Publ. Math. Debrecen
89/1-2 (2016), 253–256
DOI: 10.5486/PMD.2016.7578

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

By KATSUMASA ISHII (Tokyo)

Abstract. Let a and b be two distinct fixed positive integers such that $\min(a, b) > 1$. We give a necessary and sufficient condition for Diophantine equation $(a^n-1)(b^n-1) = x^2$ with $a \equiv 5 \pmod 6$ and $b \equiv 0 \pmod 3$ to have positive integer solutions.

Let $\mathbb{N}^+$ be the set of all positive integers. Let a and b be two distinct fixed positive integers such that $\min(a, b) > 1$ and consider the exponential Diophantine equation

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

There are many results concerned with (1) (for example, see [2], [3], [4], [5] and [6]). Szalay [6] considered the case where $(a, b) = (2, 3), (2, 5)$ and $(2, 2^k)$, and Hajdu and Szalay [3] considered the case where $(a, b) = (2, 6)$ and (a, a^k). Le [5] treated the more general case, that is where $a = 2$ and $b \equiv 0 \pmod 3$, and showed that in this case (1) has no solution.

Recently Lan and Szalay [4] showed that (1) has no solution if $a \equiv 2 \pmod 6$ and $b \equiv 0 \pmod 3$. In this note we consider the case where $a \equiv 5 \pmod 6$ and $b \equiv 0 \pmod 3$.

Let d be a positive integer which is not a square. Then the Pell equation

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

has infinitely many solutions (u, v). If (u_1, v_1) denotes the smallest non-trivial positive solution, then every positive solution (u_k, v_k) can be generated by

$$u_k + v_k\sqrt{d} = (u_1 + v_1\sqrt{d})^k.$$

Our main result is the following.

Mathematics Subject Classification: Primary: 11D41, 11D61.
Key words and phrases: exponential Diophantine equation, Pell equation.

Theorem. *Suppose that* $a \equiv 5 \pmod 6$ *and* $b \equiv 0 \pmod 3$. *Then the equation* $(a^n - 1)(b^n - 1) = x^2$ *has positive integer solution* (x, n) *if and only if* $(a, b) = (u_r, u_s)$ *with non-square* $d \equiv 2 \pmod 3$ *satisfying* $u_1 \equiv 0 \pmod 3$, $r \equiv 2 \pmod 4$ *and* s *is odd. In this case a solution is* $(x, n) = (dv_r v_s, 2)$.

In order to prove this, we need some lemmata. The first lemma is concerned with the sequence u_k, and is due to Lan and Szalay [4].

Lemma 1. *Let* d *be a positive integer which is not a 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* $u_1 | u_k$.

(3) *If* $q \in \{2, 3, 5\}$, *then* $q | u_k$ *implies* $q | u_1$.

Proof. See Lemma 1 in [4]. □

Furthermore, we need two results on Diophantine equations.

Lemma 2. *Let* p *be an odd prime with* $p > 3$. *Then the equation*

$$X^p + 1 = 2Y^2, \quad X, Y \in \mathbb{N}^+$$

has only the solution $(X, Y) = (1, 1)$.

Proof. By Theorem 1 in [1] the equation

$$x^p + y^p = 2z^2$$

has no solution in nonzero pairwise coprime integers with $x > y$ except $(x, y, z) = (3, -1, \pm 11)$ when $p = 5$. Therefore, the lemma follows. □

Lemma 3. *The equation*

$$X^3 + 1 = 2Y^2, \quad X, Y \in \mathbb{N}^+$$

has only the solutions $(X, Y) = (1, 1)$ *and* $(23, 78)$.

Proof. This is one of the results of [7]. □

Proof of the Theorem. Put $d = \gcd(a^n - 1, b^n - 1)$. Then

$$a^n - 1 = dy^2, \quad b^n - 1 = dz^2$$

for some y and z. Since $b \equiv 0 \pmod 3$ we have $z \not\equiv 0 \pmod 3$, which yields that $z^2 \equiv 1 \pmod 3$. Therefore, $d \equiv b^n - 1 \equiv 2 \pmod 3$.

Furthermore, if $y \not\equiv 0 \pmod 3$, then $y^2 \equiv 1 \pmod 3$ and hence $a^n = dy^2 + 1 \equiv 0 \pmod 3$, which contradicts that $a \equiv 2 \pmod 3$. Therefore, we have $y \equiv 0 \pmod 3$ and hence $2^n \equiv a^n = dy^2 + 1 \equiv 1 \pmod 3$. This implies that n is even.

Now put $n = 2m$. Then $u^2 - dv^2 = 1$ has two solutions (a^m, y) and (b^m, z) and hence $(a^m, y) = (u_r, v_r)$ and $(b^m, z) = (u_s, v_s)$ for some r and s. If s is even, then each prime factor p of b satisfies $p \equiv \pm 1 \pmod 8$ by Lemma 1(1), which is impossible since $b \equiv 0 \pmod 3$. Therefore, s must be odd. This implies that $u_1 \equiv 0 \pmod 3$ by Lemma 1(3). Furthermore, if r is odd, then we have $a \equiv 0 \pmod 3$ by Lemma 1(2) and $u_1 \equiv 0 \pmod 3$, a contradiction. Therefore, r is even. Put $r = 2t$. Then $u_r + v_r\sqrt{d} = (u_t + v_t\sqrt{d})^2$ and hence $a^m = u_t^2 + dv_t^2$. Since $u_t^2 - dv_t^2 = 1$ we have $a^m + 1 = 2u_t^2$.

Now notice that m is odd by Result 2 of [2]. By Lemma 2, m must be 1 or a power of 3. Suppose that $m = 3^e$ and $a_0 = a^{3^{e-1}}$. By Lemma 3, we have $a_0 = 23$ and $u_t = 78$ (and hence e must be 1, that is, $a = 23$). Furthermore, since $78^2 - dv_t^2 = 1$ we have $dv_t^2 = 6083 = 7 \cdot 11 \cdot 79$, which yields that $d = 6083$ and $v_t = 1$. Therefore, $\gcd(23^6 - 1, b^6 - 1) = 6083$, which implies that b must be even. Then $b^6 - 1 \not\equiv 6083z^2 \pmod 8$, a contradiction. Therefore, we have $m = 1$.

Now suppose that $r \equiv 0 \pmod 4$. Then t is even and hence $u_t \not\equiv 0 \pmod 3$ by Lemma 1(1). Then $u_r = u_t^2 + dv_t^2 = 2u_t^2 - 1 \not\equiv 5 \pmod 6$, which contradicts that $a \equiv 5 \pmod 6$.

Conversely, suppose that $(a, b) = (u_r, u_s)$ with $d \equiv 2 \pmod 3$, $u_1 \equiv 0 \pmod 3$, $r \equiv 2 \pmod 4$ and s is odd. Then $(a^n - 1)(b^n - 1) = x^2$ has solution $(x, n) = (dv_rv_s, 2)$. Note that $b \equiv u_t \equiv 0 \pmod 3$ by Lemma 1(2) and hence $a = 2u_t^2 - 1 \equiv 5 \pmod 6$. This completes the proof. □

Remark. Actually there exists $d \equiv 2 \pmod 3$ with $u_1 \equiv 0 \pmod 3$. For example, $u_1 = 6$ for $d = 35$. Therefore, there exist infinitely many pairs (a, b) such that (1) has the solution. In the case of $d = 35$ the first few pairs (a, b) are $(u_2, u_3) = (71, 846)$, $(u_2, u_5) = (71, 120126)$, $(u_6, u_5) = (1431431, 120126)$ and so on.

References

[1] M. A. Bennett and C. M. Skinner, Ternary Diophantine equation 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** (2002), 169–175.

[3] L. Hajdu and L. Szalay, On the Diophantine equations $(2^n-1)(6^n-1)=x^2$ and $(a^n-1)(b^{kn}-1)=x^2$, *Period. Math. Hungar.* **40** (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. H. Le, A note on the exponential diophantine equation $(2^n - 1)(b^n - 1) = x^2$, *Publ. Math. Debrecen* **74** (2009), 401–403.

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

[7] W. Robert and van der Waall, 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), 39–51.

KATSUMASA ISHII
6-3-201, MIYASAKA 2-CHOME
SETAGAYA-KU
TOKYO, 156-0051
JAPAN

E-mail: 9652okok@jcom.zaq.ne.jp

(Received August 19, 2015; revised January 22, 2016)