Bull. Math. Soc. Sci. Math. Roumanie
Tome 57(105) No. 3, 2014, 337–344

The Exponential Diophantine Equation $((2^{2m}-1)n)^x + (2^{m+1}n)^y = ((2^{2m}+1)n)^z$

by
[1]Zhang Xinwen and [2]Zhang Wenpeng

Abstract

Let $m,\ n$ be positive integers. Let (a,b,c) be a primitive Pythagorean triplet with $a^2+b^2=c^2$. In 1956, L. Jeśmanowicz conjectured that the equation $(an)^x+(bn)^y=(cn)^z$ has only the positive integer solution $(x,y,z)=(2,2,2)$. In this paper, using certain elementary methods, we prove that if $(a,b,c)=(2^{2m}-1,2^{m+1},2^{2m}+1)$, then the above equation has only the positive integer solution $(x,y,z)=(2,2,2)$. Thus it can be seen that Jeśmanowicz's conjecture is true for infinitely many primitive Pythagorean triplets.

Key Words: Exponential diophantine equation, primitive Pythagorean triplet, Jeśmanowicz's conjecture.
2010 Mathematics Subject Classification: Primary 11D20, Secondary 11D61.

1 Introduction

Let $\mathbb{Z},\mathbb{N}$ be the sets of all integers and positive integers respectively. Let $m,\ n$ be positive integers. Let $(a,\ b,\ c)$ be a primitive Pythagorean triplet such that

$$a^2+b^2=c^2,\ a,b,c\in\mathbb{N},\ \gcd(a,b,c)=1,\ 2|b. \tag{1.1}$$

Then we have

$$a=u^2-v^2,\ b=2uv,\ c=u^2+v^2,\ u,v\in\mathbb{N},$$
$$u>v,\ \gcd(u,v)=1,\ 2|uv. \tag{1.2}$$

In 1956, L. Jeśmanowicz[2] conjectured that the equation

$$(an)^x+(bn)^y=(cn)^z,\ x,y,z\in\mathbb{N} \tag{1.3}$$

has only the solution $(x,y,z)=(2,2,2)$ for any n.
This conjecture has been proved to be true in many special cases (see [7] and its references). But, in general, the problem is not solved as yet.

Most of the results concerning the above conjecture deal with the case that $n = 1$, and very little is known about (1.3) for $n > 1$. In this paper, we discuss the case that

$$u = 2^m,\ v = 1. \tag{1.4}$$

Substituting (1.4) into (1.2), we have

$$a = 2^{2m} - 1,\ b = 2^{m+1},\ c = 2^{2m} + 1, \tag{1.5}$$

and by (1.5), the equation (1.3) can be written as

$$((2^{2m} - 1)n)^x + (2^{m+1}n)^y = ((2^{2m} + 1)n)^z,\ x, y, z \in \mathbb{N}. \tag{1.6}$$

In this connection, by an early result of W. -T. Lu[5], (1.6) has only the solution $(x, y, z) = (2, 2, 2)$ for $n = 1$. In 1998, M. -J. Deng and G. L. Cohen[1] showed that if $m = 1$, then (1.6) has only the solution $(x, y, z) = (2, 2, 2)$ for $n > 1$. Recently, Z. -J. Yang and M. Tang[10] proved a similar result for $m = 2$. In this paper, using certain elementary methods, we prove a general result as follows.

Theorem 1. *For any positive integers m and n, (1.6) has only the solution $(x, y, z) = (2, 2, 2)$.*

Thus it can be seen that Jeśmanowicz's conjecture is true for infinitely many primitive Pythagorean triplets.

2 Preliminaries

Let k be a positive integer, and let $P(k)$ denote the product of all distinct prime divisors of k. Further let $P(1) = 1$.

Lemma 2.1.[6] Let t be a positive integer. If $2^t \equiv 1 \pmod{2^k - 1}$, then $k|t$.

Lemma 2.2. Every solution (X, Y, Z) of the equation

$$X^2 + Y^2 = Z^k,\ X, Y, Z \in \mathbb{N},\ \gcd(X, Y) = 1,\ 2|Y \tag{2.1}$$

can be expressed as

$$Z = A^2 + B^2,\ A, B \in \mathbb{N},\ \gcd(A, B) = 1,\ 2|B \tag{2.2}$$

and

$$X + Y\sqrt{-1} = \lambda_1(A + \lambda_2 B\sqrt{-1})^k,\ \lambda_1, \lambda_2 \in \{\pm 1\}. \tag{2.3}$$

Moreover, if $2^r||Y,\ 2^s||k$ and $2^t||B$, then $r > s$ and $r = s + t$.

Proof. By [8, Section 15.2], every solution (X, Y, Z) of (2.1) can be expressed as (2.2) and (2.3). Further, by (2.3), we have

$$Y = \lambda_1\lambda_2 B \sum_{i=0}^{[(k-1)/2]} \binom{k}{2i+1} A^{k-2i-1}(-B^2)^i, \tag{2.4}$$

where $[(k-1)/2]$ is the integral part of $(k-1)/2$.

By (2.2), we have $2 \nmid A$,

$$2^{s+t} \parallel \lambda_1\lambda_2 \binom{k}{1} A^{k-1}B \tag{2.5}$$

and

$$2^{s+3t} \mid (-1)^i\lambda_1\lambda_2 \binom{k}{2i+1} A^{k-2i-1}B^{2i+1}$$
$$= (-1)^i\lambda_1\lambda_2 k \binom{k-1}{2i} \frac{A^{k-2i-1}B^{2i+1}}{2i+1},\ i \geq 1. \tag{2.6}$$

Therefore, by (2.5) and (2.6), we get

$$2^{s+t} \parallel \lambda_1\lambda_2 B \sum_{i=0}^{[(k-1)/2]} \binom{k}{2i+1} A^{k-2i-1}(-B^2)^i. \tag{2.7}$$

Since $2|B$, we see from (2.4) and (2.7) that $r > s$ and $r = s+t$. The lemma is proved.

Lemma 2.3. Every solution (X, Y, Z) of the equation

$$X^2 + 2Y^2 = Z^k,\ X, Y, Z \in \mathbb{N},\ \gcd(X, Y) = 1 \tag{2.8}$$

can be expressed as

$$Z = A^2 + 2B^2,\ A, B \in \mathbb{N},\ \gcd(A, B) = 1,\ 2 \nmid A \tag{2.9}$$

and

$$X + Y\sqrt{-2} = \lambda_1(A + \lambda_2 B\sqrt{-2})^k,\ \lambda_1, \lambda_2 \in \{\pm 1\}. \tag{2.10}$$

Moreover, if $2^r \parallel Y$, $2^s \parallel k$ and $2^t \parallel B$, then $r \geq s$ and $r = s+t$.

Proof. Notice that $h(-8) = 1$, where $h(-8)$ is the class number of primitive binary quadratic forms of discriminant -8. Therefore, by [3, Theorems 1 and 2], every solution (X, Y, Z) of (2.8) can be expressed as (2.9) and (2.10). Further, by (2.10), we have

$$Y = \lambda_1\lambda_2 B \sum_{i=0}^{[(k-1)/2]} \binom{k}{2i+1} A^{k-2i-1}(-2B^2)^i. \tag{2.11}$$

Thus, using the same method as in the proof of Lemma 2.2, we can get from (2.11) that $r \geq s$ and $r = s+t$. The lemma is proved.

Lemma 2.4.[9] If $k \geq 3$, then the equation

$$X^k + Y^k = Z^k,\ X, Y, Z \in \mathbb{N} \tag{2.12}$$

has no solution (X, Y, Z).

Lemma 2.5.[4] If $n > 1$ and (x, y, z) is a solution of (1.3) with $(x, y, z) \neq (2, 2, 2)$, then one of the following conditions is satisfied:

(i) $\max\{x, y\} > \min\{x, y\} > z$, $P(n) \mid c$ and $P(n) < P(c)$.

(ii) $x > z > y$ and $P(n) \mid b$.

(iii) $y > z > x$ and $P(n) \mid a$.

3 Proof of Theorem

By the results of [1], [5] and [10], it suffices to prove the theorem for $m \geq 3$ and $n > 1$. We now assume that (x, y, z) is a solution of (1.6) with $(x, y, z) \neq (2, 2, 2)$. By Lemma 2.5, we only need to examine the following four cases:

Case I. $x > y > z$, $P(n) \mid 2^{2m} + 1$ and $P(n) < P(2^{2m} + 1)$.

Under these assumptions, by (1.6), we get

$$2^{2m} + 1 = c_1 c_2,\ c_1, c_2 \in \mathbb{N},\ \gcd(c_1, c_2) = 1,\ c_2 > 1, \tag{3.1}$$

$$n^{y-z} = c_1^z,\ c_1 > 1 \tag{3.2}$$

and

$$\left(2^{2m} - 1\right)^x n^{x-y} + 2^{(m+1)y} = c_2^z. \tag{3.3}$$

Since $c_1 > 1$ and every prime divisor p of $2^{2m} + 1$ satisfies $p \equiv 1(\bmod 4)$, we have $c_1 \geq 5$ and $c_2 \leq (2^{2m} + 1)/5$ by (3.1). Therefore, by (3.3), we get

$$\left(\frac{2^{2m} + 1}{5}\right)^z \geq c_2^z > \left(2^{2m} - 1\right)^x > \left(\frac{2^{2m} + 1}{2}\right)^x > \left(\frac{2^{2m} + 1}{2}\right)^z, \tag{3.4}$$

a contradiction.

Case II. $y > x > z$, $P(n) \mid 2^{2m} + 1$ and $P(n) < P(2^{2m} + 1)$.

Using the same method as in the proof of Case I, we can exclude this case immediately.

Case III. $x > z > y$ and $P(n) \mid b$.

Since $n > 1$, we get from (1.6) that $P(n) = 2$,

$$n^{z-y} = 2^{(m+1)y} \tag{3.5}$$

and

$$(2^{2m} - 1)^x n^{x-z} + 1 = (2^{2m} + 1)^z. \tag{3.6}$$

By (3.5), we have

$$n = 2^r,\ r \in \mathbb{N} \tag{3.7}$$

and

$$r(z - y) = (m + 1)y. \tag{3.8}$$

Substituting (3.7) into (3.6), we get

$$(2^{2m} - 1)^x \cdot 2^{r(x-z)} + 1 = (2^{2m} + 1)^z. \tag{3.9}$$

Since $2^{2m} + 1 \equiv 2(\bmod 2^{2m} - 1)$, we see from (3.9) that

$$2^z \equiv 1(\bmod 2^{2m} - 1). \tag{3.10}$$

Applying Lemma 2.1 to (3.10), we obtain $2m \mid z$ and therefore

$$z = 2mk,\ k \in \mathbb{N}. \tag{3.11}$$

If $2 \mid k$, then $(2^{2m}+1)^{mk} \equiv 2^{mk} \equiv 1 (\bmod\ 2^{2m}-1)$ and $\gcd((2^{2m}+1)^{mk}+1, (2^{2m}+1)^{mk}-1) = 1$. Hence, by (3.9) and (3.11), we get

$$\left(2^{2m}+1\right)^{mk}-1 = 2^{r(x-z)-1}\left(2^{2m}-1\right)^{x},\ (2^{2m}+1)^{mk}+1 = 2, \tag{3.12}$$

a contradiction.

If $2 \nmid k$, then $(2^{2m}+1)^{mk} \equiv 2^{mk} \equiv 1 (\bmod\ 2^{m}-1)$ and $(2^{2m}+1)^{mk} \equiv 2^{mk} \equiv -1 (\bmod\ 2^{m}+1)$. Hence, by (3.9) and (3.11), we get

$$(2^{2m}+1)^{mk}+1 = 2(2^{m}+1)^{x} \tag{3.13}$$

and

$$(2^{2m}+1)^{mk}-1 = 2^{r(x-z)-1}(2^{m}-1)^{x}, \tag{3.14}$$

whence we obtain

$$(2^{m}+1)^{x} - 2^{r(x-z)-2}(2^{m}-1)^{x} = 1. \tag{3.15}$$

Since $2^{m}+1 \equiv 2 (\bmod\ 2^{m}-1)$, we see from (3.15) that $2^{x} \equiv 1 (\bmod\ 2^{m}-1)$. It results that $m \mid x$, that is

$$x = ml,\ l \in \mathbb{N}. \tag{3.16}$$

Therefore, by (3.9), (3.11) and (3.16), we get

$$\left((2^{2m}-1)^{l} \cdot 2^{r(l-2k)}\right)^{m} + 1^{m} = \left((2^{2m}+1)^{2k}\right)^{m}. \tag{3.17}$$

But, since $m \geq 3$, by Lemma 2.4, (3.17) is impossible.

Case IV. $y > z > x$ and $P(n) \mid 2^{2m}-1$.

Then we have

$$2^{2m}-1 = a_1 a_2,\ a_1, a_2 \in \mathbb{N},\ \gcd(a_1, a_2) = 1, \tag{3.18}$$

$$n^{z-x} = a_1^{x},\ a_1 > 1 \tag{3.19}$$

and

$$a_2^{x} + 2^{(m+1)y} n^{y-z} = (2^{2m}+1)^{z}. \tag{3.20}$$

Let

$$x = 2^{\alpha} x_1,\ z = 2^{\beta} z_1,\ \alpha, \beta \in \mathbb{Z},\ \alpha \geq 0,\ \beta \geq 0,$$
$$x_1, z_1 \in \mathbb{N},\ 2 \nmid x_1 z_1. \tag{3.21}$$

If $a_2 = 1$, then from (3.20) we get

$$2^{(m+1)y} n^{y-z} = (2^{2m}+1)^{z} - 1 = \sum_{i=1}^{z} \binom{z}{i} 2^{2mi}. \tag{3.22}$$

Using the same method as in the proof of Lemma 2.2, we get

$$2^{2m+\beta} \,||\, \sum_{i=1}^{z} \binom{z}{i} 2^{2mi}. \tag{3.23}$$

Hence, by (3.22) and (3.23), we get

$$(m+1)y = 2m + \beta. \tag{3.24}$$

But, since $y > z > x$ and $y \geq 3$, by (3.21) and (3.24), we get

$$y > z \geq 2^{\beta} = 2^{(m+1)y-2m} = 2^{(y-2)m+y} > 2^{y}, \tag{3.25}$$

a contradiction. So we have $a_2 > 1$.

By (3.20) and (3.23), we get

$$a_2^{x} \equiv 1 (\bmod 2^{2m+\beta}). \tag{3.26}$$

Further, by (3.21) and (3.26), we have

$$a_2 \equiv \lambda (\bmod 2^{2m+\beta-\alpha}), \tag{3.27}$$

where $\lambda = (-1)^{(a_2-1)/2}$. Since $a_2 > 1$, we have $a_2 + 1 \geq a_2 - \lambda > 0$. Hence, by (3.27), we get

$$a_2 \geq 2^{2m+\beta-\alpha} - 1. \tag{3.28}$$

On the other hand, we see from (3.18) and (3.19) that $a_2 = (2^{2m} - 1)/a_1 < 2^{2m} - 1$. Therefore, by (3.28), we get

$$\alpha > \beta. \tag{3.29}$$

Further, by (3.21) and (3.29), $x/2^{\beta}$ is even and $(z-x)/2^{\beta}$ is odd. Thus, we find from (3.19) that n must be a square, namely,

$$n = l^2,\ l \in \mathbb{N},\ l > 1,\ 2 \nmid l. \tag{3.30}$$

Substituting (3.30) into (3.20), we get

$$(a_2^{x/2})^2 + 2^{(m+1)y}(l^{y-z})^2 = (2^{2m}+1)^z. \tag{3.31}$$

If $2 \mid (m+1)y$, then, by (3.31), (2.1) has the solution

$$(X, Y, Z, k) = (a_2^{x/2}, 2^{(m+1)y/2} l^{y-z}, 2^{2m}+1, z). \tag{3.32}$$

Applying Lemma 2.2 to (3.32), we have

$$2^{2m} + 1 = A^2 + B^2,\ A, B \in \mathbb{N},\ \gcd(A, B) = 1,\ 2 \mid B \tag{3.33}$$

and

$$2^{(m+1)y/2-\beta} \mid B. \tag{3.34}$$

By (3.33) and (3.34), we get

$$2^{m} \geq B \geq 2^{(m+1)y/2-\beta}, \tag{3.35}$$

whence we obtain

$$\beta \geq \frac{1}{2}\left((y-2)m + y\right). \tag{3.36}$$

Since $m \geq 3$ and $y \geq 3$, we see from (3.21) and (3.36) that $\beta \geq 3,\ y > z \geq 2^{\beta} \geq 8$ and

$$y > z \geq 2^{\beta} \geq 2^{((y-2)m+y)/2} \geq 2^{2y-3}, \tag{3.37}$$

a contradiction.

If $2 \nmid (m+1)y$, then, by (3.31), (2.8) has the solution

$$(X, Y, Z, k) = (a_2^{x/2}, 2^{((m+1)y-1)/2} l^{y-z}, 2^{2m} + 1, z). \tag{3.38}$$

Applying Lemma 2.3 to (3.38), we have

$$2^{2m} + 1 = A^2 + 2B^2,\ A, B \in \mathbb{N},\ \gcd(A, B) = 1,\ 2 \nmid A \tag{3.39}$$

and

$$2^{((m+1)y-1)/2-\beta} \mid B. \tag{3.40}$$

Therefore, by (3.39) and (3.40), we get $2^{2m} \geq 2B^2$ and (3.36) holds too. Thus, we can deduce a contradiction as (3.37).

To sum up, the theorem is proved.

Acknowledgement: *Research partially supported by the N. S. F. (11071194) of P.R.China. The authors would like to thank the referee for his very helpful and detailed comments, which have significantly improved the presentation of this paper.*

References

[1] M. -J. Deng and G. L. Cohen, On the conjecture of Jeśmanowicz concerning Pythagorean triples, *Bull. Austral. Math. Soc.*, **57** (1998), 515–524.

[2] L. Jeśmanowicz, Several remarks on Pythagorean numbers, *Wiadom. Mat.*, **1** (1955/56), 196–202. (in Polish)

[3] M. -H. Le, Some exponential diophantine equations I: The equation $D_1x^2 - D_2y^2 = \lambda k^z$, *J. Number Theory*, **55** (1995), 209–221.

[4] M.-H. Le, A note on Jeśmanowicz' conjecture concerning Pythagorean triples, *Bull. Austral. Math. Soc.*, **59** (1999), 477–480.

[5] W. -T. Lu, On the Pythagorean numbers $4n^2 - 1$, $4n$ and $4n^2 + 1$, *J. Sichuan Univ. Natur. Sci.*, **2** (1959), 39–42. (in Chinese)

[6] E. Lucas, Théorie des functions numériques simplement périodiques, *Amer. J. Math.*, **1** (1878), 184–240.

[7] T. Miyazaki, Jeśmanowicz' conjecture on exponential diophantine equations, *Funct. Approximatio Comment. Math.*, **45** (2011), 207–229.

[8] L. J. Mordell, *Diophantine equations*, London: Academic Press, 1969.

[9] A. Wiles, Modular elliptic curves and Fermat last theorem, *Ann. of Math.*, **141** (1995), 443–551.

[10] Z. -J. Yang and M. Tang, On the diophantine equation $(8n)^x + (15n)^y = (17n)^z$, *Bull. Austral. Math. Soc.*, **86** (2012), 348–352.

Received: 10.05.2013
Revised: 22.07.2013
Accepted: 01.08.2013

[1]Department of Mathematics,
Northwest University,
Xi'an, Shaanxi, P. R. China. E-mail: news_zhang@163.com

[2]Department of Mathematics,
Northwest University,
Xi'an, Shaanxi, P. R. China. E-mail: wpzhang@nwu.edu.cn