Canad. Math. Bull. Vol. **57** (3), 2014 pp. 495–505
http://dx.doi.org/10.4153/CMB-2014-020-0
© Canadian Mathematical Society 2014

Jeśmanowicz' Conjecture with Congruence Relations. II

Yasutsugu Fujita and Takafumi Miyazaki

Abstract. Let a, b, and c be primitive Pythagorean numbers such that $a^2 + b^2 = c^2$ with b even. In this paper, we show that if $b_0 \equiv \epsilon \pmod{a}$ with $\epsilon \in \{\pm 1\}$ for certain positive divisors b_0 of b, then the Diophantine equation $a^x + b^y = c^z$ has only the positive solution $(x, y, z) = (2, 2, 2)$.

1 Introduction

Let a, b, and c be relatively prime integers with $\min\{a, b, c\} > 1$. Then we consider the exponential Diophantine equation

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

where x, y, and z are positive integers. There are many works on equation (1.1) in the literature. Almost all of them concern the case where a, b, and c also satisfy $a^p + b^q = c^r$ for some other positive integers p, q, and r; in particular, the case $p = q = r = 2$ has interested many researchers. In 1956, Sierpiński [10] considered the case of $(a, b, c) = (3, 4, 5)$, and he showed that equation (1.1) has only the solution $(x, y, z) = (2, 2, 2)$. In the same year, Jeśmanowicz [5] studied some of the cases where a, b, and c are primitive Pythagorean numbers; that is, a, b and c are relatively prime with $a^2 + b^2 = c^2$, and he obtained the same conclusion as Sierpiński. Also, Jeśmanowicz proposed the following problem.

Conjecture 1.1 Let a, b, and c be primitive Pythagorean numbers such that $a^2 + b^2 = c^2$. Then Diophantine equation (1.1) has only the solution $(x, y, z) = (2, 2, 2)$.

This is an unsolved problem in spite of many studies. It is known that if a, b, and c are primitive Pythagorean numbers such that $a^2 + b^2 = c^2$ with b even, then a, b, and c are parameterized as follows:

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

where m and n are relatively prime positive integers of different parities with $m > n$. In what follows, we consider the above expressions.

Received by the editors January 18, 2013; revised February 4, 2014.
Published electronically April 28, 2014.
The first author is partially supported by JSPS KAKENHI Grant Number 25400025.
The second author is supported by JSPS KAKENHI Grant-in-Aid for JSPS Fellows 25 · 484.
AMS subject classification: **11D61**, 11D09.
Keywords: exponential Diophantine equations, Pythagorean triples, Pell equations.

https://doi.org/10.4153/CMB-2014-020-0 Published online by Cambridge University Press

After the work of Jeśmanowicz, Lu [7] proved that Conjecture 1.1 is true if $n = 1$. Dem'janenko [1] showed that Conjecture 1.1 is true if $c = b + 1$, which is equivalent to $m = n + 1$. Their results play important roles in other known results. The second author [9] generalized their results by proving the conjecture to be true if $a \equiv \pm 1 \pmod{b}$ or $c \equiv 1 \pmod{b}$. Recently, the authors [4] generalized a result of [9] and obtained related results. The aim of this paper is to give further related results in this direction.

Throughout this paper, we assume that

$$b_0 \equiv \epsilon \pmod{a}, \tag{1.2}$$

where $b_0 > 1$ is a divisor of b and $\epsilon \in \{\pm 1\}$. We write $b_1 := b/b_0$. The first main result is the following theorem.

Theorem 1.2 *If b_1 has no prime factors congruent to 1 modulo 4, then Conjecture 1.1 is true.*

This is a generalization of [4, Theorem 1.2] concerning the case where b is even, corresponding to $b_1 = 2^r$ with nonnegative integer r. We remark that the condition in the statement of Theorem 1.2 is similar to those due to Deng and Cohen [2]. We also prove the following result.

Theorem 1.3 *Conjecture 1.1 is true if one of the following holds:*

(i) *$m - n$ has a divisor congruent to 3 or 5 modulo 8;*

(ii) *$m + n$ has a divisor congruent to 5 or 7 modulo 8.*

In particular, if a has a prime factor congruent to 5 modulo 8, then Conjecture 1.1 is true.

Some examples of the theorems are given as follows.

$$\begin{aligned}
\epsilon = 1; &\quad m = 2b_1^2,\ n = 2b_1^2 - 2b_1 + 1,\\
\epsilon = 1; &\quad m = 4b_1^3 + 4b_1^2 + 3b_1 + 1,\ n = 4b_1^3 + b_1,\\
\epsilon = -1; &\quad m = 2b_1^2 + 2b_1 + 1,\ n = 2b_1^2,\\
\epsilon = -1; &\quad m = 4b_1^3 + b_1,\ n = 4b_1^3 - 4b_1^2 + 3b_1 - 1,
\end{aligned}$$

where we can take b_1 as any positive integer such that b_1 has no prime factors congruent to 1 modulo 4, or $b_1 \equiv 2 \pmod{4}$, or $b_1 \equiv -\epsilon \pmod{4}$. More generally, one can construct various parametric families of m and n satisfying the assumptions in Theorems 1.2 or 1.3 (see Section 5).

2 Preliminary Considerations

From (1.2) we can write

$$b = \epsilon b_1 + b_1 a t \tag{2.1}$$

https://doi.org/10.4153/CMB-2014-020-0 Published online by Cambridge University Press

with some nonnegative integer t. Since $b_0 > 1$, we find that $b_1 < b$, so $t \geq 1$. Putting $M = m + n$ and $N = m - n$, we see from (2.1) that

$$(M - b_1 N t)^2 - \big((b_1 t)^2 + 1\big) N^2 = 2\epsilon b_1. \tag{2.2}$$

If $t \geq 2$, then the Pell equation $U^2 - ((b_1 t)^2 + 1)V^2 = 2\epsilon b_1$ has no primitive solution (*cf., e.g.,* [3, Lemma 2.3]), and Diophantine equation (2.2) has no solution, since $\gcd(M, N) = 1$. Hence, $t = 1$ and $b_0 = \epsilon + a$. Since b_0 is even, we can write

$$m^2 - n^2 = 2m_0 n_0 - \epsilon, \tag{2.3}$$

where m_0 and n_0 are the positive divisors of m and n, respectively, such that $m_0 n_0 = b_0/2$.

We can assume that $n \geq 2$ by [7] and $n \leq m - 3$ by [1]. Suppose that $\min\{m_0, n_0\} \leq 2$. Then $m_0 n_0 \leq 2\max\{m_0, n_0\} \leq 2m$. Since $m^2 - n^2 \geq m^2 - (m-3)^2 = 6m - 9$, we find from (2.3) that $6m - 9 \leq m^2 - n^2 = 2m_0 n_0 - \epsilon \leq 4m + 1$, which implies that $m \leq 5$, hence $(m, n) = (5, 2)$, particularly, $a = b + 1$, where Conjecture 1.1 is known to be true by [9, Corollary 1]. Thus, we can assume that $m_0, n_0 \geq 3$. By (2.3) we have the congruences

$$m^2 \equiv -\epsilon \pmod{n_0} \quad \text{and} \quad n^2 \equiv \epsilon \pmod{m_0}. \tag{2.4}$$

Lemma 2.1 *Let (x, y, z) be a solution of (1.1). If $\epsilon = 1$, then x and z are even. If $\epsilon = -1$, then z is even.*

Proof Equation (1.1) implies that

$$(-n^2)^x \equiv (n^2)^z \pmod{m} \quad \text{and} \quad (m^2)^x \equiv (m^2)^z \pmod{n}.$$

The assertion now follows from (2.4) and $m_0, n_0 \geq 3$. ∎

In the following sections, we consider the cases of $\epsilon = 1$ and $\epsilon = -1$ separately.

3 The Case $\epsilon = 1$

Let us consider the case $\epsilon = 1$. Let (x, y, z) be a solution of (1.1). By Lemma 2.1, we can write $x = 2X$ and $z = 2Z$ with positive integers X and Z. By [8, Theorem 1.5], we know that both X and Z are odd. We write $(2mn)^y = DE$, where

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

It is easy to see that $\gcd(D, E) = 2$ and $y > 1$. Observe that $D \equiv 0 \pmod 4$ if m is even, and $E \equiv 0 \pmod 4$ if m is odd.

We prepare several lemmas.

Lemma 3.1 *The following congruences hold*:

if m is even, then $D \equiv 0 \pmod{2^{y-1} m_0^y}$ *and* $E \equiv 0 \pmod{2 n_0^y}$,

if m is odd, then $D \equiv 0 \pmod{2 m_0^y}$ *and* $E \equiv 0 \pmod{2^{y-1} n_0^y}$.

https://doi.org/10.4153/CMB-2014-020-0 Published online by Cambridge University Press

Moreover, if b_1 has no prime factors congruent to 1 *modulo* 4*, then*

$$(D,E)=\begin{cases}(2^{y-1}m^y,\ 2n^y) & \text{if } m \text{ is even,}\\ (2m^y,\ 2^{y-1}n^y) & \text{if } m \text{ is odd.}\end{cases}$$

Proof We assume that m is even. By (2.4), we see that

$$E\equiv 2 \pmod{m_0}, \quad D\equiv -2 \pmod{n_0}.$$

Since n_0 is odd, the second congruence implies that n_0 is prime to D. Hence n_0^y divides E. Also, the first congruence tells us that m_0^y divides D if m_0 is odd. If m_0 is even, then, since $2^{2y-1}(m_0/2)^y n_0^y b_1^y = D(E/2)$ and $E/2$ is prime to $m_0/2$ by the first congruence, we observe that $(m_0/2)^y$ divides $D/2$. This proves the first part of the lemma. Similarly, we can obtain the desired congruences in the case where m is odd.

From now on, we assume that b_1 has no prime factors congruent to 1 modulo 4. By [4] we can assume that b_1 is not a power of 2. Take any odd prime factor of b_1, say p. Then p divides m or n. It suffices to show that $D\equiv 0 \pmod p$ if $p \mid m$, and that $E\equiv 0 \pmod p$ if $p\mid n$. Consider the case of $p\mid m$. Suppose that $D\not\equiv 0 \pmod p$. Then $E\equiv 0 \pmod p$. Since $E\equiv n^{2Z}+n^{2X} \pmod p$ and $\gcd(p,n)=1$, we see that

$$n^{2|X-Z|}\equiv -1 \pmod p.$$

This tells us that -1 is a quadratic residue modulo p, which contradicts our assumption that $p\equiv 3 \pmod 4$. Hence the claim is proved. Similarly, we can show that $E\equiv 0 \pmod p$ if $p\mid n$. ∎

Lemma 3.2 *The following congruences hold*:

$$\text{if } m \text{ is even, then} \quad X\equiv Z \pmod{b_0/4},$$
$$\text{if } m \text{ is odd, then} \quad X\equiv Z \pmod{b_0/2}.$$

In particular, if $X\neq Z$, then $|X-Z|\geq (a+1)/4$.

Proof Since $y>1$ and X is odd, we see from Lemma 3.1 that

$$D\equiv n^{2Z}-n^{2X}\equiv 0 \pmod{m_0^2},$$
$$E\equiv m^{2Z}-m^{2X}\equiv 0 \pmod{n_0^2}.$$

The first congruence together with (2.3) yields $(1-b_0)^X\equiv(1-b_0)^Z \pmod{m_0^2}$. Hence,

$$b_0X\equiv b_0Z \pmod{m_0^2}.$$

Also, the second congruence together with (2.3) yields

$$b_0X\equiv b_0Z \pmod{n_0^2}.$$

Since $\gcd(m_0,n_0)=1$ and $m_0n_0=b_0/2$, we have

$$b_0X\equiv b_0Z \pmod{b_0^2/4}.$$

From (2.3) we see that b_0 is divisible by 4 if m is even, and that b_0 is exactly divisible by 2 if m is odd. It follows that $X\equiv Z \pmod{b_0/4}$ if m is even, and $X\equiv Z \pmod{b_0/2}$ if m is odd. The second assertion follows from (2.3). ∎

https://doi.org/10.4153/CMB-2014-020-0 Published online by Cambridge University Press

The following lemma holds under the condition of Theorem 1.3 (*cf.* [2]). From now on, we assume the condition of Theorem 1.2 that b_1 has no prime factors congruent to 1 modulo 4.

Lemma 3.3 *Under the preceding assumption, y is even.*

Proof First, we assume that m is even. By Lemma 3.1, we see that

$$(m^2+n^2)^Z = (D+E)/2 = 2^{y-2}m^y + n^y. \tag{3.1}$$

Taking (3.1) modulo m_0^2, we see from (2.4) that

$$n^y \equiv 1 \pmod{m_0}. \tag{3.2}$$

Suppose that y is odd. We will observe that this leads to a contradiction. Congruences (2.4) and (3.2) together imply that $n \equiv 1 \pmod{m_0}$. Putting $n = 1 + m_0 h$ with a positive integer h, we see from (2.3) that

$$(m + m_0 h)(m/m_0 - h) = 2h + 2n_0.$$

From this we see that the first factor in the left-hand side is a positive divisor of the right-hand side. Since $m > n \geq n_0$ and $m_0 \geq 3$, we find that the second factor in the left-hand side has to be 1; that is,

$$m + m_0 h = 2h + 2n_0, \tag{3.3}$$

$$m/m_0 - h = 1. \tag{3.4}$$

If $n_0 < n$, then $m > n > m_0 h \geq 3h$ and $n_0 \leq n/3$, which contradicts equation (3.3). Hence $n_0 = n$. Since $b_1 = m/m_0 = h+1$ by (3.4) and $n_0 = n = 1 + m_0 h$, we observe that

$$m_0 b_1 = m = 2h + 2(1 + m_0 h) - m_0 h = 2(h+1) + m_0 h = 2b_1 + m_0(b_1 - 1),$$

so $m_0 = 2b_1$. Therefore, we find that $(m,n) = (2b_1^2,\, 2b_1^2 - 2b_1 + 1)$. We will consider the cases where b_1 is even and b_1 is odd separately.

Suppose that b_1 is even. Then, $m \equiv 0 \pmod{2m_0}$, which together with (2.3) yields $n^2 \equiv 1 \pmod{2m_0}$. By (3.1) we have $n^y \equiv 1 \pmod{2m_0}$. Since y is odd, we obtain $n \equiv 1 \pmod{2m_0}$. It follows from $m_0 = 2b_1$ and $n = 2b_1^2 - 2b_1 + 1$ that $b_1 \equiv 1 \pmod 2$, which contradicts the evenness of b_1.

Suppose that b_1 is odd. Then $m \equiv 2 \pmod 4$, so $c = m^2 + n^2 \equiv 5 \pmod 8$. Taking $c^Z = 2^{y-2}m^y + n^y$ modulo 8, we find that $n \equiv 5 \pmod 8$, since both $y\ (\geq 3)$ and Z are odd. This implies that $b_1 \equiv 3 \pmod 4$. Then $m + n \equiv 4b_1^2 - 2b_1 + 1 \equiv 7 \pmod 8$. Taking (1.1) modulo $m+n$, we find that $(-2m^2)^y \equiv (2m^2)^{2Z} \pmod{m+n}$. This tells us that -2 is a quadratic residue modulo $m+n$, which contradicts $m+n \equiv 7 \pmod 8$. Therefore, y is even.

Second, we assume that n is even. Taking $(m^2+n^2)^Z = m^y + 2^{y-2}n^y$ modulo n_0, we see from (2.4) that $m^y \equiv -1 \pmod{n_0}$. If y is odd, then $m \equiv \pm 1 \pmod{n_0}$, and hence $m^2 \equiv 1 \pmod{n_0}$, which contradicts $m^2 \equiv -1 \pmod{n_0}$ and $n_0 \geq 3$. Therefore, y is even. ∎

https://doi.org/10.4153/CMB-2014-020-0 Published online by Cambridge University Press

By Lemma 3.3, we can write $y = 2Y$ with a positive integer Y. Now we are ready to prove the theorems. Since $\{a^X, b^Y, c^Z\}$ forms a primitive Pythagorean triple, we can write

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

where k and l are relatively prime positive integers of different parities with $k > l$. Since $b < c < a^2$ and $a^X < c^Z < b^{2Y}$, we find that

$$|X - Z| < Z < 2Y. \tag{3.5}$$

Since $(k + l)(k - l) = a^X$ and $\gcd(k + l, k - l) = 1$, we can write

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

for some relatively prime positive odd integers u and v satisfying $u > v$ and $uv = a$. Then we see that

$$b^Y = 2kl = \frac{u^{2X} - v^{2X}}{2} = \frac{u^2 - v^2}{2} w,$$

where $w = (u^{2X} - v^{2X})/(u^2 - v^2)$ is an odd integer, since u, v, and X are odd. It follows from the above equation that

$$Y \nu_2(b) = \nu_2(u^2 - v^2) - 1 = \nu_2(u \pm v)$$

holds for the proper sign for which $u \pm v \equiv 0 \pmod 4$, where ν_2 is the 2-adic valuation normalized by $\nu_2(2) = 1$. Since $u \pm v \leq u + v \leq uv + 1 = a + 1$, we find that

$$Y = \frac{\nu_2(u \pm v)}{\nu_2(b)} \leq \frac{\log(a + 1)}{2 \log 2}.$$

It follows from (3.5) that

$$|X - Z| \leq 2Y - 2 \leq \frac{\log(a + 1)}{\log 2} - 2.$$

Since the right-most number is less than $(a + 1)/4$, we can conclude that $X = Z$ by Lemma 3.2. Since X is odd, we see that

$$b^{2Y} = DE = c^{2X} - a^{2X} = b^2 w',$$

where $w' = (c^{2X} - a^{2X})/(c^2 - a^2)$ is an odd integer, since a, c, and X are odd. Hence, $\nu_2(b^{2Y}) = \nu_2(b^2)$. This implies that $Y = 1$, so $X = Z = 1$ by (3.5). This completes the proof of the theorems for the case of $\epsilon = 1$.

4 The Case $\epsilon = -1$

Let (x, y, z) be a solution of (1.1). By Lemma 2.1, we know that z is even. It suffices to show that both x and y are even. Indeed, if so, then we can prove that $x = y = z = 2$ in a similar manner to the preceding section. We will consider the cases where m is even and where m is odd separately.

First, we assume that m is even. Reducing equation (1.1) modulo 4, we find that $(-1)^x \equiv 1 \pmod 4$; that is, x is even. Then we define D and E as in the preceding section, and we can show the same assumptions as Lemma 3.1. Hence Theorem 1.3 follows from this. We assume the condition of Theorem 1.2. Since $(D, E) = (2^{y-1}m^y, 2n^y)$, taking $(m^2 + n^2)^Z = 2^{y-2}m^y + n^y$ modulo m_0, we see from (2.4) that

https://doi.org/10.4153/CMB-2014-020-0 Published online by Cambridge University Press

$n^y \equiv -1 \pmod{m_0}$. If y is odd, then $n \equiv \pm 1 \pmod{m_0}$ by (2.4), and hence $n^2 \equiv 1 \pmod{m_0}$, which contradicts (2.4) and $m_0 \geq 3$. Therefore, y is even.

Second, we assume that m is odd. We write

$$m = 2^{\beta} j + e, \quad n = 2^{\alpha} i,$$

where α, β, i, j are positive integers with i, j odd, and with $\alpha \geq 1$, $\beta \geq 2$ and $e \in \{\pm 1\}$. In order to show the evenness of x, we use the following lemma (*cf.* [9, Lemma 2.1]).

Lemma 4.1 *With the above notation, we assume that* $2\alpha \neq \beta + 1$. *Let* (x, y, z) *be a solution of* (1.1). *If* $y > 1$, *then* $x \equiv z \pmod 2$.

We claim that $2\alpha \neq \beta + 1$. We can assume that $\alpha \geq 2$. By equation (2.3), we have

$$\begin{aligned}\beta + 1 &= \nu_2(m^2 - 1) = \nu_2(\, n^2 + 2m_0 n_0\,) = \nu_2(2n_0) + \nu_2\Big(\frac{n^2}{2n_0} + m_0\Big) \\ &= \nu_2(n_0) + 1 \leq \nu_2(n) + 1 = \alpha + 1 < 2\alpha.\end{aligned}$$

Hence the claim is proved. Next, we show that $y > 1$. Suppose that $y = 1$. We will show that this leads to a contradiction. Equation (1.1) is now

$$a^x + b = c^z. \tag{4.1}$$

This is a Pillai equation. We can easily show that $x \geq 4$ and $x > z > 1$. Also, x and z are relatively prime. Indeed, if d is a common divisor of them, then we see from (4.1) that b is divisible by $(c^{z/d})^{d-1} + a^{x/d}(c^{z/d})^{d-2} + \cdots + (a^{x/d})^{d-1}$, which is greater than c $(> b)$ if $d > 1$.

Since

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

we see that

$$z \log c - x \log a < \frac{b}{a^x}. \tag{4.2}$$

The left-hand side of (4.2) is a nonzero linear form in two logarithms with $x = \max\{x, z\}$. Baker's theory gives us lower estimates of its absolute value such as $1/x^{\mathcal{C}}$, where $\mathcal{C}$ is a positive constant depending only on a and c. In order to observe this we prepare some notation as follows.

For an algebraic number α of degree d over the field of rational numbers $\mathbb{Q}$, we define as usual the absolute logarithmic height of α by

$$\mathrm{h}(\alpha) = \frac{1}{d}\Big(\log c_0 + \sum_{i=1}^{d} \log \max\big\{\, 1, |\alpha^{(i)}|\big\}\,\Big),$$

where c_0 (> 0) is the leading coefficient of the minimal polynomial of α over the ring of rational integers, and $\alpha^{(1)}, \alpha^{(2)}, \ldots, \alpha^{(d)}$ are the conjugates of α in the field of complex numbers.

Let α_1 and α_2 be two nonzero algebraic numbers with $|\alpha_1| \geq 1$ and $|\alpha_2| \geq 1$, and let $\log \alpha_1$ and $\log \alpha_2$ be any determination of their logarithms. We consider the linear

https://doi.org/10.4153/CMB-2014-020-0 Published online by Cambridge University Press

form in two logarithms

$$\Lambda = \beta_2 \log \alpha_2 - \beta_1 \log \alpha_1,$$

where β_1 and β_2 are positive integers. Put

$$D = [\mathbb{Q}(\alpha_1, \alpha_2) : \mathbb{Q}] / [\mathbb{R}(\alpha_1, \alpha_2) : \mathbb{R}],$$

where we denote by $\mathbb{R}$ the field of real numbers. Define

$$b' = \frac{\beta_1}{D \log A_2} + \frac{\beta_2}{D \log A_1},$$

where $A_1 > 1$ and $A_2 > 1$ are real numbers such that

$$\log A_i \geq \max\big\{ \mathrm{h}(\alpha_i),\ |\log \alpha_i|/D,\ 1/D \big\} \quad (i = 1, 2).$$

We choose to use a result due to Laurent [6, Corollary 2; $(m, C_2) = (10, 25.2)$].

Proposition 4.2 *With the above notation, suppose that $\alpha_1, \alpha_2, \log \alpha_1, \log \alpha_2$ are real and positive. If α_1 and α_2 are multiplicatively independent, then we have the lower estimate*

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

In order to apply Proposition 4.2 to the case of $\Lambda = z \log c - x \log a$ (> 0), we set $(\alpha_1, \alpha_2) = (a, c)$ and $(\beta_1, \beta_2) = (x, z)$. Then $D = 1$, $\mathrm{h}(a) = \log a$, and $\mathrm{h}(c) = \log c$. We can take $A_1 = a$ and $A_2 = c$. Proposition 4.2 tells us that

$$\log \Lambda > -25.2 \Big(\max\Big\{ \log\Big(\frac{x}{\log c} + \frac{z}{\log a} \Big) + 0.38,\ 10 \Big\} \Big)^2 \log a \, \log c.$$

Combining this with (4.2), we find that

$$\log b - x \log a > -25.2 \Big(\max\Big\{ \log\Big(\frac{x}{\log c} + \frac{z}{\log a} \Big) + 0.38,\ 10 \Big\} \Big)^2 \log a \, \log c,$$

or

$$\frac{x}{\log c} < \frac{\log b}{\log a \, \log c} + 25.2 \Big(\max\Big\{ \log\Big(\frac{x}{\log c} + \frac{z}{\log a} \Big) + 0.38,\ 10 \Big\} \Big)^2.$$

Since $a \geq 3$, $b < c$ and $c^z = a^x + b < a^x + a^2 \leq 2a^x$, we see that

$$\frac{x}{\log c} < 1 + 25.2 \Big(\max\Big\{ \log\Big(\frac{2x}{\log c} + \frac{\log 2}{\log c} \Big) + 0.38,\ 10 \Big\} \Big)^2.$$

This implies that

$$x < 2521 \log c. \tag{4.3}$$

Then, since

$$x - z < x - \frac{\log a}{\log c} x = \frac{\log(c/a)}{\log c} x,$$

we have

$$x - z < 2521 \log(c/a). \tag{4.4}$$

On the other hand, by taking equation (4.1) modulo m_0^2, we find that $(-n^2)^x + b \equiv n^{2z} \pmod{m_0^2}$, which together with (2.3) yields $b_0 x + b \equiv b_0 z \pmod{m_0^2}$.

https://doi.org/10.4153/CMB-2014-020-0 Published online by Cambridge University Press

Also, taking equation (4.1) modulo n_0^2, we have $b_0x + b \equiv b_0z \pmod{n_0^2}$. Since $\gcd(m_0, n_0) = 1$ and $m_0n_0 = b_0/2$, we have

$$b_0x + b \equiv b_0z \pmod{b_0^2/4}.$$

Since $x > z$ and $b_0 = a - 1$, it follows from the above congruence that

$$x - z \geq \frac{b_0}{4} - \frac{b}{b_0} = \frac{a-1}{4} - \frac{b}{a-1}.$$

Here, we can assume that $m \geq n+7$. Since, by [2], if $m - n > 1$ (by [1]) has a divisor congruent to ± 3 modulo 8, then y is even. Since

$$\frac{b}{a} = \frac{2mn}{m^2 - n^2} \leq \frac{2m(m-7)}{14m - 49},$$

we see that (4.4) gives

$$\begin{aligned}\frac{7m-25}{2} \leq \frac{a-1}{4} &< 2521\log(c/a) + \frac{b}{a-1}\\ &= \frac{2521}{2}\log\Bigl(1 + (b/a)^2\Bigr) + \frac{b/a}{1-1/a}\\ &\leq \frac{2521}{2}\log\Bigl(1 + \Bigl(\frac{2m(m-7)}{14m-49}\Bigr)^2\Bigr) + \frac{m(m-7)}{7m-25}.\end{aligned}$$

This implies that $m \leq 4926$. On the other hand, since

$$\frac{b}{a^x} \leq \frac{b}{a^4} \leq \frac{2m(m-7)}{(14m-49)^4} < \frac{1}{5042},$$

we see from (4.2) and (4.3) that

$$\Bigl|\frac{\log a}{\log c} - \frac{z}{x}\Bigr| < \frac{b}{xa^x \log c} < \frac{2521(b/a^x)}{x^2} < \frac{1}{2x^2}.$$

Therefore, $\frac{z}{x}$ is a convergent in the simple continued fraction expansion of $\frac{\log a}{\log c}$. Hence we can write $\frac{z}{x} = \frac{p_s}{q_s}$, which is the s-th such convergent. Since $\gcd(x, z) = 1$, we see that $x = q_s$ and $z = p_s$. Remark that $q_s \geq 4$. By a well-known fact on the continued fraction expansion, we find that

$$\Bigl|\frac{\log a}{\log c} - \frac{p_s}{q_s}\Bigr| > \frac{1}{(\alpha_{s+1} + 2)q_s^2},$$

where α_{s+1} is the $(s+1)$-th partial quotient to $\frac{\log a}{\log c}$. It follows that

$$\alpha_{s+1} + 2 > \frac{xa^x \log c}{bq_s^2} = \frac{a^{q_s} \log c}{bq_s}.$$

For each of the pairs (m, n) under consideration, we can numerically check that the inequality

$$\alpha_{s+1} + 2 > \frac{a^{q_s} \log c}{bq_s}$$

does not hold for any s satisfying $4 \leq q_s < 2521 \log c$. This is a contradiction. Therefore, $y > 1$.

It follows from Lemma 4.1 that x is even. It remains for us to show the evenness of y. We assume the condition of Theorem 1.2. As in the preceding section, we

https://doi.org/10.4153/CMB-2014-020-0 Published online by Cambridge University Press

define D and E, and we can show that $(D,E)=(2m^y,2^{y-1}n^y)$. Taking $(m^2+n^2)^Z=m^y+2^{y-2}n^y$ modulo n_0, we see from (2.4) that $m^y\equiv 1 \pmod{n_0}$. Suppose that y is odd. We will show that this leads to a contradiction. Congruences (2.4) and (3.2) together imply that $m\equiv 1 \pmod{n_0}$. Putting $m=1+n_0h$ with a positive integer h, we see from (2.3) that

$$(n_0h+n)(h-n/n_0)=2(m_0-h).$$

If $m_0=h$, then $h=n/n_0$, so $m_0=n/n_0$, which is absurd, since $\gcd(m,n)=1$ and $m_0>1$. Hence the value of the right-hand side is nonzero. Since $h\le n/n_0$ implies $m=1+n_0h\le 1+n$, we have $h\le n/n_0$ and $m_0>h$. Hence we see that the second factor in the left-hand side has to be 1; that is,

$$n_0h+n=2(m_0-h), \tag{4.5}$$

$$h-n/n_0=1. \tag{4.6}$$

If $m_0<m$, then $m_0\le m/3$, so equation (4.5) implies $m\le 2(m_0-h)<2m_0\le(2/3)m$, which is a contradiction. Hence, $m_0=m$. Using this together with (4.6), similarly to Lemma 3.3, we can observe that $(m,n)=(2b_1^2+2b_1+1,2b_1^2)$, which yields a contradiction. To sum up, we have completed the proof of the theorems for the case $\epsilon=-1$. ■

5 Examples

In this final section, we will explain how to find examples of m and n satisfying the assumptions of our results. As we observed in Section 2, m and n satisfy Pell equation (2.2) with $t=1$; that is,

$$U^2-(b_1^2+1)V^2=2\epsilon b_1, \tag{5.1}$$

where $U=m+n-b_1(m-n)$ and $V=m-n$. It is clear that (5.1) has the two classes of solutions

$$U+V\sqrt{b_1^2+1}=\left(U_0+V_0\sqrt{b_1^2+1}\right)\left(2b_1^2+1+2b_1\sqrt{b_1^2+1}\right)^l \tag{5.2}$$

with nonnegative integer l, where

$$(U_0,V_0)=\begin{cases}(b_1+1,\pm 1) & \text{if } \epsilon=1,\\ (\pm(b_1-1),1) & \text{if } \epsilon=-1.\end{cases} \tag{5.3}$$

Now Theorems 1.2 and 1.3 immediately imply the following.

Corollary 5.1 *Conjecture 1.1 is true if one of the following holds:*

(i) *b_1 has no prime factors congruent to 1 modulo 4, and U, V satisfy (5.2) with a positive integer l and with (U_0,V_0) satisfying (5.3).*

(ii) *Either $b_1\equiv 2 \pmod 4$ or $b_1\equiv -\epsilon \pmod 4$, and U, V satisfy (5.2) with a positive odd integer l and with (U_0,V_0) satisfying (5.3).*

https://doi.org/10.4153/CMB-2014-020-0 Published online by Cambridge University Press

Proof It is obvious from Theorem 1.2 that if (i) holds, then Conjecture 1.1 is true. Consider the case of (ii). By (5.2), we have $V = v_l$, where

$$v_0 = V_0,\ v_1 = (2b_1^2+1)V_0 + 2b_1U_0,\ v_{l+2} = 2(2b_1^2+1)v_{l+1} - v_l.$$

Equation (5.3) shows that if $b_1 \equiv 2 \pmod 4$ and l is odd, then $v_l \equiv V_0 + 4 \pmod 8$, in other words, $m - n = V = v_l \equiv \pm 5 \pmod 8$. Similarly, if $b_1 \equiv -\epsilon \pmod 4$ and l is odd, then we see that $m - n = v_l \equiv 3V_0 \equiv \pm 3 \pmod 8$. In any case, one can conclude from Theorem 1.3 that Conjecture 1.1 is true. ■

The examples in the first section are given by setting

$$(\epsilon, U_0, V_0, l) = (1, b_1+1, -1, 1), (1, b_1+1, 1, 1), (-1, 1-b_1, 1, 1), (-1, b_1-1, 1, 1).$$

Acknowledgment The author would like to thank the anonymous referee for helpful comments.

References

[1] V. A. Dem'janenko, *On Jeśmanowicz' problem for Pythagorean numbers.* (Russian) Izv. Vyssh. Ucebn. Zaved. Matematika **1965**, no. 5(48), 52–56.

[2] M. Deng and G. L. Cohen, *A note on a conjecture of Jeśmanowicz.* Colloq. Math. **86**(2000), no. 1, 25–30.

[3] Y. Fujita, *The non-extensibility of $D(4k)$-triples $\{1, 4k(k-1), 4k^2+1\}$ with $|k|$ prime.* Glas. Mat. Ser. III **41(61)**(2006), no. 2, 205–216. http://dx.doi.org/10.3336/gm.41.2.03

[4] Y. Fujita and T. Miyazaki, *Jeśmanowicz' conjecture with congruence relations.* Colloq. Math. **128**(2012), no. 2, 211–222. http://dx.doi.org/10.4064/cm128-2-6

[5] L. Jeśmanowicz, *Several remarks on Pythagorean numbers.* (Polish) Wiadom. Mat. **1**(1955/1956), 196–202.

[6] M. Laurent, *Linear forms in two logarithms and interpolation determinants II.* Acta Arith. **133**(2008), no. 4, 325–348. http://dx.doi.org/10.4064/aa133-4-3

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

[8] T. Miyazaki, *Jeśmanowicz' conjecture on exponential Diophantine equations.* Funct. Approx. Comment. Math. **45**(2011), part 2, 207–229. http://dx.doi.org/10.7169/facm/1323705814

[9] ———, *Generalizations of classical results on Jeśmanowicz' conjecture concerning Pythagorean triples.* J. Number Theory **133**(2013), no. 2, 583–595. http://dx.doi.org/10.1016/j.jnt.2012.08.018

[10] W. Sierpiński, *On the equation $3^x + 4^y = 5^z$.* (Polish) Wiadom. Mat. **1**(1955/1956), 194–195.

Department of Mathematics, College of Industrial Technology, Nihon University, 2-11-1 Shin-ei, Narashino, Chiba, Japan
e-mail: fujita.yasutsugu@nihon-u.ac.jp

Department of Mathematics, College of Science and Technology, Nihon University 1-8-14 Kanda-Surugadai, Chiyoda-ku, Tokyo 101-8308, Japan
e-mail: miyazaki-takafumi@math.cst.nihon-u.ac.jp

https://doi.org/10.4153/CMB-2014-020-0 Published online by Cambridge University Press