(2, 10), (2, 26), (2, 50), (2, 82), (3, 19), (3, 33), (3, 37), (3, 51), (3, 71)$ and $(3, 99)$. In [2], Cohn conjectured that equation (1) has no solutions if $n > 4$. Moreover, he conjectured that $(a^3 - 1)(b^3 - 1) = x^2$ has only the solutions

$$(a, b) = (2, 4), (2, 22), (3, 313), (4, 22).$$

The problem of finding solutions to equation (1) has not been settled yet, at least for the pairs (a, b) in the sets described in Theorem 1. If a and b are relatively prime, it is shown that equation (1) has no solutions when $n > 2$ is even and $4 \nmid n$. If a and b have opposite parity and $\gcd(a, b) > 1$, then we show that (1) has no solutions when $n > 4$ and $2|n$. As a result of these, it is shown that if a and b have opposite parity, then equation (1) has no solutions when $n > 4$ and $2|n$. Li and Tang [9] showed that equation (1) has no solutions for $(a, b) = (4, 13), (13, 28)$ if $n > 1$. In this paper, we give some new results which exhausts many pairs (a, b) in the sets described in Theorem 1. Especially, we solve (1) for the pairs $(a, b) = (2, 50), (4, 49), (12, 45), (13, 76), (20, 77), (28, 49)$ and $(45, 100)$. Lastly, we show that when b is even, $(a^n - 1)(b^{2n} a^n - 1) = x^2$ has no solutions n, x.

In section 2, we give some basic definitions and lemmas and in section 3, we give the proofs of our main theorems and corollaries.

Now, we state our main theorems and corollaries. For a nonzero integer m, we write $\nu_2(m)$ for the exponent of 2 in the factorization of m. If m is odd, it is clear that $\nu_2(m) = 0$.

Theorem 2. *Let* $\gcd(a, b) = 1$. *If* $(a^n - 1)(b^n - 1) = x^2$ *for some integers* x *with* $2|n$ *and* $4 \nmid n$, *then* $n = 2$.

Theorem 3. *Let* $\nu_2(a) \neq \nu_2(b)$ *and* $\gcd(a, b) > 1$. *Then the equation* $(a^n - 1)(b^n - 1) = x^2$ *has no solutions* n, x *with* $2|n$.

COROLLARY 4

If a *and* b *have opposite parity, then the equation* $(a^n - 1)(b^n - 1) = x^2$ *has no solutions for* $n > 4$ *with* $2|n$.

Theorem 5. *Let* $a \nmid b$ *and* $b \nmid a$ *with* $g = \gcd(a, b) > 1$. *If* $g^2 > a$ *or* $g^2 > b$, *then the equation* $(a^n - 1)(b^n - 1) = x^2$ *has no solutions* x, n *with* $2|n$. *If* $a|b$ *and* $a^2 > b$, *then the same is true.*

Theorem 6. *Let* a, b *be odd and* $g = \gcd(a, b) > 1$. *If* $a/g \equiv 3 (\mathrm{mod}\, 4)$ *or* $b/g \equiv 3 (\mathrm{mod}\, 4)$, *then the equation* $(a^n - 1)(b^n - 1) = x^2$ *has no solutions* n, x *with* $2|n$ *and* $4 \nmid n$.

Theorem 7. *The equation* $(2^n - 1)(50^n - 1) = x^2$ *has only the solution* $n = 1, x = 7$.

Theorem 8. *Let* b *be even. Then the equation* $(a^n - 1)(b^{2n}a^n - 1) = x^2$ *has no solutions* n, x.

COROLLARY 9

Let $(a, b) = (13, 76), (4, 49), (28, 49), (45, 100), (20, 77), (12, 45)$. *If the equation* $(a^n - 1)(b^n - 1) = x^2$ *has a solution, then* $n = 1$ *and all solutions are given by*

$$(n, x) = (1, 30), (1, 12), (1, 36), (1, 66), (1, 38), (1, 22),$$

respectively.

2. Some basic definitions and lemmas

In the proof of our main theorems, we will use the sequences $(U_n(P, Q))$ and $(V_n(P, Q))$ given in the following manner:

Let P and Q be non-zero coprime integers such that $P^2 + 4Q \neq 0$. Define

$$\begin{aligned} U_0(P, Q) &= 0, U_1(P, Q) = 1, U_{n+1}(P, Q) \\ &= PU_n(P, Q) + QU_{n-1}(P, Q) \quad (\text{for } n \geq 1), \\ V_0(P, Q) &= 2, V_1(P, Q) = P, V_{n+1}(P, Q) \\ &= PV_n(P, Q) + QV_{n-1}(P, Q) \quad (\text{for } n \geq 1). \end{aligned}$$

These sequences are called the first and second kinds of Lucas sequence, respectively. Sometimes, we write U_n and V_n instead of $U_n(P, Q)$ and $V_n(P, Q)$. It is well known that

$$U_n = \frac{\alpha^n - \beta^n}{\alpha - \beta} \quad \text{and} \quad V_n = \alpha^n + \beta^n, \tag{3}$$

where $\alpha = (P + \sqrt{P^2 + 4Q})/2$ and $\beta = (P - \sqrt{P^2 + 4Q})/2$. The following identities are valid for the terms of the sequences (U_n) and (V_n) (see [12]):

Let $d = \gcd(m, n)$. Then

$$\gcd(U_m, U_n) = U_d \tag{4}$$

and

$$\gcd(V_m, V_n) = \begin{cases} V_d & \text{if } m/d \text{ and } n/d \text{ are odd,} \\ 1 \text{ or } 2 & \text{otherwise.} \end{cases} \tag{5}$$

If P is even, then V_n is even and

$$2|U_n \text{ if and only if } 2|n. \tag{6}$$

Moreover, we have

$$V_{2n}(P,-1) = V_n^2(P,-1) - 2, \tag{7}$$
$$V_{3n}(P,-1) = V_n(P,-1)(V_n^2(P,-1) - 3) \tag{8}$$

and

$$V_n(P,-1) = U_{n+1}(P,-1) - U_{n-1}(P,-1). \tag{9}$$

The proof of the following lemma can be found in [3].

Lemma 10. *If* $P \equiv 0 \pmod 2$, *then*

$$\nu_2\left(V_n\left(P,-1\right)\right) = \begin{cases} \nu_2\left(P\right) & \text{if } n \equiv 1 (\bmod\ 2), \\ 1 & \text{if } n \equiv 0 (\bmod\ 2). \end{cases} \tag{10}$$

Lemma 11 [14]. *Let* $n \in \mathbb{N} \cup \{0\}$, $m, r \in \mathbb{Z}$ *and* m *be a nonzero integer. Then*

$$U_{2mn+r}(P,-1) \equiv U_r(P,-1) \pmod{U_m(P,-1)} \tag{11}$$

and

$$V_{2mn+r}(P,-1) \equiv V_r(P,-1) \pmod{U_m(P,-1)}. \tag{12}$$

From (11) and (12), we can deduce the following.

Lemma 12. $5 | V_n(P,-1)$ *if and only if* $5 | P$ *and* n *is odd.*

Let d be a positive integer which is not a perfect square and consider the Pell equation

$$x^2 - dy^2 = 1. \tag{13}$$

If $x_1 + y_1\sqrt{d}$ is the fundamental solution of equation (13), then all the positive integer solutions of this equation are given by

$$x_n + y_n\sqrt{d} = (x_1 + y_1\sqrt{d})^n \tag{14}$$

with $n \geq 1$. From (3) and (14), the following lemma can be given (see also [11], page 22).

Lemma 13. *Let* $x_1 + y_1\sqrt{d}$ *be the fundamental solution of equation* $x^2 - dy^2 = 1$. *Then all positive integer solutions of the equation* $x^2 - dy^2 = 1$ *are given by*

$$x_n = \frac{V_n(2x_1,-1)}{2} \quad \text{and} \quad y_n = y_1 U_n(2x_1,-1)$$

with $n \geq 1$.

Lemma 14. *Let n be even, say $n = 2k$ and $(a^n - 1)(b^n - 1) = x^2$ for some integer x. Then there exist positive integers m and r with $\gcd(m, r) = 1$ such that*

$$a^k = V_m(2x_1, -1)/2, b^k = V_r(2x_1, -1)/2,$$

where $x_1 > 1$.

Proof. Let $d = \gcd(a^n - 1, b^n - 1)$. Then $a^n - 1 = du^2$ and $b^n - 1 = dv^2$ for some integers u and v with $\gcd(u, v) = 1$. It is seen that d is not a perfect square. Let $n = 2k$. Then $(a^k)^2 - du^2 = 1$ and $(b^k)^2 - dv^2 = 1$. Assume that $x_1 + y_1\sqrt{d}$ is the fundamental solution of the equation $x^2 - dy^2 = 1$. Then by Lemma 13, we get

$$a^k = V_m(2x_1, -1)/2, u = y_1 U_m(2x_1, -1)$$

and

$$b^k = V_r(2x_1, -1)/2, v = y_1 U_r(2x_1, -1)$$

for some $m \geq 1$ and $r \geq 1$. Since $\gcd(u, v) = 1$, it follows that $1 = \gcd(u, v) = \gcd(y_1 U_m(2x_1, -1), y_1 U_r(2x_1, -1)) = y_1 \gcd(U_m, U_r) = y_1 U_{\gcd(m,r)}$ by (4). Therefore $y_1 = 1$ and $\gcd(m, r) = 1$. Since $x_1^2 - dy_1^2 = 1$, it follows that $x_1^2 = 1 + dy_1^2 = 1 + d > 1$ and so $x_1 > 1$. □

The following lemma can be deduced from [1] and [16].

Lemma 15. *Let $p > 3$ be a prime. Then the equation $x^p = 2y^2 - 1$ has only the solution $(x, y) = (1, 1)$ in non-negative integers. The equation $x^3 = 2y^2 - 1$ has only the solutions $(x, y) = (1, 1)$ and $(23, 78)$ in non-negative integers.*

The following lemma is given in [2].

Lemma 16. *If the equation $(a^n - 1)(b^n - 1) = x^2$ has a solution n, x with $4|n$, then $n = 4$ and $(a, b) = (13, 339)$.*

Lemma 17 [17]. *Let a be a positive integer which is not a perfect square and b be a positive integer for which the quadratic equation $ax^2 - by^2 = 1$ is solvable in positive integers x, y. If $u_1\sqrt{a} + v_1\sqrt{b}$ is its minimal solution, then the formula $x_n\sqrt{a} + y_n\sqrt{b} = (u_1\sqrt{a} + v_1\sqrt{b})^{2n+1}$ $(n \geq 0)$ gives all the positive integer solutions of the equation $ax^2 - by^2 = 1$.*

Although the following lemma is given in [6], we will give its proof for the sake of completeness.

Lemma 18. *Let a be a positive integer which is not a perfect square and b be a positive integer. Let $u_1\sqrt{a} + v_1\sqrt{b}$ be the minimal solution of the equation $ax^2 - by^2 = 1$ and $P = 4au_1^2 - 2$. Then all the positive integer solutions of the equation $ax^2 - by^2 = 1$ are given by $(x, y) = (u_1(U_{n+1} - U_n), v_1(U_{n+1} + U_n))$ with $n \geq 0$, where $U_n = U_n(P, -1)$.*

Proof. Since $w = u_1\sqrt{a} + v_1\sqrt{b}$ is the minimal solution of the equation $ax^2 - by^2 = 1$, all positive integer solutions of the equation $ax^2 - by^2 = 1$ are given by the formula $x_n\sqrt{a} + y_n\sqrt{b} = w^{2n+1}$ with $n \geq 0$, by Lemma 17. Then we get

$$x_n = \frac{w^{2n+1} + z^{2n+1}}{2\sqrt{a}} \quad \text{and} \quad y_n = \frac{w^{2n+1} - z^{2n+1}}{2\sqrt{b}},$$

where $z = u_1\sqrt{a} - v_1\sqrt{b}$. By using the fact that $au_1^2 - bv_1^2 = 1$, it is seen that

$$\begin{aligned} w^2 &= au_1^2 + bv_1^2 + 2u_1v_1\sqrt{ab} = \frac{2au_1^2 + 2bv_1^2 + 4u_1v_1\sqrt{ab}}{2} \\ &= \frac{2au_1^2 + 2au_1^2 - 2 + \sqrt{16u_1^2v_1^2ab}}{2} = \frac{4au_1^2 - 2 + \sqrt{(4au_1^2 - 2)^2 - 4}}{2} \\ &= (P + \sqrt{P^2 - 4})/2. \end{aligned}$$

Similarly, it can be seen that

$$z^2 = (P - \sqrt{P^2 - 4})/2.$$

Let

$$\alpha = (P + \sqrt{P^2 - 4})/2 \quad \text{and} \quad \beta = (P - \sqrt{P^2 - 4})/2.$$

By using (3) and (9), a simple calculation shows that

$$\begin{aligned} x_n &= \frac{w^{2n+1} + z^{2n+1}}{2\sqrt{a}} = \frac{w\alpha^n + z\beta^n}{2\sqrt{a}} = \frac{u_1V_n + u_1(P-2)U_n}{2} \\ &= u_1(U_{n+1} - U_n) \end{aligned}$$

and

$$\begin{aligned} y_n &= \frac{w^{2n+1} - z^{2n+1}}{2\sqrt{b}} = \frac{w\alpha^n - z\beta^n}{2\sqrt{b}} = \frac{v_1V_n + v_1(P+2)U_n}{2} \\ &= v_1(U_{n+1} + U_n). \end{aligned}$$

This completes the proof. □

3. Proofs of theorems and corollaries

Proof of Theorem 2. Let $n = 2k$ with k odd. Then by Lemma 14, we get

$$a^k = V_m(2x_1, -1)/2, b^k = V_r(2x_1, -1)/2$$

for some $m \geq 1$, $r \geq 1$ with $\gcd(m, r) = 1$ and $x_1 > 1$. Now assume that m and r are both odd. Then $2 = \gcd(2a^k, 2b^k) = \gcd(V_m, V_r) = V_{\gcd(m,r)} = V_1 = 2x_1$ by (5). This implies that $x_1 = 1$, which is impossible. Therefore, one of m and r must be even, say $m = 2t$. Then $2a^k = V_m = V_{2t} = V_t^2 - 2$ by (7). Let $V_t = 2c$. Then it follows that $2a^k = 4c^2 - 2$, which yields

$$a^k = 2c^2 - 1. \tag{15}$$

Assume that $k \geq 3$. If k has a prime factor $p > 3$, then (15) is impossible by Lemma 15 since $a > 1$. Let $k = 3^t = 3z$ with $z \geq 1$. Then $(a^z)^3 = 2c^2 - 1$ and therefore $a^z = 23, c = 78$ by Lemma 15. This shows that $z = 1$, $a = 23$ and $n = 6$. Thus $23^6 - 1 = du^2$ and $b^6 - 1 = dv^2$. Since $(V_t/2, y_1U_t) = (V_t/2, U_t)$ is a solution of the equation $x^2 - dy^2 = 1$, it is seen that $dU_t^2 = (V_t/2)^2 - 1$. Since $V_t = 2c = 2 \cdot 78$, we get

$$dU_t^2 = 78^2 - 1 = 7 \cdot 11 \cdot 79,$$

which shows that $d = 7 \cdot 11 \cdot 79 = 6083$. Then $b^6 = dv^2 + 1 = 6083v^2 + 1 \equiv 3v^2 + 1 (\bmod 8)$. Since $\gcd(23^6 - 1, b^6 - 1) = d = 6083$, it is seen that b must be even. But this is impossible since $b^6 \equiv 3v^2 + 1 (\bmod 8)$. Thus we conclude that $k = 1$ and therefore $n = 2$. □

Proof of Theorem 3. Assume that $n = 2k$. Then by Lemma 14, we get

$$a^k = V_m(2x_1, -1)/2, b^k = V_r(2x_1, -1)/2$$

for some $m \geq 1$, $r \geq 1$ with $\gcd(m, r) = 1$ and $x_1 > 1$. Since $\gcd(V_m, V_r) = \gcd(2a^k, 2b^k) = 2\,(\gcd(a, b))^k > 2$, it follows that m and r are odd by (5). Moreover, we have $2a^k = V_m$ and $2b^k = V_r$, which implies that

$$\nu_2(2a^k) = \nu_2(V_m) = \nu_2(2x_1)$$

and

$$\nu_2(2b^k) = \nu_2(V_r) = \nu_2(2x_1)$$

by (10). Therefore, $\nu_2(2a^k) = \nu_2(2b^k)$, which is impossible since $\nu_2(a) \neq \nu_2(b)$. This completes the proof. □

Proof of Corollary 4. The proof follows from Lemma 16, Theorem 2 and Theorem 3. □

Proof of Theorem 5. Let $(a^n - 1)(b^n - 1) = x^2$ and $n = 2k$. Then $(a^k)^2 - du^2 = 1$ and $(b^k)^2 - dv^2 = 1$ for some integers u and v with $\gcd(u, v) = 1$. Assume that $x_1 + y_1\sqrt{d}$ is the fundamental solution of the equation $x^2 - dy^2 = 1$. Then by Lemma 13, we get

$$a^k = V_m(2x_1, -1)/2, u = y_1U_m(2x_1, -1)$$

and

$$b^k = V_r(2x_1, -1)/2, v = y_1U_r(2x_1, -1)$$

for some $m \geq 1$ and $r \geq 1$. Since $(u, v) = 1$, it is seen that $y_1 = 1$ and $\gcd(m, r) = 1$. Since $\gcd(V_m, V_r) = \gcd(2a^k, 2b^k) = 2\,(\gcd(a, b))^k > 2$, it follows that m and r are both odd by (5). Thus we get $2x_1 = V_1 = \gcd(V_m, V_r) = 2\,(\gcd(a, b))^k$. That is, $x_1 = (\gcd(a, b))^k$. Since $g = \gcd(a, b)$, it follows that $d = x_1^2 - 1 = g^n - 1$. Let $a = gc$ and $b = ge$. Since $d|a^n - 1$ and $d|b^n - 1$, $g^n - 1|g^n c^n - 1$ and $g^n - 1|g^n e^n - 1$. Thus $g^n - 1|c^n - 1$ and $g^n - 1|e^n - 1$. Since $c > 1$ and $e > 1$, we get $g \leq c$ and $g \leq e$. Then it follows that $a \geq g^2$ and $b \geq g^2$, which contradicts the hypothesis. This completes the proof. □

Proof of Theorem 6. Let $n = 2k$ with k odd. Then there exist relatively prime integers u and v such that

$$2a^k = V_m(P, -1), u = y_1 U_m(P, -1) \tag{16}$$

and

$$2b^k = V_r(P, -1), u = y_1 U_r(P, -1), \tag{17}$$

by Lemma 13, where $P = 2x_1$. Since $\gcd(u, v) = 1$, it is seen that $y_1 = 1$ and $\gcd(m, r) = 1$. Let $g = \gcd(a, b)$. Thus $(V_m, V_r) = (2a^k, 2b^k) = 2g^k > 2$. Then m and r are odd and so $(V_m, V_r) = V_1 = P$ by (5). Thus $P = 2g^k$. Since g and k are odd, it follows that $P \equiv 2g (\text{mod}\, 8)$. Then an induction method shows that $V_n \equiv 2 (\text{mod}\, 8)$ if n is even and $V_n \equiv 2g (\text{mod}\, 8)$ if n is odd. Let $a = gc$ and $b = ge$. Then, from (16) and (17), it follows that $V_m = Pc^k$ and $V_r = Pe^k$. Thus we conclude that $Pc^k \equiv Pe^k \equiv 2g (\text{mod}\, 8)$, that is, $2gc^k \equiv 2ge^k \equiv 2g (\text{mod}\, 8)$. This implies that $2c \equiv 2 (\text{mod}\, 8)$ and $2e \equiv 2 (\text{mod}\, 8)$. Therefore, $c \equiv 1 (\text{mod}\, 4)$ and $e \equiv 1 (\text{mod}\, 4)$. But this contradicts the hypothesis. This completes the proof. □

Proof of Theorem 8. Assume that n is even, say $n = 2k$ and $(a^n - 1)(a^n b^{2n} - 1) = x^2$. Then

$$a^k = V_m(2x_1, -1)/2, b^n a^k = V_r(2x_1, -1)/2$$

for some $m \geq 1, r \geq 1$ with $\gcd(m, r) = 1$ and $x_1 > 1$ by Lemma 14. Moreover, $\gcd(V_m, V_r) = \gcd(2a^k, 2b^n a^k) = 2a^k > 2$. Then by (5), we see that m and r are odd. Thus $2x_1 = V_1 = V_{\gcd(m,r)} = (V_m, V_r) = 2a^k$. This implies that $2b^n a^k = V_r(2x_1, -1) = V_r(2a^k, -1)$, which gives a contradiction by (10) since r is odd and b is even.

Now assume that n is odd, say $n = 2k+1$. Thus $a(a^k)^2 - du^2 = 1$ and $a(a^k b^n)^2 - dv^2 = 1$. Assume that a is not a perfect square. Let $u_1\sqrt{a} + v_1\sqrt{b}$ be the minimal solution of the equation $ax^2 - by^2 = 1$ and $P = 4au_1^2 - 2$. Then by Lemma 18, we get

$$a^k = u_1(U_{m_1+1} - U_{m_1})$$

and

$$a^k b^n = u_1(U_{m_2+1} - U_{m_2})$$

for some non-negative integers m_1 and m_2, where $U_n = U_n(P, -1)$. From the above, we get $U_{m_2+1} - U_{m_2} = b^n(U_{m_1+1} - U_{m_1})$. But this is impossible since $U_{m_2+1} - U_{m_2}$ and $U_{m_1+1} - U_{m_1}$ are odd by (6) and b is even. If a is a perfect square, say $a = c^2$, then $(c^{2n} - 1)(c^{2n}b^{2n} - 1) = x^2$. Thus by Lemma 14, we get

$$c^n = V_m(2x_1, -1)/2, (cb)^n = V_r(2x_1, -1)/2$$

for some $m \geq 1$ and $r \geq 1$ with $\gcd(m, r) = 1$. Since $\gcd(V_m, V_r) > 2$, it is seen that m and r are odd by (5). Moreover, we get $V_r = b^n V_m$. But this is impossible by (10) since b is even. □

Proof of Theorem 7. Clearly, $(n, x) = (1, 7)$ is a solution. Let $d = \gcd(2^n - 1, 50^n - 1)$. Then $2^n - du^2 = 1$ and $50^n - dv^2 = 1$ for some positive integers u and v with $\gcd(u, v) = 1$ Assume that n is even, say $n = 2k$. Let $x_1 + \sqrt{d}y_1$ be the fundamental solution of $x^2 - dy^2 = 1$. By Lemma 13, we get

$$2^k = V_m(2x_1, -1)/2, 50^k = V_r(2x_1 - 1)/2$$

and

$$u = y_1 U_m(2x_1, -1), v = y_1 U_r(2x_1, -1)$$

for some positive integers m and r. Since $\gcd(u, v) = 1$ and $\gcd(V_m, V_r) = 2 \cdot 2^k > 2$, it follows that $(m, r) = 1$ and m, r are odd by (5). On the other hand, $5|V_r$ implies that $5|x_1$ by Lemma 12, which yields $5|2^k$. This is a contradiction. Now assume that n is odd and $n = 2k + 1 > 1$. Then

$$x^2 = (2^n - 1)(50^n - 1) \equiv (-1)(4^k \cdot 2 - 1) \equiv (-1)(2(-1)^k - 1)(\text{mod } 5).$$

This shows that k is even. Let $u_1\sqrt{2} + v_1\sqrt{d}$ be the minimal solution of the equation $2x^2 - dy^2 = 1$. Since $2(2^k)^2 - du^2 = 1$ and $2(5^n 2^k)^2 - dv^2 = 1$, we get

$$2^k = u_1(U_{m_1+1} - U_{m_1}), u = v_1(U_{m_1+1} + U_{m_1}) \tag{18}$$

and

$$5^n 2^k = u_1(U_{m_2+1} - U_{m_2}), v = v_1(U_{m_2+1} + U_{m_2}) \tag{19}$$

for some non-negative integers m_1, m_2 by Lemma 18, where $U_n = U_n(P, -1)$ and $P = 4au_1^2 - 2 = 8u_1^2 - 2$. Since $U_{m_1+1} - U_{m_1}$ is odd by (6), it follows that $u_1 = 2^k$ and $U_{m_1+1} - U_{m_1} = 1$. Therefore, $m_1 = 0$. Moreover, we get that $5^n = (U_{m_2+1} - U_{m_2})$ by (18) and (19). Since $m_1 = 0$, we have $u = v_1$ by (18). From (18) and (19), it follows that $v_1| \gcd(u, v)$, which yields $v_1 = 1$ since $\gcd(u, v) = 1$. Therefore, $u = v_1 = 1$. This implies that $d = 2^n - 1$ since $2^n - du^2 = 1$.

Since $2^k\sqrt{2} + \sqrt{d}$ is the minimal solution of the equation $2x^2 - dy^2 = 1$, $(2^k\sqrt{2} + \sqrt{d})^2 = 2^n + d + 2^{k+1}\sqrt{2d} = 2^n + 2^n - 1 + 2^{k+1}\sqrt{2d} = 2^{n+1} - 1 + 2^{k+1}\sqrt{2d}$ is the fundamental solution of the equation $x^2 - 2dy^2 = 1$. Moreover, $(5^n 2^k\sqrt{2} + v\sqrt{d})^2 =$

$5^{2n}2^{2k+1}+dv^2+2^{k+1}5^n v\sqrt{2d}=5^{2n}2^n+50^n-1+2^{k+1}5^n v\sqrt{2d}=2\cdot(50)^n-1+2^{k+1}5^n v\sqrt{2d}$ is a solution of the equation $x^2-2dy^2=1$. Then by Lemma 13, we get

$$2\cdot 50^n-1=V_m(P,-1)/2,\, 2^{k+1}5^n v=2^{k+1}U_m(P,-1)$$

for some $m\geq 1$, where $P=2(2^{n+1}-1)$. Since k is even and $n=2k+1$, it is seen that $P\equiv 1(\bmod 5)$. Therefore, we get $U_3=P^2-1\equiv 0(\bmod 5)$. Let $m=6q+r$ with $0\leq r\leq 5$. Then $U_m\equiv U_r(\bmod U_3)$, which implies that $U_m\equiv U_r(\bmod 5)$ by (11). Then it follows that $3|m$ since $5|U_m$. Let $m=3t$. Then $2w^2-2=V_m(P,-1)=V_{3t}=V_t(V_t^2-3)=V_t^3-3V_t$ by (8), where $w=10\cdot 50^k$. Let $V_t=2z$. Then we get $w^2=4z^3-3z+1=(z+1)(2z-1)^2$. Since $3\nmid w$, it follows that $\gcd(z+1,2z-1)=1$. Then

$$z+1=r^2,\,(2z-1)^2=s^2$$

with $rs=w=2^{k+1}5^n$. Since $\gcd(r,s)=1$, it is seen that $r=w$ and $s=1$ or $r=2^{k+1}$ and $s=5^n$. Let $s=1$. Then $z=1$, which implies that $V_t=2$. Therefore, $t=0$ and this yields $m=0$. This is impossible since $U_m=5^n v$. Let $r=2^{k+1}$ and $s=5^n$. Then $z=r^2-1=2^{n+1}-1$ and $2z-1=5^n$. This implies that $5^n+1=2^{n+2}-2$. Therefore, $5^n-1=4(2^n-1)$. Then we get $2^n-1=1+5+\cdots+5^{n-1}\equiv n(\bmod 4)$ and so $n=-1(\bmod 4)$. This is impossible since $n\equiv 1(\bmod 4)$. We conclude that $n=1$. Thus the proof of the theorem is complete. □

Proof of Corollary 9. Let $(a,b)=(13,76)$. Since $(13^2-1)(76^2-1)$ is not a perfect square, we may suppose that n is odd by Theorem 2 and Lemma 16. Clearly, $(n,x)=(1,30)$ is a solution. Assume that $n\geq 3$. Let $A=1+13+13^2+\cdots+13^{n-1}$ and $B=1+76+76^2+\cdots+76^{n-1}$. Then $A\equiv(\frac{n+1}{2})\cdot 1+(\frac{n-1}{2})\cdot 5(\bmod 8)$ and $B\equiv 5(\bmod 8)$ since $13^{2j}\equiv 1(\bmod 8)$ and $13^{2j+1}\equiv 5(\bmod 8)$. This implies that $AB\equiv 5(3n-2)(\bmod 8)$, which yields $n\equiv 5(\bmod 8)$ since AB is an odd perfect square. Let $n=5+8k$ with $k\geq 0$. Then, since $13^8\equiv 1(\bmod 17)$ and $76^8\equiv 1(\bmod 17)$, we get

$$\begin{aligned}x^2&=(13^n-1)(76^n-1)\equiv(13^5-1)(76^5-1)\equiv((-4)^5-1)(8^5-1)\equiv\\&\equiv-(4^5+1)(8^5-1)\equiv-40\equiv 11(\bmod 17).\end{aligned}$$

But this is impossible since $\left(\frac{11}{17}\right)=\left(\frac{17}{11}\right)=\left(\frac{-5}{11}\right)=(-1)\left(\frac{5}{11}\right)=-1$. This completes the proof.

Let $(a,b)=(4,49)$. Clearly, $(n,x)=(1,12)$ is a solution. Assume that $(4^n-1)(49^n-1)=x^2$. Then $(2^{2n}-1)(7^{2n}-1)=x^2$. By Lemma 16 and Theorem 2, we obtain $2n=2$, which yields $n=1$. This completes the proof.

Let $(a,b)=(28,49)$. Since $\gcd(28,49)=7$ and $\nu_2(28)\neq\nu_2(49)$, by Theorem 3, we may suppose that n is odd. Clearly $(n,x)=(1,36)$ is a solution. Assume that $n\geq 3$. Let $A=1+28+28^2+\cdots+28^{n-1}$ and $B=1+49+49^2+\cdots+49^{n-1}$. Then $A\equiv 5(\bmod 8)$ and $B\equiv n(\bmod 8)$. This implies that $5n\equiv 1(\bmod 8)$ since AB is an odd perfect square. Then it follows that $n\equiv 5(\bmod 8)$. Let $n=5+8k$. Since $\left(\frac{28}{17}\right)=-1$ and $\left(\frac{49}{17}\right)=1$, we get $28^8\equiv -1(\bmod 17)$ and $49^8\equiv 1(\bmod 17)$. Then $x^2=(28^n-1)(49^n-1)\equiv(28^5(-1)^k-1)(49^5-1)(\bmod 17)$, which implies that $x^2\equiv(10(-1)^k-1)(\bmod 17)$ since $49^5-1\equiv 1(\bmod 17)$. Therefore, k must be even. Then we get $n\equiv 5,21,37(\bmod 48)$. Let

$n \equiv 5 \pmod{48}$. Then $x^2 \equiv (28^n - 1)(49^n - 1) \equiv (28^5 - 1)(49^5 - 1) \equiv 5 \cdot 3 \equiv 2 \pmod{13}$, which is impossible since $\left(\frac{2}{13}\right) = -1$. If $n \equiv 21 \pmod{48}$, then $x^2 \equiv (28^{21} - 1)(49^{21} - 1) \equiv 4 \cdot 11 \equiv 5 \pmod{13}$, which is impossible since $\left(\frac{5}{13}\right) = \left(\frac{13}{5}\right) = \left(\frac{3}{5}\right) = -1$. Therefore, $n \equiv 37 \pmod{48}$. Then we get $n \equiv 37, 85, 133, 181, 229 \pmod{240}$. Let $n \equiv 37 \pmod{240}$. Then $x^2 \equiv (28^{37} - 1)(49^{37} - 1) \equiv 11 \pmod{31}$, which is impossible since $\left(\frac{11}{31}\right) = \left(\frac{-20}{31}\right) = -\left(\frac{5}{31}\right) = -\left(\frac{31}{5}\right) = -1$. Let $n \equiv 85 \pmod{240}$. Then $x^2 \equiv (28^{85} - 1)(49^{85} - 1) \equiv 3 \pmod{31}$, which is impossible since $\left(\frac{3}{31}\right) = -\left(\frac{31}{3}\right) = -1$. Let $n \equiv 181 \pmod{240}$. Then $x^2 \equiv (28^{181} - 1)(49^{181} - 1) \equiv 102 \pmod{241}$. But this is impossible since $\left(\frac{102}{241}\right) = \left(\frac{2}{241}\right)\left(\frac{51}{241}\right) = \left(\frac{241}{51}\right) = \left(\frac{37}{51}\right) = \left(\frac{51}{37}\right) = \left(\frac{14}{37}\right) = \left(\frac{2}{37}\right)\left(\frac{7}{37}\right) = -\left(\frac{7}{37}\right) = -\left(\frac{37}{7}\right) = -\left(\frac{2}{7}\right) = -1$. Let $n \equiv 229 \pmod{240}$, then $x^2 \equiv (28^{229} - 1)(49^{229} - 1) \equiv 8 \pmod{11}$, which is impossible since $\left(\frac{8}{11}\right) = -1$. This completes the proof.

Let $(a, b) = (45, 100)$. Since $\gcd(45, 100) = 5$ and $\nu_2(45) \neq \nu_2(100)$, by Theorem 3, we may suppose that n is odd. It is obvious that$(n, x) = (1, 66)$ is a solution. Suppose that $n \geq 3$. Then it can be seen that $n \equiv 5 \pmod 8$. Therefore,

$$n \equiv 5, 13, 21, 29, 37, 45, 53, 61, 69 \pmod{72}.$$

Let $n \equiv 5 \pmod{72}$. Then $x^2 \equiv (45^5 - 1)(100^5 - 1) \equiv 5 \pmod 7$, which is impossible since $\left(\frac{5}{7}\right) = -1$. Let $n \equiv 21 \pmod{72}$. Then we get $x^2 \equiv 43 \pmod{73}$, which is a contradiction since $\left(\frac{43}{73}\right) = -1$. If $n \equiv 29 \pmod{72}$, then we use mod 7 to get a contradiction. If $n \equiv 53 \pmod{72}$, then $x^2 \equiv 13 \pmod{37}$, which gives a contradiction since $\left(\frac{13}{37}\right) = -1$. If $n \equiv 37, 45, 61, 69 \pmod{72}$, then we get $x^2 \equiv 45, 15, 31, 10 \pmod{73}$ respectively, which gives a contradiction since $\left(\frac{43}{73}\right) = \left(\frac{45}{73}\right) = \left(\frac{15}{73}\right) = \left(\frac{31}{73}\right) = \left(\frac{10}{73}\right) = -1$. Let $n \equiv 13 \pmod{72}$. Then $n \equiv 13, 85, 157 \pmod{216}$. Thus $x^2 \equiv 14, 13, 59 \pmod{109}$, which is impossible since $\left(\frac{14}{109}\right) = \left(\frac{13}{109}\right) = \left(\frac{59}{109}\right) - 1$. This completes the proof . We omit the proof in the case $(a, b) = (20, 77), (12, 45)$ as the proof is similar. $\square$

References

[1] Bennet M A and Skinner C M, Ternary diophantine equation via Galois representations and modular forms, *Canad. J. Math.* **56** (2004) 23–54

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

[3] Damir M T, Faye B, Luca F and Tall A, Members of Lucas sequences whose Euler function is a power of 2, *Fibonacci Quart.* **52** (2014) 3–9

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

[5] Ishii K, On the exponential diophantine equation $(a^n - 1)(b^n - 1) = x^2$, *Pub. Math. Debrecen* **89** (2016) 253–256

[6] Keskin R and Şiar Z, Positive integer solutions of some diophantine equations in terms of integer sequences, *Afr. Mat.* **30** (2019) 181–184

[7] Lan L and Szalay L, On the exponential diophantine equation $(a^n - 1)(b^n - 1) = x^2$, *Publ. Math. Debrecen* **77** (2010) 1–6

[8] Le M H, A note on the exponential diophantine equation $(2^n - 1)(b^n - 1) = x^2$, *Publ. Math. Debrecen* **74** (2009) 401–403

[9] Li Z-J and Tang M, A remark on a paper of Luca and Walsh, *Integers* **11** (2011) A40, 6 pp.
[10] Luca F, Walsh P G, The product of like-indexed terms in binary recurrences, *J. Number Theory* **96** (2002) 152–173
[11] Luca F, Effective Methods for Diophantine Equations, https://math.dartmouth.edu/archive/m105f12/public_html/lucaHungary1.pdf
[12] Ribenboim P, My Numbers, My Friends (2000) (New York: Springer-Verlag)
[13] Szalay L, On the diophantine equations $(2^n - 1)(3^n - 1) = x^2$, *Publ. Math. Debrecen* **57** (2000) 1–9
[14] Şiar Z and Keskin R, Some new identities concerning generalized Fibonacci and Lucas numbers, *Hacet. J. Math. Stat.* **42** (2013) 211–222
[15] Tang M, A note on the exponential diophantine equation $(a^m - 1)(b^n - 1) = x^2$, *J. Math. Research and Exposition* **31(6)** (2011) 1064–1066
[16] van der Waall R W, On the diophantine equation $x^2 + x + 1 = 3y^2$, $x^3 - 1 = 2y^2$ and $x^3 + 1 = 2y^2$, *Simon Stevin* **46** (1972/73) 39–51
[17] Walker D T, On the diophantine equation $mX^2 - nY^2 = \pm 1$, *Amer. Math. Montly* **74** (1967) 504–513
[18] Walsh P G, On diophantine equations of the form $(x^n - 1)(y^m - 1) = z^2$, *Tatra Math. Publ.* **20** (2000) 87–89
[19] Xioyan G, A note on the diophantine equation $(a^n - 1)(b^n - 1) = x^2$, *Period. Math. Hungar.* **66** (2013) 87–93
[20] Yuan P and Zhang Z, On the diophantine equation $(a^n - 1)(b^n - 1) = x^2$, *Publ. Math. Debrecen* **80** (2012) 327–331

Communicating Editor: B Sury