



ELSEVIER

Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt



On Jeśmanowicz' conjecture concerning primitive Pythagorean triples



Nobuhiro Terai

Division of Information System Design, Faculty of Engineering,
Ashikaga Institute of Technology, 268-1 Omae, Ashikaga, Tochigi 326-8558, Japan

ARTICLE INFO

Article history:

Received 28 December 2013
Received in revised form 28
February 2014
Accepted 28 February 2014
Available online 2 April 2014
Communicated by David Goss

MSC:

11D61

Keywords:

Pythagorean triples
Exponential Diophantine equations
Generalized Fermat equations
Linear forms in two logarithms

ABSTRACT

In 1956, Jeśmanowicz conjectured that the exponential Diophantine equation $(m^2 - n^2)^x + (2mn)^y = (m^2 + n^2)^z$ has only the positive integer solution $(x, y, z) = (2, 2, 2)$, where m and n are positive integers with $m > n$, $\gcd(m, n) = 1$ and $m \not\equiv n \pmod{2}$. We show that if $n = 2$, then Jeśmanowicz' conjecture is true. This is the first result that if $n = 2$, then the conjecture is true without any assumption on m .

© 2014 Elsevier Inc. All rights reserved.

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 a, b and c are relatively prime, this triple is called *primitive*. It is well-known that a primitive Pythagorean triple (a, b, c) can be parameterized by

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

E-mail address: terai@ashitech.ac.jp.

where m and n are positive integers with $m > n$, $\gcd(m, n) = 1$ and $m \not\equiv n \pmod{2}$. In this paper, we consider the exponential Diophantine equation

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

in positive integers x, y, z . In 1956, Sierpiński [S1] showed that the equation

$$3^x + 4^y = 5^z$$

has only the positive integer solution $(x, y, z) = (2, 2, 2)$. (Cf. Sierpiński [S2].) Jeśmanowicz [J] proved that the only positive integer solution of each of the equations

$$5^x + 12^y = 13^z, \quad 7^x + 24^y = 25^z, \quad 9^x + 40^y = 41^z, \quad 11^x + 60^y = 61^z$$

is given by $(x, y, z) = (2, 2, 2)$, and proposed the following:

Conjecture 1. *Eq. (1) has only the positive integer solution $(x, y, z) = (2, 2, 2)$.*

This is one of famous unsolved problems in the field of exponential Diophantine equations. Conjecture 1 has been verified to be true in many special cases.

After the work of Jeśmanowicz, in 1959, Lu [Lu] first verified that if $n = 1$, then Conjecture 1 is true without any assumption on m . Dem'janenko [De] improved earlier results by establishing that if $m - n = 1$, then Conjecture 1 is true. Using elementary methods, Le [Le] showed that if $mn \equiv 2 \pmod{4}$ and $m^2 + n^2$ is a power of a prime, then Conjecture 1 is true. Guo–Le [GL] 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 is true. Takakuwa [Ta] extended the result of Guo–Le [GL] by proving that if $n = 3, 7, 11, 15$ and $m \equiv 2 \pmod{4}$, then Conjecture 1 is true. Cao [C] also showed that if $m \equiv 5 \pmod{8}$ and $n \equiv 2 \pmod{8}$, then Conjecture 1 is true. Moreover, Miyazaki [M3] has recently generalized both results of Lu [Lu] and Dem'janenko [De] by proving that if $a \equiv \pm 1 \pmod{b}$ or $c \equiv 1 \pmod{b}$, then Conjecture 1 is true. (For other known results, see [DC, FM, M1].) Note that all results above have restrictions on m for given $n > 1$.

The purpose of this paper is to show that if $n = 2$, then Conjecture 1 is true without any assumption on m :

Theorem 1. *Suppose that $n = 2$. Then Eq. (1) has only the positive integer solution $(x, y, z) = (2, 2, 2)$.*

The proof of Theorem 1 is given as follows. When $y > 1$, we show Theorem 1 by combining elementary methods with a result due to Miyazaki [M2], which is derived by appealing to several results (cf. [BS, Da, DM]) on generalized Fermat equations. When $y = 1$, Eq. (1) becomes a Pillai equation, which can be solved by applying a lower bound for linear forms in two logarithms due to Laurent [La]. It is worth noting that the proof

of [Conjecture 1](#) for the case $n = 1$ is elementary, while our proof for the case $n = 2$ is based on deep results on generalized Fermat equations via sophisticated arguments in the theory of elliptic curves and modular forms.

2. Preliminaries

The following result due to Miyazaki [[M2, Theorem 1.5](#)] plays an important role in the proof of [Theorem 1](#).

Proposition 1. (See Miyazaki [[M2](#)].) *Let x, y, z be a solution of (1). Assume that x and z are even. Then $x/2$ and $z/2$ are odd.*

In order to obtain an upper bound for a solution of Pillai's equation $c^z - a^x = b$ in [Section 3](#), we need a lower bound for linear forms in two logarithms. Now we introduce some notation. Let α_1 and α_2 be real algebraic numbers with $|\alpha_1| \geq 1$ and $|\alpha_2| \geq 1$. We consider the linear form

$$\Lambda = b_2 \log \alpha_2 - b_1 \log \alpha_1,$$

where b_1 and b_2 are positive integers. As usual, the *logarithmic height* of an algebraic number α of degree n is defined as

$$h(\alpha) = \frac{1}{n} \left(\log |a_0| + \sum_{j=1}^n \log \max \{1, |\alpha^{(j)}| \} \right),$$

where a_0 is the leading coefficient of the minimal polynomial of α (over $\mathbb{Z}$) and $(\alpha^{(j)})_{1 \leq j \leq n}$ are the conjugates of α . Let A_1 and A_2 be real numbers greater than 1 with

$$\log A_i \geq \max \left\{ h(\alpha_i), \frac{|\log \alpha_i|}{D}, \frac{1}{D} \right\},$$

for $i \in \{1, 2\}$, where D is the degree of the number field $\mathbb{Q}(\alpha_1, \alpha_2)$ over $\mathbb{Q}$. Define

$$b' = \frac{b_1}{D \log A_2} + \frac{b_2}{D \log A_1}.$$

We choose to use a result due to Laurent [[La, Corollary 2](#)] with $m = 10$ and $C_2 = 25.2$.

Proposition 2. (See Laurent [[La](#)].) *Let Λ be given as above, with $\alpha_1 > 1$ and $\alpha_2 > 1$. Suppose that α_1 and α_2 are multiplicatively independent. Then*

$$\log |\Lambda| \geq -25.2D^4 \left(\max \left\{ \log b' + 0.38, \frac{10}{D} \right\} \right)^2 \log A_1 \log A_2.$$

3. Proof of Theorem 1

Let (x, y, z) be a solution of (1). The proof of Theorem 1 is divided into two cases: $y > 1$ and $y = 1$.

3.1. The case $y > 1$

Lemma 1. Suppose that $y > 1$. Then:

- (i) x and z are even.
- (ii) If $m \not\equiv 1 \pmod{8}$, then y is even.

Proof. (i) In view of $y > 1$, taking (1) modulo 8 implies that $5^x \equiv 5^z \pmod{8}$. Thus, we see that $x \equiv z \pmod{2}$.

Suppose that $m \equiv 1 \pmod{4}$. Then we have

$$\left(\frac{4m}{m^2-4}\right) = 1, \quad \left(\frac{m^2+4}{m^2-4}\right) = \left(\frac{2}{m^2-4}\right) = -1,$$

where $\left(\frac{*}{*}\right)$ denotes the Jacobi symbol. From (1), we see that z is even, so x is even.

Suppose that $m \equiv 3 \pmod{4}$. Then taking (1) modulo m implies that $(-4)^x \equiv 4^z \pmod{m}$. Since $\left(\frac{-1}{m}\right) = -1$ from $m \equiv 3 \pmod{4}$, we see that x is even, so z is even.

(ii) It is easy to see that $\left(\frac{4m}{m+2}\right) = -1$ or $\left(\frac{4m}{m-2}\right) = -1$ if and only if $m \not\equiv 1 \pmod{8}$. Since z is even from (i), we see that y is even. $\square$

Now put $x = 2X$ and $z = 2Z$, where X and Z are positive integers. From (1), we define even positive integers A and B as follows:

$$(4m)^y = AB, \tag{2}$$

where

$$A = (m^2 + 4)^Z + (m^2 - 4)^X, \quad B = (m^2 + 4)^Z - (m^2 - 4)^X.$$

It is easy to see that $\gcd(A, B) = 2$, $A \equiv 2 \pmod{4}$ and $B \equiv 0 \pmod{4}$. We therefore obtain

$$(m^2 + 4)^Z + (m^2 - 4)^X = 2m_1^y, \quad (m^2 + 4)^Z - (m^2 - 4)^X = 2^{2y-1}m_2^y, \tag{3}$$

where m_1 and m_2 are odd with $m = m_1m_2$. Adding these yields

$$m_1^y + 2^{2y-2}m_2^y = (m^2 + 4)^Z. \tag{4}$$

In order to show [Theorem 1](#) with $y > 1$, it suffices to show that Eq. (4) has only the solution $(y, Z) = (2, 1)$.

Lemma 2. *Suppose that $y > 1$. Then:*

- (i) *If $y = 2$, then $Z = X = 1$.*
- (ii) *If $y \geq 3$, then Z is even.*

Proof. (i) From (2), we have

$$(4m)^2 \geq ((m^2 + 4)^Z + (m^2 - 4)^X) \cdot 2^3,$$

so $Z = X = 1$.

(ii) Since $y \geq 3$, taking (4) modulo 8 implies that

$$m_1^y \equiv 5^Z \pmod{8}.$$

If $m_1 \not\equiv 5 \pmod{8}$, then Z is even. If $m \not\equiv 1 \pmod{8}$, then Z is even, since y is even from [Lemma 1\(ii\)](#). Hence we may suppose that

$$m_1 \equiv 5 \pmod{8} \quad \text{and} \quad m \equiv 1 \pmod{8}.$$

But we show that this case does not occur. When $m_1 \equiv 5 \pmod{8}$, we see that $y \equiv Z \pmod{2}$. Note that

$$\left(\frac{m^2 + 4}{m + 2}\right) = \left(\frac{2}{m + 2}\right) = \left(\frac{m_1}{m + 2}\right) = -1,$$

since $m \equiv 1 \pmod{8}$, $m_1 \equiv 5 \pmod{8}$ and $m_1 | m$. The first equation in (3) leads to $(m^2 + 4)^Z \equiv 2m_1^y \pmod{m + 2}$ and so $(-1)^Z = (-1)^{y+1}$, which contradicts $y \equiv Z \pmod{2}$. $\square$

We are now in a position to show [Theorem 1](#) with $y > 1$. In view of [Lemmas 1, 2](#), we may suppose that $y \geq 3$ and Z is even. But this contradicts [Proposition 1](#). $\square$

3.2. The case $y = 1$

Our theorem is reduced to solving Pillai's equation

$$c^z - a^x = b \tag{5}$$

where $a = m^2 - 4$, $b = 4m$ and $c = m^2 + 4$. It is clear that $z > 1$.

We first want to obtain an upper bound for x .

Lemma 3. $x < 2521 \log c$.

Proof. From (5), we now consider the following linear form in two logarithms:

$$\Lambda = z \log c - x \log a \quad (> 0).$$

Using the inequality $\log(1+t) < t$ for $t > 0$, we have

$$0 < \Lambda = \log\left(\frac{c^z}{a^x}\right) = \log\left(1 + \frac{b}{a^x}\right) < \frac{b}{a^x}.$$

Hence we obtain

$$\log \Lambda < \log b - x \log a. \quad (6)$$

On the other hand, we use Proposition 2 to obtain a lower bound for Λ . It follows from Proposition 2 that

$$\log \Lambda \geq -25.2(\max\{\log b' + 0.38, 10\})^2 (\log a)(\log c), \quad (7)$$

where $b' = \frac{x}{\log c} + \frac{z}{\log a}$.

We note that $a^{x+1} > c^z$. Indeed,

$$\begin{aligned} a^{x+1} - c^z &= a(c^z - b) - c^z = (a-1)c^z - ab \\ &\geq (m^2 - 5)(m^2 + 4)^2 - (m^2 - 4)(4m) > 0. \end{aligned}$$

Hence $b' < \frac{2x+1}{\log c}$.

Put $M = \frac{x}{\log c}$. Combining (6) and (7) leads to

$$x \log a < \log b + 25.2 \left(\max \left\{ \log \left(2M + \frac{1}{\log c} \right) + 0.38, 10 \right\} \right)^2 (\log a)(\log c),$$

so

$$M < 1 + 25.2 \left(\max \left\{ \log \left(2M + \frac{1}{2} \right) + 0.38, 10 \right\} \right)^2,$$

since $\log c = \log(m^2 + 4) \geq \log 13 > 2$ and $b < c$. We therefore obtain $M < 2521$. This completes the proof of Lemma 3. $\square$

We next want to obtain a lower bound for x .

Lemma 4. $x > \frac{m^2-4}{8} \log c$.

Proof. From (5), we see that $x > z$. Indeed,

$$(m^2 + 4)^z = (m^2 - 4)^x + 4m < (m^2 + 4)^x$$

for $x > 1$.

Now consider another linear form in two logarithms:

$$\Lambda_0 = \log c - \log a \quad (> 0).$$

Then

$$x\Lambda_0 - \Lambda = x(\log c - \log a) - (z \log c - x \log a) = (x - z) \log c \geq \log c.$$

See Bennett [B, pp. 901–902] and Terai [Te, pp. 21–22] for a “gap principle” for two solutions of Pillai’s equation. Note that

$$\Lambda_0 < \frac{8}{m^2 - 4}.$$

Indeed,

$$\Lambda_0 = \log\left(\frac{c}{a}\right) = \log\left(\frac{m^2 + 4}{m^2 - 4}\right) = \log\left(1 + \frac{8}{m^2 - 4}\right) < \frac{8}{m^2 - 4}.$$

Hence we obtain

$$x \geq \frac{\log c}{\Lambda_0} + \frac{\Lambda}{\Lambda_0} > \frac{\log c}{\Lambda_0} > \frac{m^2 - 4}{8} \log c.$$

This completes the proof of Lemma 4. $\square$

We are now in a position to show Theorem 1 with $y = 1$. It follows from Lemmas 3, 4 that

$$m^2 - 4 < 2521 \cdot 8.$$

Consequently we obtain $m \leq 141$. Recall the result of Cao [C], as stated in Introduction, that if $m \equiv 5 \pmod{8}$ and $n \equiv 2 \pmod{8}$, then Conjecture 1 is true. We may thus suppose that $m \not\equiv 5 \pmod{8}$, since $n = 2$ in our case. Finally, we checked by Magma that in the range $3 \leq m \leq 141$ with $m \equiv 1, 3, 7 \pmod{8}$, Eq. (5) has no solutions x, z with $z < x < 2521 \log(m^2 + 4)$. This completes the proof of Theorem 1. $\square$

Acknowledgments

The author would like to thank the referee for his valuable suggestions.

References

- [B] M.A. Bennett, On some exponential equations of S.S. Pillai, *Canad. J. Math.* 53 (2001) 897–922.
- [BS] M.A. Bennett, C. Skinner, Ternary Diophantine equations via Galois representations and modular forms, *Canad. J. Math.* 56 (2004) 23–54.
- [C] Z.F. Cao, A note on the Diophantine equation $a^x + b^y = c^z$, *Acta Arith.* 91 (1999) 85–93.
- [DC] M.J. Deng, G.L. Cohen, A note on a conjecture of Jeśmanowicz, *Colloq. Math.* 86 (2000) 25–30.
- [FM] Y. Fujita, T. Miyazaki, Jeśmanowicz’ conjecture with congruence relations, *Colloq. Math.* 128 (2012) 211–222.
- [De] V.A. Dem’janenko, On Jeśmanowicz’ problem for Pythagorean numbers, *Izv. Vyssh. Uchebn. Zaved. Mat.* 48 (1965) 52–56 (in Russian).
- [Da] H. Darmon, The equation $x^4 - y^4 = z^p$, *C. R. Math. Rep. Acad. Sci. Can.* 15 (1993) 286–290.
- [DM] H. Darmon, L. Merel, Winding quotients and some variants of Fermat’s Last Theorem, *J. Reine Angew. Math.* 490 (1997) 81–100.
- [GL] Y.D. Guo, M.-H. Le, A note on Jeśmanowicz’ conjecture concerning Pythagorean numbers, *Comment. Math. Univ. St. Pauli* 44 (1995) 225–228.
- [J] L. Jeśmanowicz, Some remarks on Pythagorean numbers, *Wiadom. Mat.* 1 (1955/1956) 196–202 (in Polish).
- [Le] M.-H. Le, A note on Jeśmanowicz’ conjecture, *Colloq. Math.* 69 (1995) 47–51.
- [La] M. Laurent, Linear forms in two logarithms and interpolation determinants II, *Acta Arith.* 133 (2008) 325–348.
- [Lu] Wen-Twan Lu, On Pythagorean numbers $4n^2 - 1, 4n, 4n^2 + 1$, *Acta Sci. Natur. Univ. Szechuan* 2 (1959) 39–42 (in Chinese).
- [M1] T. Miyazaki, On the conjecture of Jeśmanowicz concerning Pythagorean triples, *Bull. Aust. Math. Soc.* 80 (2009) 413–422.
- [M2] T. Miyazaki, Jeśmanowicz’ conjecture on exponential Diophantine equations, *Funct. Approx. Comment. Math.* 45 (2011) 207–229.
- [M3] T. Miyazaki, Generalizations of classical results on Jeśmanowicz’ conjecture concerning primitive Pythagorean triples, *J. Number Theory* 133 (2013) 583–595.
- [S1] W. Sierpiński, On the equation $3^x + 4^y = 5^z$, *Wiadom. Mat.* 1 (1955/1956) 194–195 (in Polish).
- [S2] W. Sierpiński, *Elementary Theory of Numbers*, PWN-Polish Scientific Publishers, 1988.
- [Ta] K. Takakuwa, A remark on Jeśmanowicz’ conjecture, *Proc. Japan Acad. Ser. A Math. Sci.* 72 (1996) 109–110.
- [Te] N. Terai, Applications of a lower bound for linear forms in two logarithms to exponential Diophantine equations, *Acta Arith.* 90 (1999) 17–35.