Paper

Existence Conditions and the Number of Solutions in Positive Integers $(x,\ y)$ on an Equation $a^x - b^y = 2$

Nobuo Kobachi*

Abstract Let $a,\ b \in \mathrm{N} \setminus \{1\}$. We show that an equation $a^x - b^y = 2$ has at most one solution in positive integers $(x,\ y)$. Espesially, when $ab \equiv 1 \bmod 2$ and $\gcd(a,\ b) = 1$ is satisfied, under certain six conditions, we show an equation $a^x - b^y = 2$ has at most one solution by using "minimal unit". And, in its proof, we can find existence conditions of solutions.

Keywords: Diophantine equation, Number of solutions, Existence condition, Minimal unit, Quadratic field

1. INTORODUCTION

The existence of solution in positive integers $(x,\ y)$ on Diophantine equation $a^x - b^y = c$ is studied by many authors. Especially, in the case of $c = 1$, Catalan's conjecture that if $a,\ b,\ x$ and y are positive integers greater than one then $a^x - b^y = 1$ has no solutions except $3^2 - 2^3 = 1$ is well-known. This was proved by P.Mihăilescu in 2002[1]. Let p and q be prime numbers. On the number of solutions, an equation $p^x - q^y = 2^h$, where h is a positive integer , has at most one solution and an equation $p^x - b^y = c$, where b and c are positive integers relative to prime p, has at most one solution $(x,\ y)$ with $y > 1$ if $b > c$ are shown in [2].

Let $a,\ b \in \mathrm{N}^{\#} = \mathrm{N} \setminus \{1\}$. In this paper, we consider the existence conditions and the number of solutions in $(x,\ y) \in \mathrm{N} \times \mathrm{N}$ on an equation

(1.1) $a^x - b^y = 2$.

Let $ab \equiv 0,\ a + b = 0 \bmod 2$. Then $a^x - b^y \equiv 1 \bmod 2$ is satisfied. Thus (1.1) has no solutions.

Let $a,\ b \equiv 0 \bmod 2$ and $\gcd(a,\ b) \neq 2$. Then $a^x - b^y \equiv 0 \bmod \gcd(a,\ b)$ is satisfied. Thus (1.1) has no solutions.

Let $\gcd(a,\ b) = 2$. If $x,\ y \geq 2$, then $a^x - b^y \equiv 0 \bmod 4$ is satisfied. Thus (1.1) has no solutions in $(x,\ y) \in \mathrm{N}^{\#} \times \mathrm{N}^{\#}$.

Therefore $\gcd(a,\ b) = 2$ and $(x-1)(y-1) = 0$ are necessary conditions so that (1.1) with $ab \equiv 0 \bmod 2$ has solutions.

Let $x_0 = \log_a(b+2)$, $y_0 = \log_b(a-2)$ if $a \neq 2$ and $y_0 = -\infty$ if $a = 2$. Then the following proposition is satisfied.

Proposition 1 Let $ab \equiv 0 \bmod 2$.

---

* Faculty of Liberal Studies
2627 Hirayama-Shinmachi, Yatsushiro-shi, Kumamoto, 866-8501, Japan

1) In the case of $\gcd(a,\ b) \neq 2$, the equation (1.1) has no solutions.

2) In the case of $\gcd(a,\ b) = 2$, the equation (1.1) has solutions, if and only if $x_0 \in \mathbb{N}$ or $y_0 \in \mathbb{N}$ is satisfied. And there is a unique solution $(x_0,\ 1)$ or $(1,\ y_0)$.

Let $ab \equiv 1 \bmod 2$ and $\gcd(a,\ b) \neq 1$. Then $a^x - b^y \equiv 0 \bmod \gcd(a,\ b)$ is satisfied. Thus, (1.1) has no solutions.

Therefore $\gcd(a,\ b) = 1$ is a necessary condition so that (1.1) with $ab \equiv 1 \bmod 2$ has solutions.

We put six conditions as follows;

(1) $a \equiv 3,\ b \equiv 1 \bmod 4$ and $x \equiv 1,\ y \equiv 0 \bmod 2$,

(2) $a \equiv 3,\ b \equiv 3 \bmod 4$ and $x \equiv 1,\ y \equiv 0 \bmod 2$,

(3) $a \equiv 1,\ b \equiv 3 \bmod 4$ and $x \equiv 0,\ y \equiv 1 \bmod 2$,

(4) $a \equiv 3,\ b \equiv 3 \bmod 4$ and $x \equiv 0,\ y \equiv 1 \bmod 2$,

(5) $a \equiv 3,\ b \equiv 1 \bmod 4$ and $x \equiv 1,\ y \equiv 1 \bmod 2$,

(6) $a \equiv 1,\ b \equiv 3 \bmod 4$ and $x \equiv 1,\ y \equiv 1 \bmod 2$.

Then we can obtain the follwing proposition.

Proposition 2 Let $ab \equiv 1 \bmod 2$ and $\gcd(a,\ b) = 1$.

1) If all of the conditions (1)-(6) are not satisfied, the (1.1) has no solutions.
2) If one of the conditions (1)-(6) is satisfied, the (1.1) has at most one solution.

Indeed, we can obtain the first half of Proposition 2 from $a^x - b^y \equiv 0 \bmod 4$. We consider the second half of Proposition 2 in later sections.

2. PRELIMINARIES

In this section, we prepare two lemmas. These are used for the proof of Proposition 2 in section 4

Lemma 2.1 Let $a \equiv 3 \bmod 4$ and $x \in \mathbb{N}$. An inequation $a^x \geq 4x + 3$ is satisfied except two cases of $(a,\ x) = (3,\ 1),\ (3,\ 2)$.

Proof Let $f(x) = a^x - 4x - 3$. Because $f(x)$ is a monotone increasing function and $f(1) = a - 7$ are satisfied, the result is led in the case of $a \geq 7$. In the case of $a = 3$, we have $f(2) < 0,\ f(3) > 0$. Thus an inequation $3^x \geq 4x + 3$ for $x \geq 3$ is satisfied.

□

Lemma 2.2 Let $ab \equiv 1 \bmod 2$ and $(a,\ b) = 1$, and one of the condtions (1)-(6) be satisfid. Then we put x and y as follows;

1) $x = 2m + 1,\ y = 2n$ ($m \in \mathbb{N}^* = \mathbb{N} \cup \{0\},\ n \in \mathbb{N}$), if condition (1) or (2) is satisfied,

2) $x = 2m,\ y = 2n + 1$ ($m \in \mathbb{N},\ n \in \mathbb{N}^*$), if condition (3) or (4) is satisfied,

3) $x=2m+1,\ y=2n+1$ ($m,\ n\in\mathbb{N}^*$), if condition (5) or (6) is satisfied.

If $(x,\ y)$ is a solutin of (1,1), then two inequations $a^{m+1}>b^n$ and $b^{n+1}>a^m$ are satisfied.

Proof In the case of $x=2m+1$ and $y=2n$, we have $a^{2m+2}>a^{2m+1}>b^{2n}$ and $b^{2n+2}-a^{2m}>b^{2n}-a^{2m}=(a^{2m+1}-2)-a^{2m}$ $=(a-1)a^{2m}-2>2(a^{2m}-1)>0$. Thus the result is obtained. In the other cases, we can similarly lead the result.

□

3. MINIMAL UNIT

In this section, we define "minimal unit" and we show some propeties on "minimal unit"

Let $ab\equiv 1 \bmod 2$ and $(a,\ b)=1$. And one of the condtions (1)-(6) is satisfid. Then we put

$$(3.1)\qquad k=\begin{cases} a, & \text{if condition (1) or (2) is satisfied,}\\ b, & \text{if condition (3) or (4) is satisfied,}\\ ab, & \text{if condition (5) or (6) is satisfied .}\end{cases}$$

There are $\lambda\in\mathbb{N}$ and $d\in\mathbb{N}$ that $k=\lambda^2 d$ and d doesn't conculde square numbers. Then we remark that $d\equiv 3 \bmod 4$ is satisfied from $k\equiv 3 \bmod 4$. Let $\varepsilon=t+u\sqrt{d}$ be a fundamental unit of quadratic field $\mathbb{Q}(\sqrt{d})$ and we put $\varepsilon^j=t_j+u_j\sqrt{d}$ for $j\in\mathbb{N}$. Then a "minimal unit" $\eta=s+v\sqrt{k}$ is defind as follows.

1) In the case of $\lambda=1$, let $\eta:=\varepsilon=t+u\sqrt{k}$ ($\Leftrightarrow s=t,\ v=u$).

2) In the case of $\lambda\neq 1$ and $\lambda\,|\,u$, let $\eta:=\varepsilon=t+(u/\lambda)\sqrt{k}$ ($\Leftrightarrow s=t,\ v=u/\lambda$).

3) In the case of $\lambda\neq 1$ and $\lambda\nmid u$, there is a number $l\in\mathbb{N}$ that $\lambda\,|\,u_l$ and $\lambda\nmid u_j$ for $1\le j<l$.

let $\eta:=\varepsilon^l=t_l+(u^l/\lambda)\sqrt{k}$ ($\Leftrightarrow s=t_l,\ v=u_l/\lambda$).

Furthermore, let $\eta^j=s_j+v_j\sqrt{d}$ and $\omega_j=\sum_{i=0}^{\left[\frac{j-1}{2}\right]} {}_jC_{2i+1}s^{j-2i-1}(kv^2)^i$ for $j\in\mathbb{N}$.

Lemma 3.1 For $j\in\mathbb{N}$, the following relations are satisfied.

1) $N(\eta^j)=1$.

2) $s_j^2\equiv 1 \bmod k$.

3) $v_j=v\omega_j$.

4) $\begin{cases}\omega_1=1,\ \omega_2=2s\\ \omega_{j+2}=2s\omega_{j+1}-\omega_j\end{cases}$.

5) $\omega_j\equiv\begin{cases}0 \bmod 2, & if\ j\equiv 0 \bmod 2\\ 1 \bmod 2, & if\ j\equiv 1 \bmod 2\end{cases}$.

6) $\omega_j\equiv j \bmod k$ for $j\equiv 1 \bmod 2$.

Proof 1) If $t\equiv u$ mod 2 is satisfied, $N(\varepsilon)=t^2+u^2d\equiv 0 \bmod 2$ is obtained. It's contradictory to $N(\varepsilon)=1$ or

$N(\varepsilon) = -1$. Thus the case of $t \equiv u \mod 2$ doesn't occur. In the rest cases, we have $N(\varepsilon) \equiv 1 \mod 4$ from $d \equiv 3 \mod 4$. Thus $N(\varepsilon) = 1$ is satisfied. This leads $N(\eta^j) = 1$.

2) From $N(\eta^j) = s_j^2 + kv_j^2 = 1$, we have $s_j^2 \equiv 1 \mod k$.

3) We have $v_j = \sum_{i=0}^{\left[\frac{j-1}{2}\right]} {}_jC_{2i+1} s^{j-2i-1} v^{2i+1} k^i = v\omega_j$ by direct calculations.

4) From $\eta^{j+1} = (s + kv)(s_j + v_j\sqrt{k})$, we have $s_{j+1} = ss_j + kvv_j$ and $v_{j+1} = vs_j + sv_j$. These lead $v_{j+2} = 2sv_{j+1} - N(\eta)v_j$. Thus $\omega_{j+2} = 2s\omega_{j+1} - \omega_j$ holds from $N(\eta^j) = 1$ and $v_j = v\omega_j$. And we have $\omega_1 = 1,\ \omega_2 = 2s$ by easy calculations.

5) This result is obtaind from the recurrence formula on the previous item.

6) From $s_j^2 \equiv 1 \mod k$, we have $\omega_j \equiv js^{j-1} \equiv j \mod k$ for $j \equiv 1 \mod 2$.

□

Lemma 3.2 Relations $k \mid \omega_k$ and $k^2 \nmid \omega_k$ are satisfid.

Proof In the case of $k = 3$, we have $\omega_3 = 18$ from $\eta = \varepsilon = 2 + \sqrt{3}$. Thus $3 \mid \omega_3$ and $3^2 \nmid \omega_3$ are satisified.

In the case of $k > 3$, we have

$$\omega_{3k} = 3ks^{3k-1} + k^2 \left\{ {}_{3k-1}C_2 s^{3k-3} v^2 + v^4 \sum_{i=2}^{\frac{k-1}{2}} {}_{3k}C_{2i+1} s^{3k-2i-1} (kv^2)^{i-2} \right\}. \tag{3.1}$$

Thus $k \mid \omega_{3k}$ and $k^2 \nmid \omega_{3k}$ is satisified.

On the other hand, we have $v_{3k} = 3s_k^2 v_k + kv_k^3$ from $\eta^{3k} = (\eta^k)^3 = (s_k + v_k\sqrt{k})^3$. It leads $\omega_{3k} = \omega_k(3s_k^2 + kv^2\omega_k^2)$ from $v_j = v\omega_j$.

From lemma 5.1, we have $k \mid \omega_k$ and $k \nmid 3s_k^2 + kv^2\omega_k^2$. Thus $k \mid \omega_k$ and $k^2 \nmid \omega_k$ are satisified in the case of $k > 3$.

□

Lemma 3.3 For $j \equiv 1 \mod 2$ and $n \in \mathbb{N}$, the following relations are satisfied.

1) $k^n \mid \omega_j$ is equivalent to $k^n \mid j$.

2) $k^n \mid \omega_{k^n}$, $k^{n+1} \nmid \omega_{k^n}$

Proof From $\eta^{jk^n} = (\eta^{k^n})^j = (s_{k^n} + v_{k^n}\sqrt{k})^j$, we have

$$\omega_{k^n j} = \omega_{k^n} \sum_{i=0}^{\frac{j-1}{2}} {}_jC_{2i+1} s_{k^n}^{j-2i-1} (kv_{k^n}^2)^i. \tag{3.2}$$

Thus $\omega_{k^n j} / \omega_{k^n} \equiv j \mod k$ is satisfied.

Now we suppose $k^n \mid \omega_{k^n}$ and $k^{n+1} \nmid \omega_{k^n}$ are satisfied. We have the following results;

1) $k^{n+1} \mid \omega_j$ is equivalent to $k^{n+1} \mid j$,

2) $k^{n+1} \mid \omega_{k^{n+1}}$, $k^{n+2} \nmid \omega_{k^{n+1}}$.

Therefore the results are led by lemma 3.2 and the inductive method.

□

4. PROOF OF PROPOSITION

Let $ab \equiv 1 \bmod 2$ and $(a,\ b)=1$, and one of the conditions (1)-(6) be satisfied. Futhermore we use the notations defined in section 2 and section 3.

Now we put

(4.1) $$\xi = \frac{a^x+b^y}{2} + \sqrt{a^x b^y} = \frac{a^x+b^y}{2} + a^m b^n \sqrt{k}\ ,$$

Then we have

$$N(\xi) = \left(\frac{a^x+b^y}{2}\right)^2 - a^x b^y = \left(\frac{a^x-b^y}{2}\right)^2 .$$

If the equation $a^x - b^y = 2$ holds, ξ is a unit of quadratic extended field $\mathbb{Q}(\sqrt{d})$.Thus there is an odd number j that $v\omega_j = a^m b^n$ is satisfied.

Next let $\mu \in \mathbb{N}$ be $\gcd(a,\ \mu) = \gcd(b,\ \mu) = 1$. And we put $v = \mu a^{m_0} b^{n_0}$, where $m_0,\ n_0 \in \mathbb{N}^*$.

Obviously, in the case of $\mu \neq 1$, (1.1) has no solutions. That is, $\mu = 1$ is a necessary condition that (1.1) with $ab \equiv 1 \bmod 2$ and $(a,\ b) \equiv 1$ has any solutions.

Furthermore we put $\omega_j = a^{m-m_0} b^{n-n_0} = a^M b^N$.

We suppose that condition (1) or (2) holds. If $M > 0$ is satisfied, we have $a^M \mid \omega_j$. It leads $a^M \mid j$ from lemma 3.3. And, from lemma 2.1, we have

(4.2) $$\frac{j-1}{2} \geq \frac{a^M - 1}{2} \geq \frac{(4M+3)-1}{2} = 2M+1$$

except two cases of $(a,\ M) = (3,\ 1),\ (3,\ 2)$. Thus, the follwing inequation is satisfied.

(4.3) $$a^m b^n \geq a^M b^N = w_j = \sum_{i=0}^{\frac{j-1}{2}} {}_jC_{2i+1} s^{j-2i-1} (av^2)^i > a^{2M+1} v^2 > a^{2m+1} .$$

Because (4.3) leads $b^n > a^{m+1}$, if (1.1) has solutions under the above conditions, it is contoradictry to the result of lemma 2.2. Therefore, if the above conditions hold, a pair $(a,\ b,\ x=2m+1,\ y=2n)$ satisfied with $\eta = s + a^m b^n \sqrt{a}$ holds the equation $a^x - b^y = 2$. In the cases of $(a,\ M) = (3,\ 0),\ (3,\ 1)$ and $(3,\ 2)$, one pair $(a,\ b,\ x,\ y) = (3,\ 5,\ 3,\ 2)$ holds the equation $a^x - b^y = 2$. Indeed, when $a = 3$ is satisfied, we have $M = m$ from $\eta = \varepsilon = 2 + \sqrt{3}$. Thus its result is obtained by substituting the equation $3^{2m+1} - b^{2n} = 2$ for $m = 0,\ 1,\ 2$ directly.

We suppose that condition (3) or (4) holds. Then we similary obtain a result that one pair $(a,\ b,\ x=2m,\ y=2n+1)$ with $\eta = s + a^m b^n \sqrt{b}$ satiesfies an equation $a^x - b^y = 2$. And, in the case of $(b,\ N) = (3,\ 1),\ (3,\ 2)$, An equation $a^x - b^y = 2$ doesn't hold.

We suppose that condition (5) or (6) holds. Then we similary obtain a result that one pair $(a,\ b,\ x = 2m+1,\ y = 2n+1)$ with $\eta = s + a^m b^n \sqrt{ab}$ satiesfies an equation $a^x - b^y = 2$.

Thus the second half of Proposition 2 is proved.

Considering the circumstances mentioned above, the following theorem is satisfied. This theorem means existence conditions of solution in (1.1) with $ab \equiv 1 \bmod 2$ and $(a,\ b) = 1$.

Theorem 1 Let $ab \equiv 1 \bmod 2$ and $(a,\ b) = 1$.

1) One pair $(a,\ b,\ x,\ y) = (3,\ 5,\ 3,\ 2)$ satiesfies an equation $a^x - b^y = 2$.

2) In the case of $a \equiv 3 \bmod 4$ except $a = 3$, if $\eta = s + a^m b^n \sqrt{a}$ then one pair $(a,\ b,\ x = 2m+1,\ y = 2m)$ satisfies an equation $|a^x - b^y| = 2$.

3) In the case of $ab \equiv 3 \bmod 4$, if $\eta = s + a^m b^n \sqrt{ab}$ then pair $(a,\ b,\ x = 2m+1,\ y = 2m+1)$ satisfies an equation $|a^x - b^y| = 2$.

5. APPENDIX

Proposition 3 Let $ab \equiv 1 \bmod 2$ and $(a,\ b) = 1$.

1) The equation (1.1) can't have two solutions satisfying both condition (3) and (6).
2) The equation (1.1) can't have two solutions satisfying both condition (2) and (4).
3) The equation (1.1) can't have two solutions satisfying both condition (1) and (5).

Proof 1) Let $a \equiv 1,\ b \equiv 3 \bmod 4$. We suppose that there are four numbers $x_1 \equiv 0,\ y_1 \equiv x_2 \equiv y_2 \equiv 1 \bmod 2$ that $a^{x_1} - b^{y_1} = a^{x_2} - b^{y_2} = 2$. The result is led by using 2-adic valuation $v_2(a)$. Now we have $v_2(a-1) < v_2(a^{x_1}-1)$ $= v_2(b^{y_1}+1) = v_2(b+1)$. On the other hand, we have $v_2(a-1) = v_2(a^{x_2}-1) = v_2(b^{y_2}+1) = v_2(b+1)$. Thus the contradiction occurs.

2) Let $a \equiv b \equiv 3 \bmod 4$. We suppose that there are four numbers $x_1,\ y_2 \equiv 1 \bmod 2$ and $x_1 \equiv y_2 \equiv 1,\ y_1 \equiv x_2 \equiv 0 \bmod 2$ that $a^{x_1} - b^{y_1} = a^{x_2} - b^{y_2} = 2$. Then the result is led by using Jacobi symbol $\left(\dfrac{a}{b}\right)$.

We have $\left(\dfrac{2}{a}\right) = \left(\dfrac{-1}{a}\right) = -1$ and $\left(\dfrac{2}{b}\right) = \left(\dfrac{a}{b}\right)$ from $a^{x_1} - b^{y_1} = 2$. And we have $\left(\dfrac{2}{a}\right) = -\left(\dfrac{b}{a}\right)$ and $\left(\dfrac{2}{b}\right) = 1$ from $a^{2m_2} - b^{2n_2+1} = 2$. Thus $\left(\dfrac{b}{a}\right) = \left(\dfrac{a}{b}\right) = 1$ is obtained. Therefore $\left(\dfrac{b}{a}\right)\left(\dfrac{a}{b}\right) = 1$ is satisfied.

However this is contoradictry to the quadratic reciprocity law that if $a \equiv b \equiv 3 \bmod 4$ then $\left(\dfrac{b}{a}\right)\left(\dfrac{a}{b}\right) = -1$ is satisfied.

3) Let $a \equiv 3,\ b \equiv 1 \bmod 4$. We suppose that there are four numbers $x_1 \equiv y_1 \equiv x_2 \equiv 1,\ y_2 \equiv 0 \bmod 2$ that $a^{x_1} - b^{y_1} = a^{x_2} - b^{y_2} = 2$. From $a \equiv 3 \bmod 4$, there is an odd number a' that $a = 2a' + 1$ is satisfied. In the case of $a' > 1$, there is an odd prime number p that $p \mid a'$ is satisfied. Thus we have $a \equiv 1 \bmod p$ from $a = 2a' + 1$.

Therefore $b^{y_1} \equiv b^{y_2} \equiv -1 \bmod p$ is obtained from $a^{x_1} - b^{y_1} = a^{x_2} - b^{y_2} = 2$. Thus the contradiction occurs, because $b^{y_1} \equiv b^{y_2} \equiv -1 \bmod p$ leads $O_p(b) \equiv 1 \bmod 2$, where notation $O_p(b)$ is the order of b modulo a prime p .

Now we put $a' = 1$. That is $a = 3$. We have that only pair $(a, b, x, y) = (3, 5, 3, 2)$ satiesfies (1.1) with condition (1) from theorem 1. On the other hand, if $ab = 15$ is satisfied, only one pair $(a, b, x, y) = (5, 3, 1, 1)$ satisfis (1.1) with condition (5). Thus (1.1) can’t have two solutions satisfying both condition (1) and (5).

□

Thus, the follwing theorem is obtained from proposition 1-3.

Theorem 2 Let $a, b \in \mathrm{N}^{\#}$. The equation $a^x - b^y = 2$ has at most one solution in positive integers (x, y) .

ACKNOWLEDGMENT

Y. Motoda[3] was a professor in Yatsushiro National College of Technorogy. Since he retired, author has been receiving his guidance in algebratic number theorey. Author would like to express a gratitude to Y. Motoda for valuable comments in this paper overall.

(Received: Sep. 25, 2015)
(Accepted: Dec. 25, 2015)

References

[1] P.Mihăilescu : Primary Cyclotomic Units and a Proof of Catalan’s Conjecture, J.reine angew. Math.572(2004), pp.167-195

[2] R.Scott and R.Styer : On $p^x - q^y = c$ and related three term exponentia Diophantine equations with prome bases, J. Number Theory 105(2004), pp.212-234

[3] Y.Motoda : Appendix and corrigenda to “Notes on Quartic Fields”, Rep. Fac. Sci. Engrg. Saga Univ. Math. 37-1(2008), pp.1-8

[4] 高木貞治: 代数的整数論 第２版, 岩波書店(1971)