International Journal of Contemporary Mathematical Sciences
Vol. 12, 2017, no. 2, 73 - 81
HIKARI Ltd, www.m-hikari.com
https://doi.org/10.12988/ijcms.2017.728

On a Diophantine Equation[1]

Xin Zhang

Department of Mathematics
Nanjing Normal University
Nanjing 210023, P.R. China

Abstract

In this note, we mainly obtain the equation $x^{2m} - y^n = z^2$ have finite positive integer solutions (x, y, z, m, n) satisfying $x > y$ be two consecutive primes.

Mathematics Subject Classification: 11A41; 11D41

Keywords: Diophantine equation; Consecutive primes

1 Introduction and main results

In 1844, Catalan proposed the following conjecture.

Conjecture 1.1 *The only two consecutive numbers in the sequence of perfect powers of natural numbers*

$$1, 4, 8, 9, 16, 25, 27, 32, 36, 49, 64, 81, 100, 121, 125, 128, 144, 169, \ldots$$

are 8 *and* 9*.*

[1]This work was partially supported by the Grant No. 11471162 from NNSF of China and the Specialized Research Fund for the Doctoral Program of Higher Education of China (Grant No. 20133207110012).

Between 2000 and 2004, Mihăilescu [9], [10] proved this conjecture is true. Before this, there are many efforts on the Catalan Conjecture and a series of such equations were studied. As a general case, the Diophantine equation

$$ax^m - by^n = c, \quad a, b, c, x, y, m, n \in \mathbb{Z}$$

was extensive studied by many experts. One can see [3], [8], [5], [6] for more detail.

In this note, we consider the following equation

$$x^m - y^n = z^2. \tag{1.1}$$

In 2002, Le [7] showed that the equation (1.1) has no solution for $y = 2$ and $2|n$. In 2008, Bérczes and Pink [2] gave the solution about the equation (1.1) in the case that $y = p$, $2|n$, and $2 \leq p < 100$. In 2016, Ventullo [13] gave some examples to the equation (1.1) in the case that $x > y$ are two consecutive primes.

We continue to study the equation (1.1) as in [13] which consider the case that $x > y$ are two consecutive primes. It is obviously that $(m, n, z) = (0, 0, 0)$ is a solution for any given consecutive primes p, q to the equation (1.1). We call this solution as trivial solution. It is nature to ask the question that does there exists consecutive primes p, q such that the equation (1.1) has only the trivial solution? Actually, we have the following result:

Theorem 1.1 *There are infinitely many consecutive primes p and q $(p > q)$ such that the equation*

$$p^m - q^n = z^2$$

has only the trivial solution.

Anther question is that dose it have finite solutions if the equation (1.1) have non-trivial solutions. In fact, we obtain:

Theorem 1.2 *Let p, q be two primes. Then the equation*

$$p^{2m} - q^n = z^2$$

has at most one non-trivial solution (m, n, z) in natural number except $q = 2$.

Theorem 1.3 *There are only finite solutions (x, y, z, m, n) to the equation*

$$x^{2m} - y^n = z^2$$

in natural number such that $x > y$ be two consecutive primes.

2 Some lemmas

In this section, we give some examples and some useful lemmas.

Lemma 2.1 *([12]) Let A be a discrete valuation ring, and let x_i be element of the field of fractions of A such that $v(x_i) > v(x_1)$ for $i \geq 2$. One then has* $\sum_{i=1}^{n} x_i \neq 0$.

Lemma 2.2 *Let p be a prime and n a natural number. Then $ord_p(n) \leq \log n/\log p$. Moreover, if $n > 2$, then $ord_p(n(n-1)) < n-1$.*

Lemma 2.3 *Let m, n be two positive integers. Then*

$$\sum_{m=0}^{n} \binom{2n+1}{2m+1}(-1)^{m+1}2^m \neq -1.$$

Proof: Firstly, we assume that

$$\sum_{m=0}^{n} \binom{2n+1}{2m+1}(-1)^{m+1}2^m = -1.$$

Then

$$-2n + \binom{2n+1}{3}2 - \binom{2n+1}{5}2^2 + \sum_{m=3}^{n} \binom{2n+1}{2m+1}(-1)^{m+1}2^m = 0.$$

By Lemma 2.2, for $m = 3, 4, \ldots, n$,

$$ord_2\left(\frac{\binom{2n+1}{2m+1}(-1)^{m+1}2^m}{\binom{2n+1}{5}2^2}\right) = m - 1 + ord_2\left(\binom{2n-4}{2m-4}\right) - ord_2(m(m-1))$$
$$> ord_2\left(\binom{2n-4}{2m-4}\right) \geq 0.$$

Then we obtain

$$ord_2\left(\binom{2n+1}{2m+1}(-1)^{m+1}2^m\right) > ord_2\left(-\binom{2n+1}{5}2^2\right)$$
$$\geq ord_2\left(\binom{2n+1}{3}2\right) = ord_2(-2n).$$

On the other hand,

$$ord_2\left(\binom{2n+1}{3}2 - 2n\right) = ord_2(8n(n-1)) > ord_2(2n(n-1)) = ord_2\left(-\binom{2n+1}{5}2^2\right).$$

Then by Lemma 2.1, the equation is impossible. Thus the proof of Lemma 2.3 is finished.

Proposition 2.1 *The only pairs of natural numbers* (x, y) *such that* $3^x - 2^y$ *is a perfect square are* $(0,0)$, $(1,1)$, $(2,3)$, $(3,1)$, $(4,5)$.

Proof: Let

$$3^x - 2^y = z^2 \tag{2.1}$$

Clearly, if $x < 5$, then the integer solutions are $(x, y, z) = (0,0,0)$, $(1,1,1)$, $(2,3,1)$, $(3,1,5)$, $(4,5,7)$. We will prove that there are no solution in natural numbers for any $x \geq 5$.

If (x, y, z) is a solution of the equation 2.1, then

$$-2^y \equiv z^2 \pmod 3.$$

So y is odd. If $y = 1$, then $3^x - 2 = z^2$. Clearly, x is odd, otherwise $z^2 \equiv -1 \pmod 4$, which is impossible. In the ring of integers $\mathbb{Z}[\sqrt{-2}]$, we have

$$3^x = (z - \sqrt{-2})(z + \sqrt{-2}).$$

$n - \sqrt{-2}$ and $n + \sqrt{-2}$ is coprime in $\mathbb{Z}[\sqrt{-2}]$. Otherwise, let $d = gcd(n - \sqrt{-2}, n + \sqrt{-2})$. Then $|N(d)| > 1$ and $d|2\sqrt{-2}$, so $N(d)|8$, which impossible since $N(d)|9$. We have $3 = (1 - \sqrt{-2})(1 + \sqrt{-2})$, so we have $n - \sqrt{-2} = \pm(1 - \sqrt{-2})^x$ or $n - \sqrt{-2} = \pm(1 + \sqrt{-2})^x$. Consider the imaginary part of equation $n - \sqrt{-2} = (1 - \sqrt{-2})^x$ or $n + \sqrt{-2} = (1 + \sqrt{-2})^x$. We obtain

$$-1 = \sum_{k=1, k\, odd}^{x} \binom{x}{k} (-1)^{\frac{k+1}{2}} 2^{\frac{k-1}{2}}.$$

This is impossible by Lemma 2.3. Then we have $y \geq 2$. Hence $3^x \equiv z^2 \pmod 4$. So x is even. Therefore, equation 2.1 becomes $(3^{\frac{x}{2}} - z)(3^{\frac{x}{2}} + z) = 2^y$. It follows that $gcd(3^{\frac{x}{2}} - z, 3^{\frac{x}{2}} + z) = gcd(3^{\frac{x}{2}} - z, 2 \cdot 3^{\frac{x}{2}}) = 2$. Thus, $3^{\frac{x}{2}} - z = 2$, and $3^{\frac{x}{2}} - z = 2^{y-1}$. So we get

$$3^{\frac{x}{2}} - 2^{y-2} = 1.$$

By Catalan's conjecture, the only positive integer solution of this equation is $(x, y) = (4,5)$, contradiction. Thus the proof of Proposition 2.1 is finished.

Let α be an algebraic number with minimal polynomial

$$f(x) = a_0 x^d + a_1 x^{d-1} + \cdots + x_d \in \mathbb{Z}[x],$$

where $a_0 > 0$. Then we can write $f(x) = a_0 \prod_{i=1}^{d} (x - \sigma_i \alpha)$, where $\sigma_1 \alpha$, $\cdots$, $\sigma_d \alpha$ are all conjugates of α. Let

$$h(\alpha) = \frac{1}{d}\big(\log a_0 + \sum_{i=1}^{d} \log max\{1, |\sigma_i \alpha|\}\big)$$

be the absolute logarithmic height of α.

Lemma 2.4 (See [1]) Denote by $\alpha_1, \alpha_2, \ldots, \alpha_n$ algebraic numbers, not 0 or 1, by $\log\alpha_1, \log\alpha_2, \ldots, \log\alpha_n$ determinations of their logarithms, by D the degree over $\mathbb{Q}$ of the number field $\mathbb{K} = \mathbb{Q}(\alpha_1, \alpha_2, \ldots, \alpha_n)$, and by $b_1, b_2, \ldots, b_n$ rational integers. Define $B = max\{|b_1|, |b_2|, \ldots, |b_n|\}$, and $A_i = max\{Dh(\alpha_i), |\log\alpha_i|, 0.16\}$ for all $1 \leq i \leq n$, where $h(\alpha)$ denotes the absolute logarithmic height of α. Assume that the number $\Lambda = b_1\log\alpha_1 + b_2\log\alpha_2 + \ldots + b_n\log\alpha_n$ does not vanish, then

$$|\Lambda| \geq exp\{-C(n,\lambda)D^2A_1A_2\ldots A_n\log(eD)\log(eB)\},$$

where $\lambda = 1$ if $\mathbb{K} \subseteq \mathbb{R}$ and $\lambda = 2$ otherwise and

$$C(n,\lambda) = \{\frac{1}{\lambda}(\frac{en}{2})^\lambda 30^{n+3}n^{3.5}, 2^{6n+10}\}.$$

Lemma 2.5 *Let p_n denote the n-th prime. Then*
(1) $p_n \leq n\log n + n\log\log n$ *for* $n \geq 6$.
(2) $p_n \geq n\log n + n(\log\log n - 1)$ *for* $n \geq 2$.

Proof: (1) was proved by J. B. Rosser and L. Schoenfeld [11] in 1962, and (2) was proved by P. Dusart [4] in 1999.

Lemma 2.6 *Let p, q be two odd primes. If (m_0, n_0) is a solution of*

$$2p^m - q^n = 1$$

with $m_0, n_0 > 0$, then $n_0 = 2^s$ for some nonnegative integer s.

Proof: Let (m_0, n_0) be a solution of $2p^m - q^n = 1$. Suppose that there exists an odd prime l dividing n_0, we have $n_0 = kl$ for some integer $k \geq 1$. Then

$$2p^{m_0} = q^{n_0} + 1 = q^{kl} + 1 = (q^k + 1)(q^{k(l-1)} - q^{k(l-2)} + \ldots + 1).$$

Hence we have

$$\frac{q^{kl}+1}{q^k+1} = q^{k(l-1)} - q^{k(l-2)} + \ldots + 1 > l. \tag{2.2}$$

and $q^k + 1 = 2p^{m_1}$, for some $1 \leq m_1 < m_0$. Therefore,

$$p^{m_0-m_1} = \frac{q^{kl}+1}{q^k+1} = \frac{(2p^{m_1}-1)^l+1}{2p^{m_1}} = \sum_{i=1}^{l}\binom{l}{i}(2p^{m_1})^{i-1}(-1)^{l-i}. \tag{2.3}$$

Modulo p in both side of the equation (2.3), we obtain

$$0 \equiv \sum_{i=1}^{l}\binom{l}{i}(2p^{m_1})^{i-1}(-1)^{l-i} \equiv l \pmod{p}.$$

This force $l = p$. Then by equation (2.2) we have $p^{m_0 - m_1} > p$.

On the other hand, modulo p^2 in both side of the equation (2.3), we have

$$p^{m_0-m_1} = \sum_{i=1}^{l} \binom{l}{i} (2p^{m_1})^{i-1}(-1)^{l-i} \equiv p \pmod{p^2}.$$

This force $p^{m_0-m_1} = p$, contradiction. So $n_0 = 2^s$ for some integer s.

Lemma 2.7 *For any fixed integer $n > 0$, the equation $2x^m - y^n = 1$ has finite solutions $(x, y, m) \in \mathbb{Z}_{>0}$ such that $x > y$ are two consecutive primes.*

3 Proof of main results

Proof of Theorem 1.1

We will proof that if p, q satisfy the condition that

$$p \equiv 3 \pmod 4,\ q \equiv 1 \pmod 4 \tag{3.1}$$

then $p^x - q^y = z^2$ has no nontrivial integer solution. Otherwise, let (x, y, z) is a solution. Then $p^x - q^y \equiv 0 \pmod 4$, so $2|x$. Therefore, the equation becomes

$$(p^{\frac{x}{2}} - z)(p^{\frac{x}{2}} + z) = q^y.$$

It follows that $p^{\frac{x}{2}} - z = 1$ and $p^{\frac{x}{2}} + z = q^y$, since $gcd(p^{\frac{x}{2}} - z, p^{\frac{x}{2}} + z) = 1$. So we get

$$2 \cdot p^{\frac{x}{2}} = 1 + q^y.$$

In the other hand, Modulo p in the equation, we obtain $-q^y \equiv z^2 \pmod p$. So y must be odd, since $(\frac{-1}{p}) = -1$. Hence we have

$$2 \cdot p^{\frac{x}{2}} = 1 + q^y = (1 + q)(q^{y-1} - q^{y-2} + \ldots + 1),$$

so $2p|(1 + q)$, it is contradict with $p > q$.

At last, there are infinitely many consecutive primes p and q ($p > q$) that satisfy the condition 3.1. This completes the proof of Theorem 1.1.

Proof of Theorem 1.2

By Proposition 2.1, we see that there are 3 solutions when $(p, q) = (3, 2)$. In the following, we suppose that $q > 2$. Assume the assertion is false, that is, that there exists two different non-trivial solutions (x_1, y_1), (x_2, y_2) such that $x_2 > x_1 \geq 1$. Then

$$\begin{cases} p^{2x_1} - q^{y_1} = z_1^2, \\ p^{2x_2} - q^{y_2} = z_2^2. \end{cases}$$

So we obtain
$$(p^{x_1} - z_1)(p^{x_1} - z_1) = q^{y_1}.$$
It follows that $p^{x_1} - z_1 = q^a$ and $p^{x_1} + z_1 = q^b$, where $a, b \in \mathbb{N}$ and $a + b = y_1$. Thus $gcd(p^{x_1} - z_1, p^{x_1} + z_1) = q^a$. Hence $q^a \mid 2p^{x_1}$. So we get $a = 0$ because $q > 2$. Then we obtain
$$2p^{x_1} - q^{y_1} = 1.$$
Similarly, we have
$$2p^{x_2} - q^{y_2} = 1.$$

If $p = 2$. Then we have $2^{x_i+1} - 1 = q^{y_i}, \quad i = 1, 2$. Hence, $x_1 + 1$ and $x_2 + 1$ are primes. Thus, $gcd(2^{x_1+1} - 1, 2^{x_2+1} - 1) = 2^{gcd(x_1+1, x_2+1)} - 1 = 1$, which is impossible.

If $p > 2$. Then by Lemma 2.6, we obtain that there exist an integer $s > 0$ such that $y_2 = 2^s y_1$. Thus
$$2p^{x_2} = 1 + q^{y_2} = 1 + (2p^{x_1} - 1)^{2^s}.$$
Modulo p in both side of this equation, we have $0 \equiv 2 \pmod{p}$, a contradiction. This completes the proof of Theorem 1.2.

Proof of Theorem 1.3

Let $p > q$ be two consecutive primes that bigger than 2. Then by the proof of Theorem 1.2, we have $p^{2m} - q^n = z^2$ is equal to $2p^m - q^n = 1$. Hence, it is enough to prove that the equation
$$2x^m - y^n = 1 \tag{3.2}$$
only have finite solutions (x, y, m, n) in natural number such that $x > y$ be two consecutive primes.

By Lemma 2.7, the equation (3.2) only have finite solutions for $n < 16$. Hence we consider the case $n \geq 16$. Let p_k be the k-th prime, m, n positive integers, and let
$$S_0 = \{(p_{k+1}, p_k, m, n) \mid 2p_{k+1}^m - p_k^n = 1,\ n \geq 16\}.$$
We shall show that the set S_0 finite. Set
$$S_1 = \{(p_{k+1}, p_k, m, n) \mid k + 1 > e^{n^{3/4}}\},$$
$$S_2 = \{(p_{k+1}, p_k, m, n) \mid k + 1 < e^{n^{3/4}}\}.$$
Then it's enough to prove that the sets $S_0 \cap S_1$ and $S_0 \cap S_2$ are all finite.

Let $(p_{k+1}, p_k, m, n) \in S_0 \cap S_1$. Then we have $p_{k+1} > p_k \geq k+1 > e^{n^{3/4}}$. For $n \geq 16$, by Lemma 2.5, we have

$$\begin{aligned}\varepsilon &= \frac{p_{k+1} - p_k}{p_k} \\ &< \frac{(k+1)\log(k+1) + (k+1)\log\log(k+1) - k\log - k(\log\log k - 1)}{p_k} \\ &< \frac{2\log(k+1) + k + 3}{p_k} \\ &< \frac{2k}{p_k} < \frac{2}{\log k} \leq \frac{1}{\sqrt{n}}.\end{aligned}$$

Then we get $1 = p^m(2(1+\varepsilon)^m - p_k^{n-m})$. So for $n > 7$,

$$p_k \leq p_k^{n-m} < 2(1+\varepsilon)^m < 2(1+\frac{1}{\sqrt{n}})^n < 2e^{n^{1/2}} < \frac{1}{2}e^{n^{3/4}} < \frac{1}{2}p_{k+1}.$$

which is impossible. Hence, we obtain $S_0 \cap S_1 = \emptyset$.

Let $(p_{k+1}, p_k, m, n) \in S_0 \cap S_2$. We consider the linear form

$$\Lambda = m\log p_{k+1} - n\log p_k + \log 2.$$

Then we have $\Lambda < e^{\Lambda} - 1 = \frac{1}{p_k^n}$. So $\log\Lambda < -n\log p_k$. Now we apply Lemma 2.4 with $D = 1$, $\alpha_1 = p_{k+1}$, $\alpha_2 = p_k$ and $\alpha_3 = 2$. Therefore, we take $A_1 = \log p_{k+1}$, $A_2 = \log p_k$, $A_3 = 2$, $B = n$. So we have

$$\log\Lambda > -9.65 \cdot 10^{10} \log p_{k+1} \log p_k \log(en).$$

Therefore we have

$$\frac{n}{\log p_{k+1}\log(en)} < 9.65 \cdot 10^{10}.$$

On the other hand, from $k+1 < e^{n^{3/4}}$, we have for $n > 4$,

$$p_{k+1} < 2(k+1)log(k+1) = 2e^{n^{3/4}} \cdot n^{3/4} < e^{n^{4/5}}.$$

So we obtain

$$n < 7 \cdot 10^{65}.$$

Then by Lemma 2.7, we have $S_0 \cap S_2$ is finite.

This complete the proof of Theorem 1.3.

References

[1] M.A. Bennett, On some exponential equations of S. S. Pillai, *Canad. J. Math.*, **53** (2001), 897-922. https://doi.org/10.4153/cjm-2001-036-6

[2] A. Bérczes, I. Pink, On the Diophantine equation $x^2 + p^{2k} = y^n$, *Arch. Math.*, **91** (2008), 505-517. https://doi.org/10.1007/s00013-008-2847-x

[3] Z.F. Cao, On the equation $ax^m - by^n = 2$, *Kexue Tongbao*, **35** (1990), 558-559.

[4] P. Dusart, The kth prime is greater than $k(lnk + lnlnk - 1)$ for $k \geq 2$, *Mathematics of Computation*, **68** (1999), 411-415. https://doi.org/10.1090/S0025-5718-99-01037-6

[5] B. He, A. Togbé, On the number of solutions of the diophantine equation $ax^m - by^n = c$, *Bull. Aust. Math. Soc.*, **81** (2010), 177-185. https://doi.org/10.1017/S0004972709001002

[6] M.H. Le, A note on the diophantine equation $ax^m - by^n = k$, *Indag. Math.*, **3** (1992), 185-191. https://doi.org/10.1016/0019-3577(92)90007-8

[7] M.H. Le, On Cohn's conjecture concerning the Diophantine equation $x^2 + 2^m = y^n$, *Archiv der Mathematik*, **78** (2002), 26-35. https://doi.org/10.1007/s00013-002-8213-5

[8] W.J. LeVeque, On the equation $a^x - b^y = 1$, *Amer. J. Math.*, **74** (1952), 325-331. https://doi.org/10.2307/2371997

[9] P. Mihăilescu, A class number free criterion for Catalan's conjecture, *J. Number Theory*, **99** (2003), 225-231. https://doi.org/10.1016/s0022-314x(02)00101-4

[10] P. Mihăilescu, Primary cyclotomic units and a proof of Catalan's conjecture, *J. Reine Angew. Math.*, **572** (2004), 167-195. https://doi.org/10.1515/crll.2004.048

[11] J.B. Rosser and L. Schoenfeld, Approximate formulas for some functions of prime numbers, *Illinois J. Math.*, **6** (1962), 64-94.

[12] J.P. Serre, *Local Fields*, Graduate Texts in Mathematics, Vol. 67, Springer-Verlag, New York-Berlin, 1979. https://doi.org/10.1007/978-1-4757-5673-9

[13] A. Ventullo, Difference of powers of consecutive primes which are perfect squares, (2016). https://arxiv.org/abs/1604.05334v1

Received: February 27, 2017; Published: April 8, 2017