J. Aust. Math. Soc. **90** (2011), 355–370
doi:10.1017/S1446788711001340

THE SHUFFLE VARIANT OF JEŚMANOWICZ' CONJECTURE CONCERNING PYTHAGOREAN TRIPLES

TAKAFUMI MIYAZAKI

(Received 18 August 2010; accepted 25 October 2010)

Communicated by I. E. Shparlinski

Abstract

Let (a, b, c) be a primitive Pythagorean triple such that b is even. In 1956, Jeśmanowicz conjectured that the equation $a^x + b^y = c^z$ has the unique solution $(x, y, z) = (2, 2, 2)$ in the positive integers. This is one of the most famous unsolved problems on Pythagorean triples. In this paper we propose a similar problem (which we call the shuffle variant of Jeśmanowicz' problem). Our problem states that the equation $c^x + b^y = a^z$ with x, y and z positive integers has the unique solution $(x, y, z) = (1, 1, 2)$ if $c = b + 1$ and has no solutions if $c > b + 1$. We prove that the shuffle variant of the Jeśmanowicz problem is true if $c \equiv 1 \bmod b$.

2010 *Mathematics subject classification*: primary 11D61; secondary 11A51.

Keywords and phrases: exponential Diophantine equations, Pythagorean triples, lower bounds for linear forms in the logarithms.

1. Introduction

Let $\mathbb{N} = \{1, 2, 3, \ldots\}$ be the set of positive integers. When a, b and c are positive integers we call (a, b, c) a *Pythagorean triple* if $a^2 + b^2 = c^2$. If, in addition, a, b and c are relatively prime, then we call the triple (a, b, c) *primitive*. Pythagorean triples appear in many mathematical subjects, especially Diophantine equations.

For fixed relatively prime positive integers a, b and c, we call the equation

$$a^x + b^y = c^z, \tag{1.1}$$

where $x, y, z \in \mathbb{N}$, an exponential Diophantine equation. This field has a rich history. Originally this problem was considered for fixed triples (a, b, c). Using elementary congruences, the quadratic reciprocity law and factorizations in number fields, several authors determined complete solutions of (1.1) for small values of a, b and c (see, for example [12]). Mahler [7] first proved that (1.1) has finitely many solutions under the assumption that $a, b, c > 1$. Further, by Baker's theory of linear forms in logarithms, we can calculate a computable upper bound for solutions (which depends on a, b

and c only). Almost all recent work concerns various families of triples (a, b, c), for example, Pythagorean triples (see also [1, 3, 9, 11]), consecutive integers (see also [4]) and prime numbers (see also [13]).

One of the most famous unsolved problems in the field of exponential Diophantine equations was proposed by Jeśmanowicz [5], and may be stated as follows.

CONJECTURE 1.1. Let (a, b, c) be a primitive Pythagorean triple. Then (1.1) has the unique solution $(x, y, z) = (2, 2, 2)$.

Sierpiński [14] considered (1.1) for the most famous Pythagorean triple $(3, 4, 5)$, that is,

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

where $x, y, z \in \mathbb{N}$, and proved that the unique solution is $(x, y, z) = (2, 2, 2)$. Later Jeśmanowicz (see [5]) showed similar results for each of the following equations:

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

and proposed his conjecture. It is well known that, for any primitive Pythagorean triple (a, b, c) (we may assume that b is even), there exist integers m and n such that

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

where $m > n > 0$, $\gcd(m, n) = 1$ and $m \not\equiv n \bmod 2$. We will always consider the above expressions in this paper.

A number of special cases of Conjecture 1.1 have now been settled. In the first result concerning this conjecture that is true for an infinite number of triples, Lu [6] proved that the conjecture is true if $n = 1$. Extending some earlier work, Dem'janenko [2] proved that the conjecture is true if $c = b + 1$. These results use earlier results of Sierpiński and Jeśmanowicz and are crucially important since they are used in much early work. Recently the author [10] generalized these results by proving that the conjecture is true if $a \equiv \pm 1 \bmod b$ or $c \equiv 1 \bmod b$. For other known results see, for example, [1, 3, 9, 11].

On the other hand, for the Pythagorean triples studied by Sierpiński and Jeśmanowicz (also Dem'janenko and others),

$$(3, 4, 5), \quad (5, 12, 13), \quad (7, 24, 25), \quad (9, 40, 41), \quad (11, 60, 61),$$

we observe that

$$5 + 4 = 3^2, \quad 13 + 12 = 5^2, \quad 25 + 24 = 7^2, \quad 41 + 40 = 9^2, \quad 61 + 60 = 11^2,$$

in other words, $c + b = a^2$. Note that $c = b + 1$ for each of the above cases, so it is worth studying a variant of Equation (1.1) such as

$$c^x + b^y = a^z, \tag{1.2}$$

where $x, y, z \in \mathbb{N}$.

We propose an analogue of Conjecture 1.1 which we call the *shuffle* variant of the Jeśmanowicz' problem.

https://doi.org/10.1017/S1446788711001340 Published online by Cambridge University Press

Conjecture 1.2. Let (a, b, c) be a primitive Pythagorean triple such that b is even. If $c = b + 1$, then (1.2) has the unique solution $(x, y, z) = (1, 1, 2)$. If $c > b + 1$, then (1.2) has no solutions.

If $c = b + 1$, then, since $a^2 = c^2 - b^2 = (c + b)(c - b) = c + b$, we see that $(x, y, z) = (1, 1, 2)$ is always a solution of (1.2). It is easy to see that $c = b + 1$ if and only if $m = n + 1$.

We now state the main result in this paper.

Theorem 1.3. *If $c \equiv 1 \bmod b$, then Conjecture 1.2 is true.*

Clearly this is an analogue of our previous result in [10]. In the proof of Theorem 1.3, we use similar techniques to those found in [10] and, in addition, a lower bound for the linear forms in the logarithms of algebraic numbers based on Baker's theory.

In the next section, we prove that Conjecture 1.2 is true if $n = 1$ (which can be regarded as an analogue of the result in [6]). This is an important step in our proof. In fact, if $n > 1$, then we can use the parameters introduced by the author in [11] which are useful to examine parities of exponential variables x, y and z. It is crucially important to know the parities of the exponential variables for Conjecture 1.2. Using the parameters found in Section 4 we prove that if $c \equiv 1 \bmod b$ with $c > b + 1$, then (1.2) has no solutions. In the final section we prove that if $c = b + 1$, then (1.2) has the unique solution $(x, y, z) = (1, 1, 2)$ by using various elementary arguments and the result on lower bounds for linear forms in two logarithms due to Mignotte [8].

In what follows we frequently consider the equation

$$(m^2 + n^2)^x + (2mn)^y = (m^2 - n^2)^z, \tag{1.3}$$

where $x, y, z \in \mathbb{N}$.

2. The case where $n = 1$

In this section we prove that Conjecture 1.2 is true if $n = 1$. When $n = 1$ we note that m may be any even positive integer.

The following proposition can be regarded as an analogue of the result in [6].

Proposition 2.1. *If $n = 1$, then Conjecture 1.2 is true.*

Proof. When $n = 1$, we rewrite (1.3) as

$$(m^2 + 1)^x + (2m)^y = (m^2 - 1)^z, \tag{2.1}$$

where $x, y, z \in \mathbb{N}$ and m is an even positive integer.

Let (x, y, z) be a solution of (2.1). Taking (2.1) modulo $2m$, we have $(-1)^z \equiv 1 \bmod 2m$. Hence z is even since $2m \geq 3$. We can write $z = 2Z$ for some $Z \geq 1$.

Suppose that $y > 1$. We will observe that this leads to a contradiction. Taking (2.1) modulo $2m^2$, we obtain

$$xm^2 + 1 \equiv 1 \mod 2m^2$$

https://doi.org/10.1017/S1446788711001340 Published online by Cambridge University Press

and so $x \equiv 0 \bmod 2$. We can write $x = 2X$ for some $X \geq 1$. Rearranging (2.1), we define even positive integers A and B as follows:

$$(2m)^y = AB, \tag{2.2}$$

where

$$A = (m^2-1)^Z + (m^2+1)^X, \quad B = (m^2-1)^Z - (m^2+1)^X.$$

It is easy to see that $\gcd(A, B) = 2$ and

$$A \equiv (-1)^Z + 1, \quad B \equiv (-1)^Z - 1 \mod 2m.$$

We claim that Z is odd. Indeed, if Z is even, then $A \equiv 2 \bmod 2m$, that is, $A/2 \equiv 1 \bmod m$. This means that $A/2$ is odd and coprime to m. It follows from (2.2) that $A = 2$, which is clearly absurd. Hence Z is odd. It follows that $B \equiv -2 \bmod 2m$, that is, $B/2 \equiv -1 \bmod m$. This means that $B/2$ is odd and coprime to m. It follows from (2.2) that

$$B = (m^2-1)^Z - (m^2+1)^X = 2.$$

Taking B modulo m^2, we obtain $4 \equiv 0 \bmod m^2$ since Z is odd. Hence $m = 2$ and so $A = 3^Z + 5^X = 2^{2y-1}$ and $B = 3^Z - 5^X = 2$. However, this implies that

$$3^Z = (A+B)/2 = 4^{y-1} + 1 \equiv 2 \mod 3,$$

which is a contradiction. Therefore $y = 1$.

Taking (2.1) modulo m^2, we obtain $1 + 2m \equiv 1 \bmod m^2$ and so $2 \equiv 0 \bmod m$. Hence $m = 2$ and $5^x + 4 = 3^{2Z}$. From this we may conclude that $5^x = (3^Z + 2)(3^Z - 2)$. Since these two factors are relatively prime we see that $3^Z - 2 = 1$ and so $Z = 1$. Hence $x = 1$. This completes the proof of Proposition 2.1. □

3. Preliminaries

In this section we prove some lemmas that will be of use when proving Theorem 1.3. First we give lemmas that examine the parities of the exponential variables x, y and z. In order to examine Conjecture 1.2, it is crucially important to know the parities of the exponential variables.

The following notation was previously established by the author in [11]. By Proposition 2.1, we may assume that $n > 1$. We define integers α, β, and e, satisfying the conditions $\alpha \geq 1$, $\beta \geq 2$, and $e = \pm 1$, and odd positive integers i and j as follows:

$$\begin{aligned} &m = 2^\alpha i, \quad n = 2^\beta j + e \quad \text{if } m \text{ is even,} \\ &m = 2^\beta j + e, \quad n = 2^\alpha i \quad \text{if } m \text{ is odd.} \end{aligned} \tag{3.1}$$

We will see that if $c \equiv 1 \bmod b$, then $2\alpha \neq \beta + 1$.

The following two lemmas will be used to determine the parities of the exponential variables. In particular, Lemma 3.1 will play an important role in the proof of our main theorem.

Lemma 3.1. *Assume that $2\alpha \neq \beta + 1$. Let (x, y, z) be a solution of (1.3). If $y > 1$, then $x \equiv z \bmod 2$.*

https://doi.org/10.1017/S1446788711001340 Published online by Cambridge University Press

Proof. Suppose that $2\alpha \neq \beta + 1$. We consider the case where m is even. As in Equation (3.1), we set $m = 2^\alpha i$ and $n = 2^\beta j + e$.

Let (x, y, z) be a solution of (1.3). Then it is easy to see that z is even by taking (1.3) modulo 4. Suppose that $x \not\equiv z \bmod 2$ or, in other words, that x is odd. Taking (1.3) modulo $2^{2\alpha+1}$, we obtain

$$\begin{aligned}(2mn)^y &= (m^2 - n^2)^z - (m^2 + n^2)^x \\ &\equiv -zm^2n^{2z-2} + n^{2z} - xm^2n^{2x-2} - n^{2x} \\ &\equiv -m^2(zn^{2z-2} + xn^{2x-2}) + n^{2z} - n^{2x} \mod 2^{2\alpha+1}.\end{aligned}$$

Now write

$$A = -m^2(zn^{2z-2} + xn^{2x-2}), \quad B = n^{2z} - n^{2x}.$$

Then

$$(2mn)^y \equiv A + B \mod 2^{2\alpha+1}.$$

We denote the 2-adic valuation by ν_2.

Since $x \not\equiv z \bmod 2$ we have that $zn^{2z-2} + xn^{2x-2}$ is odd and hence

$$\nu_2(A) = \nu_2(m^2) = \nu_2(2^{2\alpha}i^2) = 2\alpha,$$
$$\nu_2(B) = \nu_2(n^{2|x-z|} - 1) = \nu_2(n^2 - 1) = \nu_2(2^{2\beta}j^2 \pm 2^{\beta+1}j) = \nu_2(2^{\beta+1}j) = \beta + 1.$$

Since $\nu_2((2mn)^y) = (\alpha + 1)y$ and $2\alpha \neq \beta + 1$ it follows that

$$(\alpha + 1)y = \begin{cases} 2\alpha & \text{if } 2\alpha < \beta + 1, \\ \beta + 1 & \text{if } 2\alpha > \beta + 1. \end{cases}$$

This implies that $\alpha = 1$ and $y = 1$ or $\alpha = \beta$ and $y = 1$. Therefore, if $y > 1$, then $x \equiv z \bmod 2$. We can prove the lemma similarly for the case where m is odd. □

Lemma 3.2. *Suppose that $2\alpha \neq \beta + 1$. Let (x, y, z) be a solution of (1.3). If x and z are even, then $X \equiv Z \bmod 2$ where $X = x/2$ and $Z = z/2$.*

Proof. Suppose that $2\alpha \neq \beta + 1$. Let (x, y, z) be a solution of (1.3). Suppose that x and z are even. We can write $x = 2X$ and $z = 2Z$ for some $X, Z \geq 1$. We define even positive integers D and E by

$$D = (m^2 - n^2)^Z + (m^2 + n^2)^X \quad \text{and} \quad E = (m^2 - n^2)^Z - (m^2 + n^2)^X.$$

Then $(2mn)^y = DE$ by (1.3). It follows that $y > 1$ since

$$(2mn)^y \geq D > m^2 + n^2 > 2mn.$$

It is easy to see that $\gcd(D, E) = 2$. Since DE is exactly divisible by $2^{(\alpha+1)y}$, we see that the congruence

$$(m^2 + n^2)^X \pm (m^2 - n^2)^Z \equiv 0 \mod 2^{(\alpha+1)y-1}$$

holds for the proper sign.

https://doi.org/10.1017/S1446788711001340 Published online by Cambridge University Press

We first consider the case where $2\alpha > \beta + 1$. Since

$$(\alpha + 1)y - 1 > 2\alpha \geq \beta + 2,$$

the above congruence can be reduced to

$$(m^2 + n^2)^X \pm (m^2 - n^2)^Z \equiv 0 \mod 2^{\beta+2}.$$

Substituting the expressions for α and β from Equation (3.1) into this congruence, we obtain

$$2^{\beta+1} ejX \equiv \pm 2^{\beta+1} ejZ \mod 2^{\beta+2}.$$

This implies that $X \equiv Z \bmod 2$ since ej is odd.

Next we consider the case where $2\alpha < \beta + 1$. Since we have $(\alpha + 1)y - 1 \geq 2\alpha + 1$ and $\beta + 1 \geq 2\alpha + 1$ it follows from the above congruence that

$$2^{2\alpha} i^2 X \equiv \pm 2^{2\alpha} i^2 Z \mod 2^{2\alpha+1}.$$

This implies that $X \equiv Z \bmod 2$ since i is odd. □

Next, in order to obtain an upper bound for solutions, we quote a result on lower bounds for linear forms in the logarithms of two algebraic numbers. The following lemma is an immediate consequence of the corollary found in [8, pp. 110–111].

LEMMA 3.3. *Let α_1 and α_2 be relatively prime positive integers greater than* 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. Let ρ, λ, a_1 and a_2 be real positive numbers such that $\rho \geq 4$, $\lambda = \log \rho$,

$$a_i \geq (\rho + 1) \log \alpha_i$$

when $1 \leq i \leq 2$, and

$$a_1 a_2 \geq \max\{20, 4\lambda^2\}.$$

In addition, let h be a real number such that

$$h \geq \max\left\{3.5, 1.5\lambda, \log\left(\frac{b_1}{a_2} + \frac{b_2}{a_1}\right) + \log \lambda + 1.4\right\}.$$

We write $\chi = h/\lambda$ and $v = 4\chi + 4 + 1/\chi$. Then we have the lower bound

$$\log |\Lambda| \geq -(C_0 + 0.06)(\lambda + h)^2 a_1 a_2,$$

where

$$C_0 = \frac{1}{\lambda^3}\left\{\left(2 + \frac{1}{2\chi(\chi+1)}\right)\left(\frac{1}{3} + \sqrt{\frac{1}{9} + \frac{4\lambda}{3v}\left(\frac{1}{a_1} + \frac{1}{a_2}\right) + \frac{32\sqrt{2}(1+\chi)^{3/2}}{3v^2\sqrt{a_1 a_2}}}\right)\right\}^2.$$

We use Lemma 3.3 to prove the following lemma.

LEMMA 3.4. *Let (x, y, z) be a solution of (1.3). If $y = 1$, then $x < 4020 \log a$.*

https://doi.org/10.1017/S1446788711001340 Published online by Cambridge University Press

PROOF. Let (x, y, z) be a solution of (1.3). Suppose that $y = 1$, that is,

$$c^x + b = a^z,$$

where $a = m^2 - n^2$, $b = 2mn$ and $c = m^2 + n^2$. Note that $a \geq 3$ and $c \geq 5$. Write

$$\Lambda = z \log a - x \log c.$$

Then $\Lambda > 0$. Since

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

we have

$$\log \Lambda < \log b - x \log c.$$

We will obtain a lower bound for $\log \Lambda$ by using Lemma 3.3. Applying the notation from Lemma 3.3 we write $(\alpha_1, \alpha_2, b_1, b_2) = (c, a, x, z)$. We may take $a_1 = (\rho + 1) \log c$ and $a_2 = (\rho + 1) \log a$. Let $\rho = 4.69$ and $\lambda = \log \rho$. Then we see that $a_1 a_2 \geq \max\{20, 4\lambda^2\}$. Since

$$c^{x+1} - a^z = (c - 1)c^x - b \geq 4c - b > 0,$$

we have $z/\log c < (x + 1)/\log a$ and so

$$\frac{x}{\log a} + \frac{z}{\log c} < 2s + \frac{1}{\log a} \leq 2s + \frac{1}{\log 3},$$

where $s = x/\log a$. Now we may take

$$h = \max\left\{3.5, \log\left(2s + \frac{1}{\log 3}\right) + \log \lambda + 1.4\right\}.$$

We will treat the two possible choices for h in turn. First, if $h = 3.5$, then $\log(2s + 1/\log 3) < 1.7$ and so $s < e^{1.7}/2 < 2.8$. Hence the lemma holds in this case.

Next we consider the case where

$$h = \log\left(2s + \frac{1}{\log 3}\right) + \log \lambda + 1.4 \geq 3.5.$$

We find an upper bound for C_0. Since $\chi \geq (3.5)/\lambda$ and $v/4 > \chi + 1$ in Lemma 3.3 we see that

$$\frac{1}{2\chi(\chi + 1)} \leq \frac{\lambda}{(24.5)/\lambda + 7},$$

$$\begin{aligned}\frac{4\lambda}{3v}\left(\frac{1}{a_1} + \frac{1}{a_2}\right) &< \frac{\lambda}{3(\chi + 1)(\rho + 1)}\left(\frac{1}{\log 3} + \frac{1}{\log 5}\right) \\ &\leq \frac{\lambda}{3((3.5)/\lambda + 1)(\rho + 1)}\left(\frac{1}{\log 3} + \frac{1}{\log 5}\right)\end{aligned}$$

https://doi.org/10.1017/S1446788711001340 Published online by Cambridge University Press

and

$$\frac{32\sqrt{2}(1+\chi)^{3/2}}{3v^2\sqrt{a_1a_2}} < \frac{32\sqrt{2}(v/4)^{3/2}}{3v^2\sqrt{a_1a_2}} = \frac{4\sqrt{2}}{3\sqrt{va_1a_2}}$$
$$< \frac{2\sqrt{2}}{3(\rho+1)\sqrt{(\chi+1)\log 3\log 5}}$$
$$\le \frac{2\sqrt{2}}{3(\rho+1)\sqrt{((3.5)/\lambda+1)\log 3\log 5}}.$$

Hence $C_0 < 0.7508$. By Lemma 3.3,

$$-26.25(h+\lambda)^2 \log a \log c < \log \Lambda < \log b - x \log c$$

and so

$$s < \frac{\log b}{\log a \log c} + 26.25(h+\lambda)^2$$
$$\le \frac{1}{\log 3} + 26.25\left(\log\left(2s + \frac{1}{\log 3}\right) + \lambda + \log\lambda + 1.4\right)^2.$$

This implies that $s < 4020$. □

4. The case where $c \equiv 1 \bmod b$ with $c > b + 1$

In this section, we prove that if $c \equiv 1 \bmod b$ with $c > b + 1$, then (1.3) has no solutions.

Assume that $c \equiv 1 \bmod b$, or equivalently, that

$$m^2 + n^2 = 1 + 2mnt, \tag{4.1}$$

where t is a positive integer. Then

$$m^2 \equiv 1 \mod n, \tag{4.2}$$
$$n^2 \equiv 1 \mod m. \tag{4.3}$$

By Proposition 2.1 we may assume that $n > 1$. We first verify that $2\alpha \ne \beta + 1$.

Lemma 4.1. *With notation as in Equation (3.1), the following hold.*

(i) *m or n is divisible by $2t$.*
(ii) $2\alpha \ne \beta + 1$.

Proof. (i) Since $m > n$ we see from Equation (4.1) that $2m^2 > m^2 + n^2 > 2mnt$ and so $m > nt$. By Equation (4.1) we see that $(U, V) = (m - nt, n)$ is a positive integer solution of the Pellian equation

$$U^2 - (t^2 - 1)V^2 = 1.$$

Since $t + \sqrt{t^2 - 1}$ is the fundamental solution of the above Pellian equation, all of the pairs (m, n) satisfying Equation (4.1) are given by

$$m = U_l + tV_l, \quad n = V_l,$$

https://doi.org/10.1017/S1446788711001340 Published online by Cambridge University Press

where the positive integers U_l and V_l (where $l \geq 1$) are defined by

$$U_l + V_l\sqrt{t^2-1} = (t+\sqrt{t^2-1})^l.$$

We prove (i) by induction on l. Statement (i) is clearly true when $l = 1$. Suppose that statement (i) holds for some positive integer l, that is,

$$U_l + tV_l \equiv 0 \mod 2t \quad \text{or } V_l \equiv 0 \mod 2t.$$

Then $U_{l+1} = tU_l + (t^2-1)V_l$ and $V_{l+1} = U_l + tV_l$. If we have $U_l + tV_l \equiv 0 \bmod 2t$, then $V_{l+1} \equiv 0 \bmod 2t$. If $V_l \equiv 0 \bmod 2t$, then

$$U_{l+1} + tV_{l+1} = 2tU_l + (2t^2-1)V_l \equiv 0 \mod 2t.$$

Now statement (i) follows by induction.

(ii) We consider the case where m is even. As defined in Equation (3.1), we set $m = 2^\alpha i$ and $n = 2^\beta j + e$. By (i) we know that $2^\alpha i$ is divisible by $2t$. In particular we have $\nu_2(2t) \leq \alpha$ since i is odd. It follows from Equation (4.1) that

$$\beta + 1 = \nu_2((n-1)(n+1)) = \nu_2(m(m-2nt)) = \alpha + \nu_2(m-2nt).$$

Hence it suffices to check that $\nu_2(m-2nt) \neq \alpha$. If $\nu_2(2t) < \alpha$, then $\nu_2(2nt) < \alpha$ and so

$$\nu_2(m-2nt) = \nu_2(2nt) < \alpha.$$

If $\nu_2(2t) = \alpha$, then

$$\nu_2(m-2nt) = \alpha + \nu_2(i - n(2t/2^\alpha)) > \alpha.$$

Therefore $2\alpha \neq \beta + 1$. We can similarly prove statement (ii) in the case where m is odd. □

Lemma 4.2. *Let (x, y, z) be a solution of (1.3). Then z is even.*

Proof. Taking (1.3) modulo m, we have $(n^2)^x \equiv (-n^2)^z \bmod m$. Then $(-1)^z \equiv 1 \bmod m$ by Equation (4.3). It follows that z is even since $m > n > 1$. □

The first aim of this section is to prove the following proposition.

Proposition 4.3. *If $c \equiv 1 \bmod b$ with $c > b + 1$, then (1.3) has no solutions with $y > 1$.*

In order to prove Proposition 4.3 we further assume that $c > b + 1$, that is, $m > n + 1$ or $t > 1$. Let (x, y, z) be a solution of (1.3). Then $x < z$ since $c > a$. By Lemma 4.2 we can write $z = 2Z$ for some $Z \geq 1$.

Suppose that $y > 1$. We will observe that this leads to a contradiction. By Lemma 3.1 and part (ii) of Lemma 4.1 we see that x is even. We can write $x = 2X$ for some $X \geq 1$. Using (1.3) we define even positive integers D and E as follows:

$$(2mn)^y = DE, \tag{4.4}$$

https://doi.org/10.1017/S1446788711001340 Published online by Cambridge University Press

where

$$D = (m^2 - n^2)^Z + (m^2 + n^2)^X,$$
$$E = (m^2 - n^2)^Z - (m^2 + n^2)^X.$$

It is easy to see that $\gcd(D, E) = 2$. By Equations (4.2) and (4.3) we have

$$D \equiv (-1)^Z + 1, \quad E \equiv (-1)^Z - 1 \mod m$$

and

$$D \equiv 2, \quad E \equiv 0 \mod n.$$

We now prove some lemmas.

LEMMA 4.4. *The integers X and Z are odd.*

PROOF. By Lemma 3.2 and part (ii) of Lemma 4.1 we know that $X \equiv Z \bmod 2$. Suppose that X and Z are even. Then

$$D \equiv 2 \mod 4, \quad D \equiv 2 \mod m, \quad D \equiv 2 \mod n.$$

This implies that $D/2$ is odd and coprime to mn. It follows from Equation (4.4) that $D = 2$, which is clearly absurd. Therefore X and Z are odd. □

By Lemma 4.4 we have

$$D \equiv 0, \quad E \equiv -2 \mod m.$$

It is easy to see that if m is even, then $E \equiv 2 \bmod 4$ and if m is odd, then $D \equiv 2 \bmod 4$.

LEMMA 4.5. *The integer y is even.*

PROOF. We first consider the case where m is even. Now

$$E \equiv 2 \mod 4, \quad E \equiv -2 \mod m, \quad D \equiv 2 \mod n.$$

This implies that $E/2$ is odd and coprime to m and that D is coprime to n. It follows from Equation (4.4) that $D = 2^{y-1}m^y$ and $E = 2n^y$. Hence

$$(m^2 - n^2)^Z = (D + E)/2 = 2^{y-2}m^y + n^y.$$

Since Z is odd we see from Equation (4.3) that

$$n^y \equiv -1 \mod m.$$

By Equation (4.3) we can see that if y is even, then $2 \equiv 0 \bmod m$. It follows that $m = 2$ and hence $n = 1$ which is an excluded case. Further, if y is odd, then $n + 1 \equiv 0 \bmod m$ and so $m = n + 1$ which is an excluded case.

Next we consider the case where m is odd. We have

$$D \equiv 2 \mod 4, \quad E \equiv -2 \mod m, \quad D \equiv 2 \mod n.$$

This implies that $D/2$ is odd and coprime to n and that E is coprime to m. It follows from Equation (4.4) that $D = 2m^y$ and $E = 2^{y-1}n^y$. Hence

$$(m^2 - n^2)^Z = (D + E)/2 = m^y + 2^{y-2}n^y.$$

https://doi.org/10.1017/S1446788711001340 Published online by Cambridge University Press

We may deduce from Equation (4.2) that

$$m^y \equiv 1 \mod n.$$

Suppose that y is odd. We will observe that this leads to a contradiction. If y is odd, then $m \equiv 1 \bmod n$ by Equation (4.2). We write $m = 1 + hn$ for some $h \geq 1$. Substituting this into (4.1), we obtain

$$np = 2(t - h),$$

where $p = h(h - 2t) + 1$. By part (i) of Lemma 4.1 we know that n is divisible by $2t$ and so h is divisible by t. In particular, we have either $h = t$ or $h \geq 2t$. If $h = t$, then $p = 0$ and so $t^2 = 1$ and hence $t = 1$ which is an excluded case. If $h \geq 2t$, then $p = h(h - 2t) + 1 > 0$ and so $t - h = (np)/2 > 0$, which is clearly absurd. We conclude that y is even. □

By Lemma 4.5 and its proof we may assume that m is odd and y is even. We can write $y = 2Y$ for some $Y \geq 1$. Moreover,

$$D = 2m^{2Y}, \quad E = 2^{2Y-1}n^{2Y}.$$

We will obtain sharp upper and lower bounds for solutions X, Y, Z.

Lemma 4.6. *We have* $2m \leq Z - X$.

Proof. Taking (1.3) modulo m^2, we obtain $(n^2)^{2X} \equiv (n^2)^{2Z} \bmod m^2$. We may deduce from Equation (4.1) that

$$n^2 \equiv 1 + 2mnt \mod m^2.$$

It follows that

$$(1 + 2mnt)^{2X} \equiv (1 + 2mnt)^{2Z} \mod m^2$$

and so $4mntX \equiv 4mntZ \bmod m^2$.

We can similarly prove that $4mntX \equiv 4mntZ \bmod n^2$ by taking (1.3) modulo n^2. It follows that

$$4mntX \equiv 4mntZ \mod m^2n^2$$

since $\gcd(m, n) = 1$ and so $4tX \equiv 4tZ \bmod mn$. By part (i) of Lemma 4.1 we know that n is divisible by $2t$. Therefore $2X \equiv 2Z \bmod m$ and so, since m is odd, we have $X \equiv Z \bmod m$. Moreover $X \equiv Z \bmod 2m$ by Lemma 4.4. Since $Z > X$ we conclude that $2m \leq Z - X$. □

Lemma 4.7. *We have the following upper bound on the integer* Z*:*

$$Z < 4Y \leq (\log(c - 1))/(2 \log 2).$$

Proof. Since $\{c^X, b^Y, a^Z\}$ forms a primitive Pythagorean triple there exist integers k and l satisfying the conditions $k > l > 0$, $\gcd(k, l) = 1$ and $k \not\equiv l \bmod 2$ and such that

$$c^X = k^2 - l^2, \quad b^Y = 2kl, \quad a^Z = k^2 + l^2.$$

Since $b < a^2$ we see that $a^Z < 4k^2l^2 = b^{2Y} < a^{4Y}$ and so

$$Z < 4Y.$$

https://doi.org/10.1017/S1446788711001340 Published online by Cambridge University Press

Since $E = a^Z - c^X = 2l^2$ we have

$$l = 2^{Y-1}n^Y.$$

Further, since $(k+l)(k-l) = c^X$ and $\gcd(k+l, k-l) = 1$, there exist relatively prime odd integers u and v satisfying the conditions $u > v > 0$ and $c = uv$ and such that

$$k + l = u^X, \qquad k - l = v^X.$$

Hence we have

$$(2n)^Y = 2l = u^X - v^X = (u - v)w,$$

where

$$w = (u^X - v^X)/(u - v) = u^{X-1} + u^{X-2}v + \cdots + v^{X-1}$$

is an integer.

Since w is a sum of X odd integers we deduce from Lemma 4.4 that w is odd. Therefore we obtain

$$Y(\alpha + 1) = \nu_2(u - v).$$

Since $u - v \le u - 1 \le c - 1$ it follows that

$$Y = \frac{\nu_2(u-v)}{\alpha+1} \le \frac{\log(u-v)}{(\alpha+1)\log 2} \le \frac{\log(c-1)}{2\log 2}.$$ □

Since

$$c = m^2 + n^2 \le m^2 + (m-1)^2 = 2m^2 - 2m + 1,$$

it follows from Lemmas 4.6 and 4.7 that

$$2m + 2 \le \frac{2\log(2m^2 - 2m)}{\log 2},$$

which is a contradiction. This completes the proof of Proposition 4.3.

To complete this section we prove the following proposition.

PROPOSITION 4.8. *If $c \equiv 1 \bmod b$ where $c > b + 1$, then (1.3) has no solutions with $y = 1$.*

PROOF. Suppose that $c \equiv 1 \bmod b$ where $c > b + 1$. By Proposition 2.1 it suffices to consider the case where $n > 1$. Let (x, y, z) be a solution of (1.3). By the observations in the proof of Lemma 4.2 we see that z is even. We can write $z = 2Z$ for some $Z \ge 1$.

Suppose that $y = 1$. We will observe that this leads to a contradiction. By similar observations to those found in the proof of Lemma 4.6 we see that

$$(1 + 2mnt)^x + 2mn \equiv (1 + 2mnt)^z \mod m^2n^2$$

and so

$$2xt + 2 \equiv 2zt \mod mn.$$

It follows from part (i) of Lemma 4.1 that $2 \equiv 0 \bmod 2t$ and so $t = 1$, that is, $c = b + 1$. This is a contradiction. This completes the proof of Proposition 4.8. □

https://doi.org/10.1017/S1446788711001340 Published online by Cambridge University Press

5. Proof of Theorem 1.3

In this final section we will complete the proof of Theorem 1.3. By Propositions 4.3 and 4.8 it suffices to prove that if $c = b + 1$, that is, if $m = n + 1$, then (1.3) has the unique solution $(x, y, z) = (1, 1, 2)$.

When $m = n + 1$ we rewrite (1.3) as

$$(2m^2 - 2m + 1)^x + (2m(m-1))^y = (2m-1)^z, \tag{5.1}$$

where $x, y, z \in \mathbb{N}$, and m is a positive integer such that $m \geq 2$. By Proposition 2.1, it suffices to consider the case where $m \geq 3$.

Let (x, y, z) be a solution of (5.1). Then z is even by Lemma 4.2. We can write $z = 2Z$ for some $Z \geq 1$. First we will prove that $y = 1$. For this proof we consider the cases where m is even and where m is odd separately.

Lemma 5.1. *If m is even, then $y = 1$.*

Proof. Assume that m is even and suppose that $y > 1$. We will observe that this leads to a contradiction.

By Lemma 3.1 and part (ii) of Lemma 4.1 we see that x is even. We can write $x = 2X$ with $X \geq 1$. We observe in a manner similar to that found in the proof of Lemma 4.5 that

$$D = (2m-1)^Z + (2m^2 - 2m + 1)^X = 2^{y-1}m^y,$$
$$E = (2m-1)^Z - (2m^2 - 2m + 1)^X = 2(m-1)^y.$$

It follows that

$$(2m^2 - 2m + 1)^X = (D - E)/2 = 2^{y-2}m^y - (m-1)^y.$$

Since $2^{y-2}m^y$ is divisible by $2m$ and

$$(m-1)^y \equiv (-1)^{y-1}my + (-1)^y \mod 2m,$$

we see that

$$1 \equiv (-1)^y my + (-1)^{y+1} \mod 2m,$$

that is,

$$(-1)^y + 1 \equiv my \mod 2m.$$

From this we may deduce that $(-1)^y \equiv -1 \bmod m$ and so y is odd since $m \geq 3$. However, the above congruence implies that $my \equiv 0 \bmod 2m$ and so $y \equiv 0 \bmod 2$, which is a contradiction. We conclude that $y = 1$. □

Lemma 5.2. *If m is odd, then $y = 1$.*

Proof. Assume that m is odd. Suppose that $y > 1$. We will observe that this leads to a contradiction.

By Lemma 3.1 and part (ii) of Lemma 4.1 we see that x is even. We can write $x = 2X$ for some $X \geq 1$. A similar observation to that found in the proof of Lemma 4.5

https://doi.org/10.1017/S1446788711001340 Published online by Cambridge University Press

allows us to deduce that

$$D = (2m-1)^Z + (2m^2-2m+1)^X = 2m^y,$$
$$E = (2m-1)^Z - (2m^2-2m+1)^X = 2^{y-1}(m-1)^y.$$

If $m = 3$, then

$$5^Z = (D+E)/2 = 3^y + 4^{y-1},$$

which contradicts the result in [14]. If $y = 2$, then $X = Z = 1$ by the first equation above, which is absurd since $x < z$. Hence $m \geq 5$ and $y \geq 3$. Since $D > E$, it follows that

$$1 < \frac{D}{E} = 4\left(\frac{m}{2(m-1)}\right)^y = 4\left(\frac{5}{8}\right)^y \leq 4\left(\frac{5}{8}\right)^3 = \frac{125}{128},$$

which is a contradiction. We conclude that $y = 1$. □

By Lemmas 5.1 and 5.2, we may rewrite (5.1) as

$$(M+1)^x + M = (2M+1)^Z \tag{5.2}$$

for $x, Z \in \mathbb{N}$ where $M = 2m(m-1)$. Note that M is divisible by 4 since the product of two consecutive integers m and $(m-1)$ is even. It suffices to prove that (5.2) has the unique solution $(x, Z) = (1, 1)$.

Let (x, Z) be a solution of (5.2). Taking (5.2) modulo $M+1$ we have $(-1)^Z \equiv -1 \bmod M+1$. Hence Z is odd.

We claim that if $x \leq Z$ or $x+1 \geq 2Z$, then $x = 1$. If $x \leq Z$, then

$$M \leq (2M+1)^x - (M+1)^x \leq (2M+1)^Z - (M+1)^x = M.$$

This implies that $x = Z = 1$. If $x+1 \geq 2Z$, then

$$\begin{aligned}(M+1)^{2Z} &< (M+1)^{2Z} + M(M+1)\\ &\leq (M+1)^{x+1} + M(M+1)\\ &= (M+1)(2M+1)^Z\\ &< (M+1)^{Z+1}2^Z,\end{aligned}$$

and so

$$\left(\frac{M+1}{2}\right)^{Z-1} < 2.$$

Since $M \geq 4$ it follows that $Z = 1$ and so $x = 1$.

In order to obtain a sharp lower bound for x and some necessary conditions on the existence of solutions of (5.2) we prove the following lemma.

LEMMA 5.3. *If $x > 1$, then the following hold.*

(i) $2Z \equiv 1 \bmod M+1$ *and* $x+1 \equiv 2Z \bmod 2M$. *In particular, x is odd.*

(ii) $2M + 5 \leq x$.

https://doi.org/10.1017/S1446788711001340 Published online by Cambridge University Press

Proof. We know that Z is odd. Suppose that $x > 1$. Then $Z < x$ and $x + 1 < 2Z$.

(i) Taking (5.2) modulo $(M+1)^2$, we obtain

$$M \equiv -M^{2Z} \mod (M+1)^2$$

so that

$$M^{2Z-1} + 1 \equiv 0 \mod (M+1)^2.$$

Hence

$$1 - M + M^2 - \cdots + M^{2Z-2} = \frac{M^{2Z-1}+1}{M+1} \equiv 0 \mod M+1$$

and we may deduce that $2Z \equiv 1 \bmod M+1$.

Since M is divisible by 4 we observe that

$$(M+1)^x \equiv \binom{x}{2} M^2 + Mx + 1, \quad (2M+1)^Z \equiv 2MZ + 1 \mod 2M^2.$$

By (5.2), we have

$$\binom{x}{2} M^2 + Mx + 1 + M \equiv 2MZ + 1 \mod 2M^2,$$

and so

$$x + 1 + \binom{x}{2} M \equiv 2Z \mod 2M.$$

Reducing this modulo 4, we obtain $x \equiv 1 \bmod 4$ since Z is odd. It follows from the above congruence that

$$x + 1 \equiv 2Z \mod 2M.$$

(ii) Since $Z \le x - 2$ and $x + 1 < 2Z$ it follows from part (i) that

$$x + 1 + 2M \le 2Z \le 2x - 4$$

and so $2M + 5 \le x$. □

Now we are ready to prove Theorem 1.3.

Proof of Theorem 1.3. Let (x, Z) be a solution of (5.2). By Lemma 3.4 we may deduce that

$$x < 2010 \log(2M+1).$$

Suppose that $x > 1$. We will observe that this leads to a contradiction. By part (ii) of Lemma 5.3 we have

$$2M + 5 \le x < 2010 \log(2M+1).$$

This implies that $M \le 9940$.

https://doi.org/10.1017/S1446788711001340 Published online by Cambridge University Press

It remains to consider values of M such that $M \leq 9940$ and $M \equiv 0 \bmod 4$. Fix such an M. Then, for each x in the above range, we can determine the corresponding Z by using the inequality

$$(2M+1)^Z < (M+1)^{x+1} < (2M+1)^{Z+1},$$

which easily follows from (5.2). Additionally, we can check that such a pair (x, Z) does not satisfy all of the conditions of part (i) of Lemma 5.3. This is a contradiction. We conclude that $x = 1$ and so $Z = 1$. This completes the proof of Theorem 1.3. □

Acknowledgements

The author would like to thank Professors Hirofumi Tsumura, Nobuhiro Terai and Masaki Sudo for their valuable suggestions and many encouragements. He is also grateful to the referee for the comments and suggestions made.

References

[1] Z. F. Cao, 'A note on the Diophantine equation $a^x + b^y = c^z$', *Acta Arith.* **91** (1999), 85–93.
[2] V. A. Dem'janenko, 'On Jeśmanowicz' problem for Pythagorean numbers', *Izv. Vyssh. Uchebn. Zaved. Mat.* **48** (1965), 52–56 (in Russian).
[3] M.-J. Deng and G. L. Cohen, 'A note on a conjecture of Jeśmanowicz', *Colloq. Math.* **86** (2000), 25–30.
[4] B. He and A. Togbé, 'The Diophantine equation $n^x + (n+1)^y = (n+2)^z$ revisited', *Glasg. Math. J.* **51** (2009), 659–667.
[5] L. Jeśmanowicz, 'Several remarks on Pythagorean numbers', *Wiadom. Mat.* **1** (1955/56), 196–202 (in Polish).
[6] W. T. Lu, 'On the Pythagorean numbers $4n^2 - 1$, $4n$ and $4n^2 + 1$', *Acta Sci. Natur. Univ. Szechuan* **2** (1959), 39–42 (in Chinese).
[7] K. Mahler, 'Zur Approximation algebraischer Zahlen I: Über den grössten Primteiler binärer Formen', *Math. Ann.* **107** (1933), 691–730.
[8] M. Mignotte, 'A corollary to a theorem of Laurent–Mignotte–Nesterenko', *Acta Arith.* **86** (1998), 101–111.
[9] T. Miyazaki, 'Jeśmanowicz' conjecture on exponential Diophantine equations', *Funct. Approx. Comment. Math.*, in press.
[10] T. Miyazaki, 'Generalizations of classical results on Jeśmanowicz' conjecture concerning Pythagorean triples', *Diophantine Analysis and Related Fields 2010, AIP Conf. Proc.*, Vol. 1264, Tokyo, Japan, 2010 (American Institute of Physics, Melville, NY, 2010), pp. 41–51.
[11] T. Miyazaki, 'On the conjecture of Jeśmanowicz concerning Pythagorean triples', *Bull. Aust. Math. Soc.* **80** (2009), 413–422.
[12] T. Nagell, 'Sur une classe d'equations exponentielles', *Ark. Mat.* **3** (1958), 569–582.
[13] R. Scott, 'On the equations $p^x - b^y = c$ and $a^x + b^y = c^z$', *J. Number Theory* **44** (1993), 153–165.
[14] W. Sierpiński, 'On the equation $3^x + 4^y = 5^z$', *Wiadom. Mat.* **1** (1955/56), 194–195 (in Polish).

TAKAFUMI MIYAZAKI, Department of Mathematics and Information Sciences,
Tokyo Metropolitan University, 1-1, Minami-Ohsawa, Hachioji,
Tokyo 192-0397, Japan
e-mail: miyazaki-takafumi@ed.tmu.ac.jp

https://doi.org/10.1017/S1446788711001340 Published online by Cambridge University Press