An Elementary Proof of a Result Ma and Chen

Qing Han[1], Pingzhi Yuan[2]

[1]School of Information Science and Technology, South China Business College of Guangdong University of Foreign Studies, Guangzhou, China

[2]School of Mathematics, South China Normal University, Guangzhou, China

Email address:

46620467@qq.com (Qing Han), yuanpz@scnu.edu.cn (Pingzhi Yuan)

Abstract: In 1956, Jeśmanowicz conjectured that, for positive integers m and n with $m > n$, $\gcd(m, n) = 1$ and $m \not\equiv n$ (mod 2), the exponential Diophantine equation $(m^2 - n^2)^x + (2mn)^y = (m^2 + n^2)^z$ has only the positive integer solution $(x, y, z) = (2, 2, 2)$. Recently, Ma and Chen proved the conjecture if $4 \nmid mn$ and $y \geq 2$. In this paper, we provide a proposition that, for positive integers m and n with $m > n$, $\gcd(m, n) = 1$ and $m^2 + n^2 \equiv 5 \pmod 8$, the exponential Diophantine equation $(m^2 - n^2)^x + (2mn)^y = (m^2 + n^2)^z$ has only the positive integer solution $x = y = z = 2$ with $2 | \gcd(x, y)$. Then we present an elementary and simple proof of the result of Ma and Chen by using Jacobi's symbols.

Keywords: Pythagorean Triple, Jeśmanowicz Conjecture, Exponential Diophantine Equations

1. Introduction

Let a, b and c be positive integers satisfying $a^2 + b^2 = c^2$. Such a triple (a, b, c) is called a *Pythagorean triple*. If $\gcd(a, b, c) = 1$, this triple is called *primitive*. It is well-known that a primitive Pythagorean triple (a, b, c) can be parameterized by

$$a = m^2 - n^2, \quad b = 2mn, \quad c = m^2 + n^2,$$

where m and n are relatively prime positive integers with $m > n$ and $m \not\equiv n \pmod 2$. In 1956, Jeśmanowicz [8] proposed the following problem:

Conjecture 1.1

The exponential Diophantine equation

$$(m^2 - n^2)^x + (2mn)^y = (m^2 + n^2)^z \qquad (1)$$

has only one positive integer solution $(x, y, z) = (2, 2, 2)$.

Using elementary methods, Le [9] showed that if $mn \equiv 2 \pmod 4$ and $m^2 + n^2$ is a power of a prime, then Conjecture 1.1 is true. Guo, Le [6] applied the theory of linear forms in two logarithms to prove that if $n = 3$, $m \equiv 2 \pmod 4$ and $m > 6000$, then Conjecture 1.1 is true. Takakuwa

[20] extended the result of Guo, Le [6] by proving that if $n = 3, 7, 11, 15$ and $m \equiv 2 \pmod 4$, then Conjecture 1.1 is true. Cao [1] also showed that if $m \equiv 5 \pmod 8$ and $n \equiv 2 \pmod 8$, then Conjecture 1.1 is true. In 2014, Terai [23] showed that if $n = 2$, then Conjecture 1.1 is true without any assumption on m. In 2015, Miyazaki and Terai [17] proved some further results.

Recently, Ma and Chen [11] proved the following proposition.

Proposition 1.1

Suppose that $4 \nmid mn$. Then the equation

$$(m^2 - n^2)^x + (2mn)^y = (m^2 + n^2)^z, \quad y \geq 2,$$

has only the positive integer solution $(x, y, z) = (2, 2, 2)$.

Deng and Huang[2], Deng and Guo [3] proved some theorems for $2 \| mn$ by using biquadratic character theory and an elementary method. For more results on the conjecture, see [4, 5, 10, 7, 12, 13, 14, 15, 16, 18, 21, 22, 24, 25].

For the proof of the above Proposition 1.1, Ma and Chen [11] used some complicated computations of Jacobi's symbols and a known result of Miyazaki ([13] Theorem 1.5), which is based on deep results on generalized Fermat equations via sophisticated arguments in the theory of elliptic curves and

modular forms. We also note that the proof of the main result in Terai [23] used the same known result of Miyazaki ([13] Theorem 1.5).

In this paper, we present an elementary proof of Proposition 1.1 by using Jacobi's symbols, however the computations of Jacobi's symbols are more involved here.

2. Some Lemmas

For more self-contained, in this section, we provide some simple lemmas which will be used in the proof of Proposition 1.1. The following two results are well-known.

Lemma 2.1

Let (u, v, w) be a primitive Pythagorean triple such that $u^2 + v^2 = w^2$, $2|v$ and $w \equiv 5 \pmod 8$. Then there exists coprime positive integers s and t with $s > t$, $2||st$ and

$$u = s^2 - t^2, \quad v = 2st, \quad w = s^2 + t^2.$$

proof

The others being obvious, only $2||st$ needs a proof, this follows from the condition $w \equiv 5 \pmod 8$.

The equation $x^4 - y^4 = z^2$ has no nonzero integer solutions.

For the proof of the above Lemma, we refer to Mordell [19].

Let m, n be coprime positive integers with $m^2 + n^2 \equiv 5 \pmod 8$ and $m > n$, then the Diophantine equation

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

has only the positive integer solution $x = y = z = 2$ with $2|\gcd(x, y)$.

Let (x, y, z) be a positive integer solution of (2) with $2|\gcd(x, y)$ and $(x, y, z) \neq (2, 2, 2)$. Since $m^2 + n^2 \equiv 5 \pmod 8$ and $(m^2 + n^2)^z = (m^2 - n^2)^x + (2mn)^y \equiv 1 \pmod 8$, we obtain that $2|z$. Put

$$x = 2X, \quad y = 2Y, \quad z = 2Z,$$

then we have

$$(m^2 - n^2)^X = u^2 - v^2,$$
$$(2mn)^Y = 2uv, \tag{3}$$
$$(m^2 + n^2)^Z = u^2 + v^2,$$

where u, v are positive integers with $u > v$. If $Y = 1$ and $Z = 1$, then it is easy to see that $X = 1$, and we are done.

If $Y = 1$ and $Z > 1$, then we have

$$\begin{aligned}(2mn)^2 &= (m^2 + n^2)^{2Z} - (m^2 - n^2)^{2X} \\ &\geq (m^2 + n^2)^Z + (m^2 - n^2)^X \\ &> (m^2 + n^2)^Z > (2mn)^2,\end{aligned}$$

a contradiction. Finally we consider the case where $Y > 1$. If $Y > 1$ and Z is even, we have

$$m^2 + n^2 \equiv 5 \pmod 8, \quad m^2 - n^2 \equiv \pm 5 \pmod 8.$$

Considering equation (2) by taking modulo 16, we have

$$(m^2 - n^2)^{2X} \equiv 1 \pmod{16},$$

hence $2|X$, which is impossible by Lemma 2.2 since $4|x$, $4|z$ and $(m^2 + n^2)^x - (m^2 - n^2)^y = (2mn)^{2Y}$. Therefore Z is odd when $Y > 1$. Now

$$(m^2 + n^2)^Z \equiv 5 \pmod 8.$$

It follows from (3) that $(m^2 + n^2)^Z = s^2 + t^2 \equiv 5 \pmod 8$, hence $2||st$ by Lemma 2.1, which contradicts to $2st = (2mn)^Y$ and $Y > 1$. This completes the proof.

Lemma 2.3

Let (x, y, z) be a solution of (1) with $y \geq 2$. Suppose that $2||mn$. Then both x and z are even.

proof

Let (x, y, z) be a solution of (1). Since $2||mn$, so $m^2 + n^2 \equiv 5 \pmod 8$ and we have

$$\left(\frac{2mn}{m^2 + n^2}\right) = \left(\frac{(m + n)^2}{m^2 + n^2}\right) = 1,$$
$$\left(\frac{m^2 - n^2}{m^2 + n^2}\right) = \left(\frac{2m^2}{m^2 + n^2}\right) = \left(\frac{2}{m^2 + n^2}\right) = -1.$$

Taking (1) modulo $m^2 + n^2$, we have $\left(\frac{m^2 - n^2}{m^2 + n^2}\right)^x = \left(\frac{-1}{m^2 + n^2}\right)\left(\frac{2mn}{m^2 + n^2}\right)^y$, i.e. $(-1)^x = 1$, so $2|x$. In view of $y \geq 2$, (3) and $4|2mn$,

$$5^z \equiv (m^2 + n^2)^z = (m^2 - n^2)^x + (2mn)^y \equiv 1 \pmod 8.$$

It follows that z is even.

3. A Simple Proof of Proposition 1.1

In this section, we will present an elementary and simple proof of Proposition 1.1.

A simple proof of Proposition 1.1: Let (x, y, z) be a solution of (1) with $y \geq 2$. Noting that $2||mn$, by Lemma 2.3, $2|x$ and $2|z$. If $2|y$, then (1) has only the solution $(x, y, z) = (2, 2, 2)$ by Proposition 2.1. Hence we may assume that $2 \nmid m$, $2||n, n = 2n', 2 \nmid n'$ and $2 \nmid y$. Let t be the positive integer with $2^t||z$. Since $2|x$, we have

$$(4mn')^y = (m^2 + 4n'^2)^z - (m^2 - 4n'^2)^x > (m^2 + 4n'^2)^{z/2}.$$

If $t = 1$, then we have $y \geq 3$ because $2 \nmid y$ and $y > 1$. If $t > 1$, then $y \geq z/2 + 1 \geq t + 1$, and thus $2y \geq 2(t + 1) > t + 2$.

Taking modulo 2^{t+3} for (1), we get

$$\begin{aligned}(m^2 - 4n'^2)^x + 2^{2y}(mn')^y &\equiv (m^2 - 4n'^2)^x \\ &\equiv (m^2 + 4n'^2)^z \\ &\equiv 1 + 2^{t+2} \pmod{2^{t+3}},\end{aligned}$$

which yields $2^t||x$ since $m^2 - 4n'^2 \equiv \pm 5 \pmod 8$.

Let $x = 2^t X$ and $z = 2^t Z$, where X and Z are positive integers and $2 \nmid XZ$.

Case I: t is even: By (1), we have

$$(m^2 + 4n'^2)^{2^t Z} - (m^2 - 4n'^2)^{2^t X}$$
$$= \left((m^2 + 4n'^2)^Z - (m^2 - 4n'^2)^X\right)$$
$$\prod_{i=0}^{t-1} \left((m^2 + 4n'^2)^{2^i Z} + (m^2 - 4n'^2)^{2^i X}\right)$$
$$= 2^{2y}(mn')^y.$$

Since $\gcd(m, n') = 1$, it is easy to show that the greatest common divisor of any two terms in the above product is 2 and $(m^2 + 4n'^2)^Z - (m^2 - 4n'^2)^X \equiv 0 \pmod{8}$, hence we have

$$(m^2 + 4n'^2)^Z + (m^2 - 4n'^2)^X = 2(m_1 n_1)^y \qquad (4)$$

and

$$(m^2 + 4n'^2)^Z - (m^2 - 4n'^2)^X = 2^{2y-t}(m_2 n_2)^y, \qquad (5)$$

where $m_i | m$, $n_i | n'$, $i = 1, 2$ and $\gcd(m_1, m_2) = 1$, $\gcd(n_1, n_2) = 1$.

By (4) and (5), we have

$$(m^2 + 4n'^2)^Z = (m_1 n_1)^y + 2^{2y-t-1}(m_2 n_2)^y. \qquad (6)$$

In view of (6), $2y - t - 1 \geq t + 1 \geq 3$ and $2 \nmid yZ$, we have

$$m_1 n_1 \equiv (m_1 n_1)^y \equiv m^2 + n^2 \equiv 5 \pmod{8}. \qquad (7)$$

For any prime factor p of n_1, by (4),

$$m^{2Z} + n'^{2X} \equiv 0 \pmod{p},$$

it follows that $p \equiv 1 \pmod{8}$. Hence $n_1 \equiv 1 \pmod{8}$, and so $m_1 \equiv 5 \pmod{8}$ by (7). Similarly, by (5) we have $m_2 \equiv 1 \pmod{8}$.

On the other hand, since t is even, it follows from (6) that

$$\left(\frac{2m_2 n_2}{m_1}\right) = \left(\frac{n'^2}{m_1}\right) = 1, \quad \left(\frac{2m_2 n_2}{n_1}\right) = 1$$

and

$$\left(\frac{m_1 n_1}{m_2}\right) = \left(\frac{n'^2}{m_2}\right) = 1, \quad \left(\frac{m_1 n_1}{n_2}\right) = 1.$$

In view of t is even, $n_1 \equiv m_2 \equiv 1 \pmod{8}$ and $m_1 \equiv 5 \pmod{8}$, we have

$$\left(\frac{m_2 n_2}{m_1}\right) = -1, \quad \left(\frac{m_2 n_2}{n_1}\right) = 1 \qquad (8)$$

and

$$\left(\frac{m_1 n_1}{m_2}\right) = 1, \quad \left(\frac{m_1 n_1}{n_2}\right) = 1. \qquad (9)$$

Let $\left(\frac{m_2}{m_1}\right) = u$, $u \in \{-1, 1\}$, by the first equalities of (8) and (9), we have

$$\left(\frac{n_2}{m_1}\right) = -u, \quad \left(\frac{n_1}{m_2}\right) = u. \qquad (10)$$

Now, by the second equalities of (8) and (10), we get

$$\left(\frac{n_2}{n_1}\right) = u. \qquad (11)$$

By the first equality of (10) and the second equality of (9), we have

$$\left(\frac{n_2}{n_1}\right) = -u. \qquad (12)$$

Therefore we derive a contradiction from (11) and (12).

Case II: t is odd. Similarly, by (1), we have

$$\left(m^2 + 4n'^2\right)^{2^{t-i} Z} + \left(m^2 - 4n'^2\right)^{2^{t-i} X} = 2(m_i n_i)^y, \qquad (13)$$
$$i = 1, 2, \ldots, t-1,$$

$$\left(m^2 + 4n'^2\right)^Z + \left(m^2 - 4n'^2\right)^X = 2(m_t n_t)^y \qquad (14)$$

and

$$\left(m^2 + 4n'^2\right)^Z - \left(m^2 - 4n'^2\right)^X = 2^{2y-t}(m_{t+1} n_{t+1})^y. \qquad (15)$$

Similarly, we have $m_1 \equiv n_1 \equiv \cdots m_{t-1} \equiv n_{t-1} \equiv n_t \equiv m_{t+1} \equiv 1 \pmod{8}$ and $m_t \equiv m^2 + 4n'^2 \equiv 5 \pmod{8}$.

By (13), we have

$$\left(\frac{2m_i n_i}{m + 2n'}\right) = 1, \; i = 1, 2, \ldots, t-1. \qquad (16)$$

Since $m_1 \equiv n_1 \equiv \cdots m_{t-1} \equiv n_{t-1} \equiv 1 \pmod{8}$, by (16)

$$\left(\frac{2}{m + 2n'}\right) = \left(\frac{n'}{m_i}\right)\left(\frac{m}{n_i}\right), \; i = 1, 2, \ldots, t-1. \qquad (17)$$

By (14), we have

$$\left(\frac{2}{m + 2n'}\right) = \left(\frac{2m_t n_t}{m + 2n'}\right). \qquad (18)$$

Since $m_t \equiv 5 \pmod{8}$ and $n_t \equiv 1 \pmod{8}$, by (18)

$$1 = \left(\frac{2n'}{m_t}\right)\left(\frac{m}{n_t}\right) = -\left(\frac{n'}{m_t}\right)\left(\frac{m}{n_t}\right). \qquad (19)$$

By (15) and t is odd, we have

$$\left(\frac{2}{m + 2n'}\right) = \left(\frac{2m_{t+1} n_{t+1}}{m + 2n'}\right). \qquad (20)$$

Since $m_{t+1} \equiv 1 \pmod{8}$, by (20)

$$1 = \left(\frac{2n'}{m_{t+1}}\right)\left(\frac{m}{n_{t+1}}\right) = \left(\frac{n'}{m_{t+1}}\right)\left(\frac{m}{n_{t+1}}\right). \qquad (21)$$

Combine the three equations (17), (19) and (21), we obtain

$$\left(\frac{2}{m + 2n'}\right)^{t-1} = -\prod_{i=1}^{t+1} \left(\frac{n'}{m_i}\right)\left(\frac{m}{n_i}\right)$$
$$= -\left(\frac{n'}{m}\right)\left(\frac{m}{n'}\right) = -1,$$

contradicts to the fact that t is odd. This completes the proof. $\square$

4. Conclusion

64 years ago, Jeśmanowicz proposed the Conjecture 1.1. 3 years ago Ma and Chen partly proved the conjecture, i.e. Proposition 1.1. But their method is deep and complicated. In this paper, we prove the Proposition 2.1, and then present an elementary and simple proof of Proposition 1.1.

References

[1] Z. Cao, A note on the Diophantine equation $a^x + b^y = c^z$, Acta Arith. 91 (1999) 85-93.

[2] M. Deng, D. Huang, A note on Jeśmanowicz' conjecture concerning primitive Pythagorean triples. Bull. Aust. Math. Soc. 95 (2017) 5-13.

[3] M. Deng, J. Guo, A note on Jeśmanowicz' conjecture concerning primitive Pythagorean triples. II. Acta Math. Hungar. 153 (2017) 436-448.

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

[5] Y. Fujita and T. Miyazaki, Jeśmanowicz' conjecture with congruence relations, Colloq. Math. 128 (2012) 211-222.

[6] Y. Guo and M. Le, A note on Jeśmanowicz' conjecture concerning Pythagorean numbers, Comment. Mat., Univ. St. Pauli 44 (1995) 225-228

[7] Q. Han and P. Yuan, A note on Jeśmanowicz' conjecture, Acta Math Hungar. https://doi.org/10.1007/s10474-018-0837-4.

[8] L. Jeśmanowicz, Several remarks on Pythagorean numbers. Wiadom. Mat. 1 (1955/56) 196-202.

[9] M. Le, A note on Jeśmanowicz' conjecture concerning Pythagorean triples', Bull. Aust. Math. Soc. 59 (1999), 477-480.

[10] W. Lu, On the Pythagorean numbers $4n^2 - 1, 4n$ and $4n^2 + 1$, Acta Sci. Natur. Univ. Szechuan 2 (1959) 39-42.

[11] Ma, Mi-Mi; Chen, Yong-Gao Jeśmanowicz' conjecture on Pythagorean triples. Bull. Aust. Math. Soc. 96 (2017) 30-35.

[12] T. Miyazaki, On the conjecture of Jesmanowicz concerning Pythagorean triples, Bull. Aust. Math. Soc. 80 (2009), 413C422.

[13] T. Miyazaki, Jeśmanowicz' conjecture on exponential Diophantine equations, Funct. Approximatio Comment Math. 45 (2011) 207-229.

[14] T. Miyazaki, Generalizations of classical results on Jeśmanowicz' conjecture concerning Pythagorean triples, J. Number Theory 133 (2013) 583-595 .

[15] T. Miyazaki, A remark on Jeśmanowicz' conjecture for the non-coprimality case, Acta Math. Sin. (Engl. Ser.) 31 (2015) 1255-1260.

[16] T. Miyazaki, Contributions to some conjectures on a ternary exponential Diophantine equations, Acta Arith. (to appear).

[17] T. Miyazaki and N. Terai, On Jeśmanowicz' conjecture concerning Pythagorean triples II, Acta Math. Hungar. 142 (2015) 286-293.

[18] T. Miyazaki, P. Yuan, D. Wu, Generalizations of classical results on Jeśmanowicz' conjecture concerning Pythagorean triples II, J. Number Theory, 141 (2014) 184-201.

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

[20] K. Takakuwa, A remark on Jeśmanowicz' conjecture, Proc. Japan Acad. Ser. A Math. Sci. 72 (1996) 109-110.

[21] M. Tang, Z. Yang, Jeśmanowicz' conjecture revisited, Bull. Aust. Math. Soc. 88 (2013) 486-491.

[22] N. Terai, Applications of a lower bound for linear forms in two logarithms to exponential Diophantine equations, Acta Arith. 90 (1999) 17-35.

[23] N. Terai, On Jeémanowicz' conjecture concerning primitive Pythagorean triples, J. Number Theory 141 (2014) 316-323.

[24] P. Yuan and Q. Han, Jeśmanowicz' conjecture and related equations, Acta Arith. 184 (2018), 37-49.

[25] X. Zhang, W. Zhang, The exponential Diophantine equation $((2^{2m} - 1)n)^x + (2^{m+1}n)^y = ((2^{2m} + 1)n)^z$, Bull. Math. Soc. Sci. Math. Roumanie (N.S.) 57 (2014) 337-344.