Notes on Number Theory and Discrete Mathematics
Print ISSN 1310–5132, Online ISSN 2367–8275
Vol. 27, 2021, No. 3, 123–129
DOI: 10.7546/nntdm.2021.27.3.123-129

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

Yasutsugu Fujita[1] **and Maohua Le**[2]

[1] Department of Mathematics, College of Industrial Technology, Nihon University
2-11-1 Shin-ei, Narashino, Chiba, Japan
e-mail: fujita.yasutsugu@nihon-u.ac.jp

[2] Institute of Mathematics, Lingnan Normal College
Zhangjiang, Guangdong, 524048 China
e-mail: lemaohua2008@163.com

Received: 22 December 2020 **Revised:** 3 August 2021 **Accepted:** 4 August 2021

Abstract: For any positive integer t, let $\mathrm{ord}_2\, t$ denote the order of 2 in the factorization of t. Let a, b be two distinct fixed positive integers with $\min\{a, b\} > 1$. In this paper, using some elementary number theory methods, the existence of positive integer solutions (x, n) of the polynomial-exponential Diophantine equation $(*)$ $(a^n - 1)(b^n - 1) = x^2$ with $n > 2$ is discussed. We prove that if $\{a, b\} \neq \{13, 239\}$ and $\mathrm{ord}_2(a^2 - 1) \neq \mathrm{ord}_2(b^2 - 1)$, then $(*)$ has no solutions (x, n) with $2 \mid n$. Thus it can be seen that if $\{a, b\} \equiv \{3, 7\}, \{3, 15\}, \{7, 11\}, \{7, 15\}$ or $\{11, 15\}$ $\pmod{16}$, where $\{a, b\} \equiv \{a_0, b_0\} \pmod{16}$ means either $a \equiv a_0 \pmod{16}$ and $b \equiv b_0 \pmod{16}$ or $a \equiv b_0 \pmod{16}$ and $b \equiv a_0 \pmod{16}$, then $(*)$ has no solutions (x, n).

Keywords: Polynomial-exponential Diophantine equation, Pell's equation.
2020 Mathematics Subject Classification: 11D61.

1 Introduction

Let $\mathbb{N}$ be the set of all positive integers. Let a, b be two distinct fixed positive integers with $\min\{a, b\} > 1$. In 2000, L. Szalay [16] first discussed the solution of the polynomial-exponential Diophantine equation

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

He proved, e.g., that if $\{a, b\} = \{2, 3\}$, then (1) has no solutions (x, n). This result has been generalized and it has been proved that if $a \equiv 3 \pmod 4$ and $b \equiv 0 \pmod 2$ (or vice versa), then (1) has no solutions (x, n) by P.-Z. Yuan and Z.-F. Zhang [20] with the correction on the exceptional case due to A. Noubissie, A. Togbé and Z.-F. Zhang [15]. J. H. E. Cohn [2] gave several criteria which help to solve (1). For example, he showed that if $\operatorname{ord}_2(a-1)$ and $\operatorname{ord}_2(b-1)$ have opposite parity, where $\operatorname{ord}_2 t$ is said the order of 2 in the factorization of a positive integer t, then (1) has no solutions (x, n) with $2 \nmid n$. Using this result, X.-Y. Guo [3] proved that if $\{a, b\} \neq \{13, 239\}$ and $\operatorname{ord}_2(a-1) \not\equiv \operatorname{ord}_2(b-1) \pmod 2$, then (1) has no solutions (x, n). In addition, several researchers have solved a lot of cases for (1) (see [4–6, 8–13, 17–20] and [7, Section 3.1]). But, in general, this is a problem that is far from resolved.

In this paper, we prove the following theorem:

Theorem 1.1. *If* $\{a, b\} \neq \{13, 239\}$ *and* $\operatorname{ord}_2(a^2-1) \neq \operatorname{ord}_2(b^2-1)$, *then* (1) *has no solutions* (x, n) *with* $2 \mid n$.

Combining Theorem 1.1 with [2, Result 5 (b)] (see Lemma 3.3 below) enables us to solve (1) in many of the cases where $a \equiv b \equiv 3 \pmod 4$, which have not been studied so far.

Corollary 1.2. *Suppose that either of the following conditions holds*:

(1) $a \equiv b \equiv 3 \pmod 4$ *and* $a \not\equiv b \pmod 8$;

(2) $a \equiv b \equiv 7 \pmod 8$ *and* $a \not\equiv b \pmod{16}$.

Then, (1) *has no solutions* (x, n).

2 Preliminaries

Let d be a fixed nonsquare positive integer. By the basic properties of Pell's equation

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

(see Chapter 8 of [14]), we can obtain the following lemma immediately.

Lemma 2.1. *Equation* (2) *has solutions* (u, v), *and it has a unique solution* (u_1, v_1) *such that* $u_1 + v_1\sqrt{d} \le u + v\sqrt{d}$, *where* (u, v) *runs through all solutions of* (2). *The solution* (u_1, v_1) *is called the least solution of* (2). *Moreover, for any positive integer* k, *let*

$$u_k = \frac{1}{2}\left(\theta^k + \bar{\theta}^k\right), \quad v_k = \frac{1}{2\sqrt{d}}\left(\theta^k - \bar{\theta}^k\right), \tag{3}$$

where

$$\theta = u_1 + v_1\sqrt{d}, \quad \bar{\theta} = u_1 - v_1\sqrt{d}. \tag{4}$$

Then, $(u, v) = (u_k, v_k)$ $(k = 1, 2, \cdots)$ *are all solutions of* (2).

Lemma 2.2. *If* $2 \mid k$*, then* $\operatorname{ord}_2 v_k \geq 1 + \operatorname{ord}_2(u_1 v_1)$.

Proof. Since $2 \mid k$, by (3) and (4), we have

$$v_k = u_1 v_1 \sum_{i=0}^{k/2-1} \binom{k}{2i+1} \left(u_1^2\right)^{k/2-i-1} \left(dv_1^2\right)^i. \tag{5}$$

Since $u_1^2 - dv_1^2 = 1$, one of u_1^2 and dv_1^2 has to be even and the other has to be odd, whence we get

$$2 \mid \sum_{i=0}^{k/2-1} \binom{k}{2i+1} \left(u_1^2\right)^{k/2-i-1} \left(dv_1^2\right)^i. \tag{6}$$

Therefore, by (5) and (6), we obtain the lemma immediately. □

Lemma 2.3. *Let* $r,\ s$ *be two positive integers. If* $\operatorname{ord}_2 v_r < \operatorname{ord}_2 v_s$*, then* $2 \mid s$.

Proof. For any positive integer k, by (3) and (4), we have $v_k \equiv 0 \pmod{v_1}$. It implies that

$$\operatorname{ord}_2 v_r \geq \operatorname{ord}_2 v_1. \tag{7}$$

If $2 \nmid s$, by (3) and (4), then we have

$$v_s = v_1 \sum_{j=0}^{(s-1)/2} \binom{s}{2j+1} \left(u_1^2\right)^{(s-1)/2-j} \left(dv_1^2\right)^j. \tag{8}$$

Recall that $u_1^2 \not\equiv dv_1^2 \pmod 2$. Hence, since $2 \nmid s$, we get

$$2 \nmid \sum_{j=0}^{(s-1)/2} \binom{s}{2j+1} \left(u_1^2\right)^{(s-1)/2-j} \left(dv_1^2\right)^j. \tag{9}$$

Therefore, by (8) and (9), we have

$$\operatorname{ord}_2 v_s = \operatorname{ord}_2 v_1. \tag{10}$$

However, since $\operatorname{ord}_2 v_r < \operatorname{ord}_2 v_s$, by (7) and (10), we get $\operatorname{ord}_2 v_1 \leq \operatorname{ord}_2 v_r < \operatorname{ord}_2 v_s = \operatorname{ord}_2 v_1$, a contradiction. Thus, we obtain $2 \mid s$. The lemma is proved. □

Lemma 2.4 (Proposition 8.1 of [1])**.** *The equation*

$$2X^2 - 1 = Y^m, \quad X, Y, m \in \mathbb{N},\ X > 1,\ Y > 1,\ m > 2 \tag{11}$$

has the only solution $(X, Y, m) = (78, 23, 3)$.

3 Proofs of Theorem 1.1 and Corollary 1.2

In this section, let (x, n) be a solution of (1).

Lemma 3.1 ([15])**.** *We have*

$$a^n - 1 = dy^2,\ b^n - 1 = dz^2, \quad d, y, z \in \mathbb{N},\ d > 1,\ d \textit{ is square-free}. \tag{12}$$

Lemma 3.2 ([2, Result 2])**.** *If* $\{a, b\} \neq \{13, 239\}$*, then* $4 \nmid n$.

Lemma 3.3 ([2, Result 5 (b)]). *If* $\operatorname{ord}_2(a-1) = \operatorname{ord}_2(b-1) > 0$ *and* $2^{3+\operatorname{ord}_2(a-1)} \nmid (a-b)$, *then* $2 \mid n$.

Proof of Theorem 1.1. We now assume that $2 \mid n$. Then, by Lemma 3.1, we see from (12) that (2) has two solutions $(u,v) = (a^{n/2}, y)$ and $(b^{n/2}, z)$. Hence, by Lemma 2.1, we have

$$a^{n/2} = u_r,\ y = v_r,\ b^{n/2} = u_s,\ z = v_s, \quad r,s \in \mathbb{N}. \tag{13}$$

Since $\{a,b\} \neq \{13, 239\}$, by Lemma 3.2, we have

$$2 || n. \tag{14}$$

Hence, we get

$$\operatorname{ord}_2(a^n-1) = \operatorname{ord}_2(a^2-1),\ \operatorname{ord}_2(b^n-1) = \operatorname{ord}_2(b^2-1). \tag{15}$$

On the other hand, since $n > 2$, by (14), $n/2$ is an odd positive integer with

$$\frac{n}{2} \geq 3. \tag{16}$$

By (12) and (15), we have

$$\begin{aligned}\operatorname{ord}_2(a^2-1) &= \operatorname{ord}_2(a^n-1) = \operatorname{ord}_2(dy^2) = \operatorname{ord}_2 d + 2\operatorname{ord}_2 y,\\ \operatorname{ord}_2(b^2-1) &= \operatorname{ord}_2(b^n-1) = \operatorname{ord}_2(dz^2) = \operatorname{ord}_2 d + 2\operatorname{ord}_2 z.\end{aligned} \tag{17}$$

Since $\operatorname{ord}_2(a^2-1) \neq \operatorname{ord}_2(b^2-1)$, we see from (17) that $\operatorname{ord}_2 y \neq \operatorname{ord}_2 z$. Further, since a and b are symmetric in (1), by (12), we may assume that

$$\operatorname{ord}_2 y < \operatorname{ord}_2 z \tag{18}$$

without loss of generality.

By (13) and (18), we have

$$\operatorname{ord}_2 v_r < \operatorname{ord}_2 v_s. \tag{19}$$

Hence, by Lemma 2.3, we get from (19) that $2 \mid s$. Then, by (3), (4) and (13), we have

$$\begin{aligned}b^{n/2} + z\sqrt{d} &= u_s + v_s\sqrt{d} = \left(u_1 + v_1\sqrt{d}\right)^s\\ &= \left(\left(u_1 + v_1\sqrt{d}\right)^{s/2}\right)^2 = \left(u_{s/2} + v_{s/2}\sqrt{d}\right)^2,\end{aligned}$$

whence we get

$$b^{n/2} = u_{s/2}^2 + dv_{s/2}^2. \tag{20}$$

Further, by Lemma 2.1, we have

$$u_{s/2}^2 - dv_{s/2}^2 = 1. \tag{21}$$

By (20) and (21), we get

$$b^{n/2} = 2u_{s/2}^2 - 1. \tag{22}$$

We find from (16) and (22) that (11) has a solution $(X, Y, m) = (u_{s/2}, b, n/2)$. Therefore, by Lemma 2.4, we have

$$u_{s/2} = 78,\ b = 23,\ \frac{n}{2} = 3. \tag{23}$$

By (21) and (23), we get $d = 6083 = 7 \times 11 \times 79$ and $v_{s/2} = 1$. It implies that $s/2 = 1$ and

$$u_1 = 78,\ v_1 = 1,\ v_s = v_2 = 2u_1v_1 = 156. \tag{24}$$

We see from (24) that $\operatorname{ord}_2 v_s = 2$. Hence, by (19), we have

$$\operatorname{ord}_2 v_r \leq 1. \tag{25}$$

Since $\operatorname{ord}_2(u_1v_1) = 1$ by (24), applying Lemma 2.2 to (25), we get $2 \nmid r$. Therefore, by (3), (4), (13), (23) and (24), we have

$$\begin{aligned} a^3 = a^{n/2} = u_r &= \frac{1}{2}\left(\left(78 + \sqrt{6083}\right)^r + \left(78 - \sqrt{6083}\right)^r\right) \\ &= 78 \sum_{i=0}^{(r-1)/2} \binom{r}{2i} 78^{r-2i-1} \cdot 6083^i. \end{aligned} \tag{26}$$

However, since $2||78$ and $2 \nmid r$, we get from (26) that $2||a^3$, a contradiction. Thus, the theorem is proved. □

Proof of Corollary 1.2. Suppose first that condition (1) holds. Then, $\operatorname{ord}_2(a-1) = \operatorname{ord}_2(b-1) = 1$ and $b - a \not\equiv 0 \pmod 8$. Hence, by Lemma 3.3 we obtain

$$2 \mid n. \tag{27}$$

On the other hand, putting $a = 4a_0 + 3$ and $b = 4b_0 + 3$ with $a_0,\ b_0$ non-negative integers, we have $b - a = 4(b_0 - a_0) \not\equiv 0 \pmod 8$, that is,

$$a_0 \not\equiv b_0 \pmod 2. \tag{28}$$

Since $a^2 - 1 = 8(2a_0^2 + 3a_0 + 1)$ and $b^2 - 1 = 8(2b_0^2 + 3b_0 + 1)$, we see from (28) that $\operatorname{ord}_2(a^2 - 1) \neq \operatorname{ord}_2(b^2 - 1)$. It follows from Theorem 1.1 that $2 \nmid n$, which contradicts (27).

Suppose second that condition (2) holds. Then, in the same way as above we obtain (27). On the other hand, putting $a = 8a_0 + 7$ and $b = 8b_0 + 7$ with $a_0,\ b_0$ non-negative integers, we have $b - a = 8(b_0 - a_0) \not\equiv 0 \pmod{16}$, that is, (28) holds. Since $a^2 - 1 = 16(4a_0^2 + 7a_0 + 3)$ and $b^2 - 1 = 16(4b_0^2 + 7b_0 + 3)$, we see from (28) that $\operatorname{ord}_2(a^2 - 1) \neq \operatorname{ord}_2(b^2 - 1)$. It follows from Theorem 1.1 that $2 \nmid n$, which contradicts (27). Therefore, the corollary is proved. □

Acknowledgements

The authors thank the referees for their careful reading and pointing out several typos.

References

[1] Bennett, M. A., & Skinner, C. M. (2004). Ternary Diophantine equations via Galois representations and modular forms. *Canadian Journal of Mathematics*, 56, 23–54.

[2] Cohn, J. H. E. (2002). The Diophantine equation $(a^n - 1)(b^n - 1) = x^2$. *Periodica Mathematica Hungarica*, 44, 169–175.

[3] Guo, X.-Y. (2013). A note on the Diophantine equation $(a^n - 1)(b^n - 1) = x^2$. *Periodica Mathematica Hungarica*, 66, 87–93.

[4] Hajdu, L., & Szalay, L. (2000). On the Diophantine equations $(2^n - 1)(6^n - 1) = x^2$ and $(a^n - 1)(a^{kn} - 1) = x^2$. *Periodica Mathematica Hungarica*, 40, 141–145.

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

[6] Le, M.-H. (2009). A note on the exponential Diophantine equation $(2^n - 1)(b^n - 1) = x^2$. *Publicationes Mathematicae Debrecen*, 74, 401–403.

[7] Le, M.-H., & Soydan, G. (2020). A brief survey on the generalized Lebesgue–Ramanujan–Nagell equation. *Surveys in Mathematics and its Applications*, 15, 473–523.

[8] Li, L., & Szalay, L. (2010). On the exponential Diophantine equation $(a^n - 1)(b^n - 1) = x^2$. *Publicationes Mathematicae Debrecen*, 77, 465–470.

[9] Li, Z.-J. (2011). *Research for the solution of the Diophantine equation* $(a^n - 1)(b^n - 1) = x^2$. Master's thesis, Wuhu: Anhui Normal University (in Chinese).

[10] Li, Z.-J., & Tang, M. (2010). On the Diophantine equation $(2^n - 1)(a^n - 1) = x^2$. *Journal of Anhui Normal University, Natural Science*, 33, 515–517 (in Chinese).

[11] Li, Z.-J., & Tang, M. (2011). A remark on a paper of Luca and Walsh. *Integers*, 11, 827–832.

[12] Liang, M. (2012). On the Diophantine equation $(a^n - 1)((a + 1)^n - 1) = x^2$. *Journal of Mathematics (Wuhan)*, 32, 511–514 (in Chinese).

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

[14] Mordell, L. J. (1969). *Diophantine Equations*, London: Academic Press.

[15] Noubissie, A., Togbé, A., & Zhang, Z.-F. (2020). On the exponential Diophantine equation $(a^n - 1)(b^n - 1) = x^2$. *The Bulletin of the Belgian Mathematical Society*, 27, 161–166.

[16] Szalay, L. (2000). On the Diophantine equation $(2^n - 1)(3^n - 1) = x^2$. *Publicationes Mathematicae Debrecen*, 57, 1–9.

[17] Tang, M. (2011). A note on the exponential Diophantine equation $(a^m - 1)(b^n - 1) = x^2$. *Journal of Mathematical Research and Exposition*, 31, 1064–1066.

[18] Yang, H., Pei, Y.-T., & Fu, R.-Q. (2016). The solvability of the Diophantine equation $(a^n - 1)((a + 1)^n - 1) = x^2$. *Journal of Xiamen University, Natural Science*, 55, 91–93 (in Chinese).

[19] Yang, S.-C., Wu, W.-Q., & Zheng, H. (2011). The solution of the Diophantine equation $(a^n - 1)(b^n - 1) = x^2$. *Journal of Southwest University, Natural Science*, 37, 31–34 (in Chinese).

[20] Yuan, P.-Z., & Zhang, Z.-F. (2012). On the Diophantine equation $(a^n - 1)(b^n - 1) = x^2$. *Publicationes Mathematicae Debrecen*, 80, 327–331.