Journal of Number Theory 141 (2014) 184–201

Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

Generalizations of classical results on Jeśmanowicz' conjecture concerning Pythagorean triples II

Takafumi Miyazaki[a,*], Pingzhi Yuan[b], Danyao Wu[b]

[a] *Department of Mathematics, College of Science and Technology, Nihon University, 1-8-14 Kanda-Surugadai, Chiyoda-ku, Tokyo 101-8308, Japan*
[b] *School of Mathematics, South China Normal University, Guangzhou 510631, PR China*

ARTICLE INFO

Article history:
Received 9 July 2013
Received in revised form 28 January 2014
Accepted 28 January 2014
Available online 25 March 2014
Communicated by David Goss

MSC:
primary 11D61
secondary 11J86, 11D09

Keywords:
Pythagorean triples
Jeśmanowicz' conjecture
Exponential Diophantine equations

ABSTRACT

A conjecture proposed by Jeśmanowicz on Pythagorean triples states that for any fixed primitive Pythagorean triple (a, b, c) such that $a^2 + b^2 = c^2$, the Diophantine equation $a^x + b^y = c^z$ has only the trivial solution in positive integers x, y and z. In this paper we establish the conjecture for the case where b is even and either a or c is congruent to ± 1 modulo the product of all prime factors of b.

1. Introduction

A triple of positive integers (a, b, c) is called a Pythagorean triple if $a^2 + b^2 = c^2$, and primitive if a, b and c are co-prime. The following is one of the major unsolved problems about Pythagorean triples.

* Corresponding author.
E-mail addresses: miyazaki-takafumi@math.cst.nihon-u.ac.jp (T. Miyazaki), yuanpz@scnu.edu.cn (P. Yuan), wudanrao@163.com (D. Wu).

http://dx.doi.org/10.1016/j.jnt.2014.01.011
0022-314X/

Conjecture 1. *For any fixed primitive Pythagorean triple (a, b, c) such that $a^2 + b^2 = c^2$, the Diophantine equation*

$$a^x + b^y = c^z \tag{1}$$

has only the trivial solution in positive integers x, y and z.

In 1956, Sierpiński [S] considered (1) for $(a, b, c) = (3, 4, 5)$, and he showed that it has no positive integer solutions other than $(x, y, z) = (2, 2, 2)$. In the same year, Jeśmanoiwcz [J] obtained similar results for some other Pythagorean triples, and he proposed the above problem. Up to the present, Conjecture 1 has been proved to be true under various conditions, but it is still open (see for example [M2] and its references).

It is well-known that for any primitive Pythagorean triple (a, b, c) such that $a^2 + b^2 = c^2$, we can write

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

where m and n are co-prime positive integers of different parities with $m > n$. We will always consider the above expressions. It is important to examine the potential conditions on m and n, such as $n = 1$ and $m = n + 1$. Indeed, these play important roles in many studies in the literature. In these cases, Conjecture 1 is known to be true by the works of Lu [Lu] for $n = 1$ and Dem'janenko [D] for $m = n + 1$. Recently, the first author [M2] generalized their results by proving the conjecture to be true if $a \equiv \pm 1 \pmod{b}$ or $c \equiv 1 \pmod{b}$. In this paper, we extend this result to more general cases.

For any positive integer N, we denote the exact exponent of 2 in N by $\mathrm{ord}_2(N)$, and the product of all prime factors of N by $\mathrm{rad}(N)$. In what follows, we put

$$A \in \{a, c\}, \quad \epsilon \in \{1, -1\}.$$

The main result of this paper is the following.

Theorem 1. *If $A \equiv \epsilon \pmod{b/2^{\mathrm{ord}_2(b)}}$, then Conjecture 1 is true.*

This is a generalization of the results in [M2]. It is a consequence of a result (Theorem 2 below) concerning more general cases. We shall be concerned with the following case:

$$A \equiv \epsilon \pmod{b_0}, \tag{2}$$

where b_0 is a positive divisor of b which is divisible by $\mathrm{rad}(b)$. The second result is the following.

Theorem 2. *Assume that Conjecture 1 is true under assumption (2). Moreover, if* $\epsilon = -1$, $n \geqslant 4$ *is a power of* 2 *and* $m \equiv \pm 1 + n^2/2 \pmod{n^2}$, *then assume that*

$$b_0 > \frac{4m}{\mathrm{p}(m)},$$

where $\mathrm{p}(m)$ *is the least prime factor of* m. *Then Conjecture 1 is true under assumption (2) with the modulo replaced by* $b_0/2$.

Theorem 1 follows from the results in [M2] and Theorem 2 with $b_0 = b/2^r$ for $r \in \{0, 1, 2, \ldots, \mathrm{ord}_2(b) - 1\}$.

The organization of this paper is the following. In the next section, we prove a proposition which plays a crucial role in the proof of our results. In Section 3, we prepare some lemmas which are useful to examine the parities of solutions. In Section 4, we prove Theorem 2 for the case $\epsilon = 1$. In Section 5, we give a sufficient condition to ensure $y > 1$. In Section 6, we prove Theorem 2 for the case $\epsilon = -1$. In the final section, we give some examples of Theorem 1 and make some remarks.

The paper is mainly devoted to the proof of Theorem 2. Although the proof proceeds along a similar line as [M2], we need to treat several parts by more careful or sophisticated observations, in particular, we are not able to use the theory of Pellian equations. The first step is to show that for any solution, both x and z are even. This is reduced to the problem of analyzing the case where $\epsilon = -1$ and n is a power of 2. Under the assumption that b_0 is suitably large, which is ensured from our assumption on b_0, we can deal with this case by an application of the theory of linear forms in logarithms of algebraic numbers. As a result, together with the fact that b_0 is divisible by $\mathrm{rad}(b)$, we obtain some non-trivial (desired) equations. The second step is to show that y is even. This can be reduced to the previous cases. We can deal with this by applying Baker's method to the non-trivial equations. Finally, using an idea from the work of Deng and Cohen [DC] to the non-trivial equations, we obtain the desired conclusion, where the method is another treatment of the results in [FM] and [M2].

2. An important proposition

The proof of Theorem 2 is mainly divided into two parts. The first part is to prove that x, y and z are even, and also that some non-trivial equations hold (see (3), (4) below). The second part is to solve such non-trivial equations. The first part will be done in Sections 4 and 6 for the cases $(A, \epsilon) = (a, 1), (c, 1), (a, -1), (c, -1)$, respectively.

In this section, we complete the second part, where we do not need assumption (2). Indeed, we prove the following proposition.

Proposition 1. *Let* m *and* n *be co-prime positive integers of different parities with* $m > n$.

(i) *Assume that m is even. Then the system of equations*

$$\begin{cases} (m^2+n^2)^Z + (m^2-n^2)^X = 2^{2Y-1}m^{2Y}, \\ (m^2+n^2)^Z - (m^2-n^2)^X = 2n^{2Y} \end{cases} \tag{3}$$

has only the trivial solution $X = Y = Z = 1$ in positive integers X, Y and Z.

(ii) *Assume that n is even. Then the system of equations*

$$\begin{cases} (m^2+n^2)^Z + (m^2-n^2)^X = 2m^{2Y}, \\ (m^2+n^2)^Z - (m^2-n^2)^X = 2^{2Y-1}n^{2Y} \end{cases} \tag{4}$$

has only the trivial solution $X = Y = Z = 1$ in positive integers X, Y and Z.

Proof. It is easy to observe that if (3) or (4) has a solution, then taking the equations modulo $m^2 - n^2$ yields the congruence

$$2^{2Y-2} \equiv 1 \pmod{m^2 - n^2}. \tag{5}$$

(i) Let (X, Y, Z) be a positive integer solution of (3). From (3) we see

$$(m^2-n^2)^X = (2^{Y-1}m^Y + n^Y)(2^{Y-1}m^Y - n^Y).$$

Since $\gcd(2m, n) = 1$, the factors on the right-hand side are co-prime. Hence, we can write

$$2^{Y-1}m^Y + n^Y = s^X, \qquad 2^{Y-1}m^Y - n^Y = t^X$$

for some positive odd integers s and t with $s > t$ and $st = m^2 - n^2$. Since $m > n$ and $s \geqslant t + 2$, we find

$$s^X + t^X = 2^Y m^Y > 2^{Y-1} \cdot 2n^Y = 2^{Y-1}(s^X - t^X),$$

so

$$\begin{aligned}(2^{Y-1}+1)t^X &> (2^{Y-1}-1)s^X \\ &\geqslant (2^{Y-1}-1)(t+2)^X \\ &\geqslant (2^{Y-1}-1)(t^X + 2Xt^{X-1}).\end{aligned}$$

It follows $t > (2^{Y-1} - 1)X$, and in particular,

$$t \geqslant 2^{Y-1}.$$

From this we see that the left-hand side of (5) is at most $t^2 < st = m^2 - n^2$, so (5) is an equality, hence $Y = 1$, and $X = Z = 1$ by the first equation in (3).

(ii) First, we assume $n \equiv 2 \pmod 4$. Note that $m^2 \pm n^2 \equiv 5 \pmod 8$. Let (X, Y, Z) be a positive integer solution of (4). Then taking the equations in (4) modulo 8, we find

$$5^X \equiv 1 - 2^{2Y-2} n^{2Y}, \qquad 5^Z \equiv 1 + 2^{2Y-2} n^{2Y} \pmod 8.$$

Suppose $Y \geqslant 2$. Then $5^X \equiv 5^Z \equiv 1 \pmod 8$ so that both X and Z are even. This gives rise to a non-trivial solution of the Diophantine equation $S^4 + T^2 = U^4$, indeed, we find from (4) that

$$\left(m^2 - n^2\right)^{4(X/2)} + (2mn)^{2Y} = \left(m^2 + n^2\right)^{4(Z/2)}.$$

This is a contradiction. Therefore, $Y = 1$, and $X = Z = 1$ by the first equation in (4).

Second, we assume $n \equiv 0 \pmod 4$. Let (X, Y, Z) be a positive integer solution of (4). From (4) we see that

$$\left(m^2 - n^2\right)^X = \left(m^Y + 2^{Y-1} n^Y\right)\left(m^Y - 2^{Y-1} n^Y\right).$$

Since $\gcd(m, 2n) = 1$, the factors on the right-hand side are co-prime. Hence, we can write

$$m^Y + 2^{Y-1} n^Y = s^X, \qquad m^Y - 2^{Y-1} n^Y = t^X$$

for some co-prime positive odd integers s and t with $s > t$ and $st = m^2 - n^2$. Since $s^X - t^X = (2n)^Y$ and $s - t \equiv 0 \pmod 4$ (by $st = m^2 - n^2 \equiv 1 \pmod 4$), it follows from [R, p. 11; P1.2] that

$$\operatorname{ord}_2(s - t) + \operatorname{ord}_2(X) = \left(1 + \operatorname{ord}_2(n)\right)Y.$$

From the equations in (4) we see that

$$2m^X < 2\left(m^2 - n^2\right)^X < \left(m^2 + n^2\right)^Z + \left(m^2 - n^2\right)^X = 2m^{2Y},$$

and so $X < 2Y$. These together with $n \equiv 0 \pmod 4$ imply

$$\operatorname{ord}_2(s - t) = \left(1 + \operatorname{ord}_2(n)\right)Y - \operatorname{ord}_2(X) \geqslant 3Y - \frac{\log X}{\log 2} \geqslant 2Y,$$

so

$$s - t \equiv 0 \pmod{2^{2Y}}.$$

From this we see that the left-hand side of (5) is less than $2^{2Y} \leqslant s - t < st = m^2 - n^2$, and so (5) is an equality. Hence $Y = 1$ and $X = Z = 1$. $\square$

3. Parities of solutions

In the study of Conjecture 1, it is very important to examine the parities of solutions of the equation

$$\left(m^2-n^2\right)^x+(2mn)^y=\left(m^2+n^2\right)^z \tag{6}$$

in positive integers x, y and z, where m and n are fixed co-prime positive integers of different parities with $m>n$. By [Lu], we may assume $n>1$. We use the following notation from [M,M2]. We define integers $\alpha \geqslant 1$, $\beta \geqslant 2$, $e \in \{1,-1\}$, and positive odd integers i, j as follows:

$$\begin{cases} m=2^\alpha i, & n=2^\beta j+e \quad \text{if } m \text{ is even,} \\ m=2^\beta j+e, & n=2^\alpha i \quad \text{if } m \text{ is odd.} \end{cases} \tag{7}$$

With the notation in (7), we have the following lemmas.

Lemma 1. *Assume $\alpha>1$, $\alpha \neq \beta$ and $2\alpha \neq \beta+1$. Let (x, y, z) be a solution of (6). Then we have $x \equiv z \pmod 2$.*

Lemma 2. *Assume $2\alpha \neq \beta+1$. Let (x, y, z) be a solution of (6). Suppose $y>1$. Then we have $x \equiv z \pmod 2$.*

Lemma 3. *Let (x, y, z) be a solution of (6). Assume that both x and z are even. Write $X=x/2$ and $Z=z/2$. Then both X and Z are odd.*

Lemmas 1, 2 and 3 are Lemma 2.4(i), Lemma 2.4(ii) and Theorem 1.5(i) from [M], respectively.

Lemma 4. *We have*

$$c-1 \equiv 0 \quad \left(\bmod 2^{\min\{2\alpha, \beta+1\}}\right)$$

and

$$\begin{cases} a+1 \equiv 0 \quad \left(\bmod 2^{\min\{2\alpha, \beta+1\}}\right) & \text{if } m \text{ is even,} \\ a-1 \equiv 0 \quad \left(\bmod 2^{\min\{2\alpha, \beta+1\}}\right) & \text{if } m \text{ is odd.} \end{cases}$$

Proof. This easily follows from substituting (7) into (6). $\square$

4. The case $\epsilon = 1$

In this section, we prove Theorem 2 for the case $\epsilon=1$. We consider the cases $A=a$ and $A=c$ separately.

4.1. The case $(A, \epsilon) = (a, 1)$

Assume that Conjecture 1 is true under assumption (2) with $A = a$ and $\epsilon = 1$. Note that b_0 is even. Now, we assume $a \equiv 1 \pmod{b_0/2}$. Write $a = 1 + (b_0/2)t$ with a positive integer t. Since Conjecture 1 is now ensured to be true if $a \equiv 1 \pmod{b_0}$, we may assume that t is odd. The fact that t is odd will be used in several places in the arguments below.

Since $b_0/2$ is a divisor of $b/2 = mn$, we can write

$$b_0/2 = m_0 n_0,$$

where m_0 and n_0 are positive divisors of m and n, respectively. Note that these are uniquely determined. Then

$$m^2 - n^2 = 1 + m_0 n_0 t. \tag{8}$$

Since t is odd, Eq. (8) implies that m_0 or n_0 is even, and so

$$\mathrm{rad}(m_0) = \mathrm{rad}(m), \qquad \mathrm{rad}(n_0) = \mathrm{rad}(n). \tag{9}$$

From (8) we find

$$m^2 \equiv 1 \pmod{n_0}, \tag{10}$$

$$n^2 \equiv -1 \pmod{m_0}. \tag{11}$$

First, we prove an important lemma.

Lemma 5. *Assume that m is odd. Then, with the notation in (7), we have $\alpha \geqslant \beta + 1$.*

Proof. Since t is odd, it follows from Lemma 4 and (8) that

$$\min\{2\alpha, \beta + 1\} \leqslant \mathrm{ord}_2(a - 1) = \mathrm{ord}_2(m_0 n_0 t) \leqslant \mathrm{ord}_2(mn) = \alpha.$$

This gives the desired conclusion. □

Let (x, y, z) be a solution of (6).

Lemma 6. *z is even.*

Proof. Taking (6) modulo m_0, we have $(-n^2)^x \equiv (n^2)^z \pmod{m_0}$. Then $(-1)^z \equiv 1 \pmod{m_0}$ by (11). Hence, z is even if $m_0 \geqslant 3$. If $m_0 \leqslant 2$, then (9) implies $m_0 = 2$, so m is a power of 2, where Conjecture 1 is true by [M, Theorem 1.2]. □

Lemma 7. *x is even.*

Proof. If m is even, then the conclusion follows from taking (6) modulo 4. Hence we may assume that m is odd. In view of Lemmas 1, 5 and 6, we conclude that x is even. $\square$

In view of Lemmas 3, 6 and 7, we can write $x = 2X$ and $z = 2Z$ with positive odd integers X and Z. Define positive even integers D and E as follows:

$$(2mn)^y = DE,$$

where

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

It is easy to see $y > 1$ and $\gcd(D, E) = 2$.

Lemma 8. *We have equality of the ordered pairs*

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

Proof. Since $m \not\equiv n \pmod 2$, it follows that

$$\begin{cases} D \equiv 0, \qquad E \equiv 2 \pmod 4 & \text{if } m \text{ is even,} \\ D \equiv 2, \qquad E \equiv 0 \pmod 4 & \text{if } m \text{ is odd.} \end{cases}$$

Further, from (10) and (11) we see

$$D \equiv \pm 2 \pmod{n_0}, \qquad E \equiv \pm 2 \pmod{m_0}.$$

These congruences together imply that $D/2$ is prime to n_0 (hence, to n by (9)), and that $E/2$ is prime to m_0 (hence, to m by (9)). It follows from the equation $(D/2)(E/2) = 2^{y-2}m^y n^y$ that m^y divides $D/2$, and n^y divides $E/2$. The factor 2^{y-2} divides $D/2$ or $E/2$ according to whether m is even or not. This proves the lemma. $\square$

Lemma 9. *y is even.*

Proof. First we assume that m is even. Then Lemma 8 tells us $(1 + m_0 n_0 t)^X = (D - E)/2 = 2^{y-2}m^y - n^y$. Taking this modulo m_0, we have $n^y \equiv -1 \pmod{m_0}$. Then squaring this we get $(-1)^y \equiv 1 \pmod{m_0}$ by (11). From this we may conclude that y is even in the same manner as Lemma 6.

Second we assume that m is odd. Then Lemma 8 tells us $(1+m_0 n_0 t)^X = (D-E)/2 = m^y - 2^{y-2}n^y$. Taking this modulo n_0, we have $m^y \equiv 1 \pmod{n_0}$. Suppose that y is odd. Then $m \equiv 1 \pmod{n_0}$ by (10). This together with (8) and the fact that both t and m are odd yields a contradiction as follows:

$$\begin{aligned}\operatorname{ord}_2(n_0) &\leqslant \operatorname{ord}_2(m-1)\\ &< \operatorname{ord}_2\bigl(m^2-1\bigr)\\ &= \operatorname{ord}_2\bigl(n^2+m_0n_0t\bigr)\\ &= \operatorname{ord}_2(n_0)+\operatorname{ord}_2\bigl(n^2/n_0+m_0t\bigr)=\operatorname{ord}_2(n_0).\end{aligned}$$

Therefore, y is even. □

By Lemma 9, we can write $y = 2Y$ with a positive integer Y. Then Lemma 8 yields (3), and Proposition 1 gives $X = Y = Z = 1$, as desired.

4.2. *The case* $(A, \epsilon) = (c, 1)$

Assume that Conjecture 1 is true under assumption (2) with $A = c$ and $\epsilon = 1$. Similarly to the preceding case, we may write

$$m^2 + n^2 = 1 + m_0n_0t, \tag{12}$$

where t is a positive odd integer, and m_0, n_0 are positive divisors of m and n, respectively, such that condition (9) holds. From (12) we find

$$m^2 \equiv 1 \pmod{n_0}, \tag{13}$$
$$n^2 \equiv 1 \pmod{m_0}. \tag{14}$$

Lemma 10. *With the notation in (7), we have* $\alpha \geqslant \beta + 1$.

Proof. Similarly to Lemma 5, we have the conclusion by using the fact that t is odd and Lemma 4. □

Let (x, y, z) be a solution of (6).

Lemma 11. *Both x and z are even.*

Proof. Similarly to Lemma 6, we can prove that x is even by taking (6) modulo m_0 together with (14). Hence, Lemmas 1 and 10 yield that z is even. □

By Lemmas 3 and 11, we can write $x = 2X$ and $z = 2Z$ with positive odd integers X and Z. As in the preceding section, we consider positive even integers D and E, and from (13) and (14), we have the same congruences on D and E. As a result, Lemma 8 holds in this case as the same proof goes through. Hence, by Proposition 1, it suffices to show that y is even.

First, assume that m is even. Then Lemma 8 tells us $(1 + m_0n_0t)^Z = 2^{y-2}m^y + n^y$. Taking this modulo m_0, we have $n^y \equiv 1 \pmod{m_0}$. Suppose that y is odd. Then

$n \equiv 1 \pmod{m_0}$ by (14). This together with (12) and the fact that both t and n are odd yields a contradiction as follows:

$$\begin{aligned}\mathrm{ord}_2(m_0) &\leqslant \mathrm{ord}_2(n-1)\\ &< \mathrm{ord}_2\left(n^2-1\right)\\ &= \mathrm{ord}_2\left(-m^2+m_0n_0t\right)\\ &= \mathrm{ord}_2(m_0)+\mathrm{ord}_2\left(-m^2/m_0+n_0t\right)=\mathrm{ord}_2(m_0).\end{aligned}$$

Second, assume that m is odd. Then Lemma 8 tells us $(1+m_0n_0t)^Z = m^y + 2^{y-2}n^y$. Taking this modulo n_0, we have $m^y \equiv 1 \pmod{n_0}$. Suppose that y is odd. Then $m \equiv 1 \pmod{n_0}$ by (13). This yields a contradiction as in the preceding case. Therefore, we conclude that y is even. This completes the proof of Theorem 2 for the case $\epsilon = 1$.

5. The case $y = 1$

Before proving Theorem 2 in the case $\epsilon = -1$, we study Eq. (6) in the case $y = 1$, where Eq. (6) has the form of the Pillai equation. A usual application of the theory of linear forms in (two) logarithms of algebraic numbers gives us a sufficient condition to ensure $y > 1$. Indeed, we prove the following.

Lemma 12. *Let (x, y, z) be a solution of (6). Suppose $y = 1$. Then the following holds.*

(i) *We have*

$$1 \leqslant x - z < 2521 \log\left(\frac{r^2+1}{r^2-1}\right),$$

where $r = m/n$. In particular, $r < 72$.

(ii) *For $i \geqslant 0$, let q_i be the denominator of the i-th convergent in the simple continued fraction expansion of $\frac{\log a}{\log c}$, and let α_i be the i-th partial quotient of $\frac{\log a}{\log c}$. Then there exists a non-negative integer s with $4 \leqslant q_s < 2521 \log c$ such that*

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

Proof. (i) Since $y = 1$, we have

$$\left(m^2-n^2\right)^x + 2mn = \left(m^2+n^2\right)^z. \tag{15}$$

It is not hard to show $x \geqslant 4$ and $x > z > 1$. Also, x and z are co-prime. Indeed, if d is a common divisor of them, then (15) implies that b is divisible by $(c^z - a^x)/(c^{z/d} - a^{x/d}) = (c^{z/d})^{d-1} + a^{x/d}(c^{z/d})^{d-2} + \cdots + (a^{x/d})^{d-1}$, which is greater than c $(> b)$ if $d > 1$.

Put

$$\Lambda_1 := z \log c - x \log a \quad (> 0).$$

Observe $\Lambda_1 < ba^{-x}$. In order to obtain a lower bound for Λ_1, we use a result from [La]. To state it, we prepare some notation.

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

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

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 non-zero algebraic numbers with $|\alpha_1| \geqslant 1$ and $|\alpha_2| \geqslant 1$, and let $\log \alpha_1$ and $\log \alpha_2$ be any determination of their logarithms. Consider the linear 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

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

where we denote $\mathbb{R}$ by 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 $A_2 > 1$ be real numbers such that

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

We rely the following result due to Laurent [La].

Proposition 2. *(Corollary 2; $m = 10$, [La]) With the above notation, suppose that $\alpha_1, \alpha_2, \log \alpha_1, \log \alpha_2$ are all real positive numbers. If α_1 and α_2 are multiplicatively independent, then we have*

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

We set $(\alpha_1, \alpha_2) = (a, c)$ and $(b_1, b_2) = (x, z)$. Then $D = 1$, and we may take $(A_1, A_2) = (a, c)$. Hence, Proposition 2 gives us

$$\log \Lambda_1 > -25.2(\log a)(\log c)\bigl(\max\bigl\{\log b' + 0.38, 10\bigr\}\bigr)^2,$$

where $b' = x/\log c + z/\log a$. It follows that

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

Since $b < c$ and $c^z = a^x + b < a^x + a^2 \leqslant 2a^x$, we see $b' < 3s$, where $s = x/\log c$, and so

$$s < 1 + 25.2\bigl(\max\bigl\{\log(3s) + 0.38, 10\bigr\}\bigr)^2.$$

This implies $s < 2521$. Then, since

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

we find

$$(1 \leqslant) \quad x - z < 2521\log\left(\frac{r^2+1}{r^2-1}\right),$$

where $r = m/n$. Also, the above yields $r < 72$.

(ii) The fact that $\Lambda_1 < ba^{-x}$ together with $x < 2521\log c$ gives

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

Since we may assume $m \geqslant n + 3$ by [D], we have $r = m/n \geqslant 1 + 3/n$, giving

$$\frac{b}{a} = \frac{2mn}{m^2 - n^2} = \frac{2r}{r^2-1} \leqslant \frac{2(1+3/n)}{(1+3/n)^2-1} = \frac{2n(n+3)}{6n+9},$$
$$a = m^2 - n^2 \geqslant (n+3)^2 - n^2 \geqslant 6n + 9.$$

Hence, $b/a^x \leqslant b/a^4 \leqslant 2n(n+3)/(6n+9)^4 \leqslant 8/15^4 < 1/5042$, which implies

$$\left|\frac{\log a}{\log c} - \frac{z}{x}\right| < \frac{1}{2x^2}.$$

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 $x = q_s$ and $z = p_s$. Note $4 \leqslant q_s = x < 2521\log c$. By a well-known fact due to Legendre on the continued fraction expansion, we find

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

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

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

This proves the lemma. $\square$

6. The case $\epsilon = -1$

In this section, we prove Theorem 2 for the case $\epsilon = -1$. We consider the cases $A = a$ and $A = c$ separately.

6.1. The case $(A, \epsilon) = (a, -1)$

We may write

$$m^2 - n^2 = -1 + m_0 n_0 t,$$

where t, m_0, n_0 are defined similarly to Section 4. Then

$$m^2 \equiv -1 \pmod{n_0}, \qquad n^2 \equiv 1 \pmod{m_0}.$$

Let (x, y, z) be a solution of (6). Note that the inequality on b_0 in the statement of Theorem 2:

$$b_0 > \frac{4m}{\mathrm{p}(m)}, \tag{16}$$

where $\mathrm{p}(m)$ is the least prime factor of m, will be used only to show that z is even.

In a similar manner to Lemma 6, we can prove that x is even by taking (6) modulo m_0 together with $n^2 \equiv 1 \pmod{m_0}$.

Next, we show that z is even. If m is even, then Lemma 4 and the fact that t is odd imply

$$\min\{2\alpha, \beta + 1\} \leqslant \mathrm{ord}_2(a + 1) = \mathrm{ord}_2(m_0 n_0 t) \leqslant \mathrm{ord}_2(mn) = \alpha,$$

and so z is even by Lemma 1. Hence, we may assume that m is odd. Taking (6) modulo n_0, we have $(m^2)^x \equiv (m^2)^z \pmod{n_0}$, which together with $m^2 \equiv -1 \pmod{n_0}$ implies $(1=)\ (-1)^x \equiv (-1)^z \pmod{n_0}$. Hence, z is even if $n_0 \geqslant 3$.

Suppose $n_0 \leqslant 2$. Then $n_0 = 2$ and n is a power of 2, so, with the notation in (7), we have $n = 2^\alpha$. By Lemma 1, we may assume $\beta \geqslant \alpha$. Then $m = 2^\beta j + e \equiv e \pmod{n}$. Write $m = e + hn$ with a positive integer h. If $h = 1$, then, since $m > n$, we have $e = 1$, that is, $m = n + 1$, where Conjecture 1 is true by [D]. Hence, we may assume $h \geqslant 2$.

We claim that $y > 1$. Suppose $y = 1$. We will observe that this yields a contradiction. Observe

$$m^2 \pm n^2 \equiv m^2 \equiv 1 + 2ehn \pmod{n^2}, \qquad 2mn \equiv 2en \pmod{n^2}.$$

Taking (6) modulo n^2, we find

$$2hx + 2 \equiv 2hz \pmod{n}.$$

Then, Lemma 12(i) together with the fact $r = m/n = h + e/n \geqslant h - 1/2$ implies

$$n - 2 \leqslant 2h(x - z) < 5042h \log\left(\frac{(h-1/2)^2 + 1}{(h-1/2)^2 - 1}\right).$$

Since $h \geqslant 2$, the above implies $n \leqslant 4818$. Therefore, $n \leqslant 4096 = 2^{12}$. Also, $m = rn < 294\,912$ by Lemma 12(i). We can observe that for each of the pairs (m, n) under consideration, the inequality in the statement of Lemma 12(ii) does not hold for any s satisfying $4 \leqslant q_s < 2521 \log c$. Hence, the claim is proved.

Since $y > 1$, we may assume $2\alpha = \beta + 1$ by Lemma 2. Note that $\alpha \geqslant 2$ as $\beta > 1$. In this case, using (16), we have

$$4m_0 = b_0 > \frac{4m}{\mathrm{p}(m)},$$

so $m_0 > m/\mathrm{p}(m)$, which implies $m_0 = m$. Then, since $m^2 \equiv 1 \pmod{2n}$ and $n^2 \equiv 1 \pmod{m}$, we see that

$$c - 1 = \left(m^2 - 1\right) + n^2 = 2mt + 2\left(n^2 - 1\right)$$

is divisible by both m and $2n$, hence by $b = 2mn$, where Conjecture 1 is true by [M2]. Therefore, we conclude that z is even.

In a similar manner to Section 4, we can write $x = 2X$ and $z = 2Z$ with positive odd integers X and Z, and we have the same result as Lemma 8. By Proposition 1, it suffices to show that y is even.

First, assume that m is even. Then by Lemma 8 and $\epsilon = -1$ we have $(-1+m_0n_0t)^X = 2^{y-2}m^y - n^y$. Taking this modulo m_0, we have $n^y \equiv 1 \pmod{m_0}$. Suppose that y is odd. Then, since $n^2 \equiv 1 \pmod{m_0}$, we have $n \equiv 1 \pmod{m_0}$. But, this yields a contradiction as in Section 4.2.

Second, assume that m is odd. Then $(-1 + m_0n_0t)^X = m^y - 2^{y-2}n^y$. Taking this modulo n_0, we have $m^y \equiv -1 \pmod{n_0}$, which together with $m^2 \equiv -1 \pmod{n_0}$ implies $(-1)^y \equiv 1 \pmod{n_0}$. Hence, y is even if $n_0 \geqslant 3$. So suppose $n_0 \leqslant 2$. Then $n_0 = 2$ and n is a power of 2.

Suppose $2\alpha \geqslant \beta + 1$. Let us observe the equation $c^Z = m^y + 2^{y-2}n^y$. It is clear that $y \geqslant 2Z$. Since

$$c^Z \equiv 1 \pmod{2^{\beta+1}}, \qquad 2^{y-2}n^y \equiv 0 \pmod{2^{2\alpha}},$$

we see $(2^\beta j + e)^y = m^y \equiv 1 \pmod{2^{\beta+1}}$, and so

$$2^\beta jye^{y-1} + e^y \equiv 1 \pmod{2^{\beta+1}}.$$

Reducing this modulo 4, we have $e^y - 1 \equiv 0 \pmod 4$, so $e^y - 1 = 0$, which together with the above congruence implies $jy \equiv 0 \pmod 2$ and y is even. Hence, we may assume $2\alpha \leqslant \beta$, and also $m > n^2$ (cf. [M2, Example 5.1]). Since

$$c^Z m^{-y} = 1 + \frac{1}{4}\left(\frac{2n}{m}\right)^y < 1 + \left(2m^{-1/2}\right)^y,$$

we have

$$(0 <) \quad \Lambda_2 := Z\log c - y\log m < \left(2m^{-1/2}\right)^y.$$

We apply Proposition 2 to Λ_2 with $(\alpha_1, \alpha_2) = (m, c)$ and $(b_1, b_2) = (y, Z)$. Since we may take $(A_1, A_2) = (m, c)$, it follows that

$$\frac{y}{\log c} < \frac{50.4}{1 - \frac{\log 4}{\log m}}\left(\max\left\{\log b' + 0.38, 10\right\}\right)^2,$$

where $b' = y/\log c + Z/\log m$. Since $c^Z < 2m^y$ and $m > n^2 \geqslant 4$, the above inequality implies $y < 36\,352\log c$. Suppose $y > 2Z$. Then we observe that

$$1 \leqslant y - 2Z < y - \frac{\log m}{\log\sqrt{c}}y = \frac{y}{\log c}\log\left(c/m^2\right) < \frac{36\,352n^2}{m^2},$$

so $m^2 < 36\,352n^2$. Hence, $m < 36\,352$ (as $n^2 < m$), also we have $n < \sqrt{m} < 191$. Since n is a power of 2, we have $n \leqslant 128$, which yields a better bound: $m < \sqrt{36\,352}n < 24\,405$. For any pair (m, n) with these bounds, note that $n^2 \equiv 1 \pmod{\mathrm{rad}(m)}$ does not hold. This is a contradiction. Hence, $y \leqslant 2Z$, so $y = 2Z$. We conclude that y is even.

6.2. The case $(A, \epsilon) = (c, -1)$

We may write

$$m^2 + n^2 = -1 + m_0 n_0 t,$$

where t, m_0, n_0 are defined similarly to the preceding case.

Let (x, y, z) be a solution of (6). Note that inequality (16) will be used only to show that x is even.

We can prove that z is even by taking (6) modulo m_0 together with $n^2 \equiv -1 \pmod{m_0}$.

Next, we show that x is even. We may assume that m is odd. Taking (6) modulo n_0, we have $(m^2)^x \equiv (m^2)^z \pmod{n_0}$, which together with $m^2 \equiv -1 \pmod{n_0}$ implies $(-1)^x \equiv (-1)^z\ (= 1) \pmod{n_0}$. Hence, x is even if $n_0 \geqslant 3$. Suppose $n_0 \leqslant 2$. Then $n_0 = 2$ and n is a power of 2. From this, we may assume $2\alpha = \beta + 1$ as in Section 6.1. So, by our assumption (16), we have $m_0 = m$. Since $m^2 \equiv 1 \pmod{2n}$ and $n^2 \equiv -1 \pmod{m}$, we see that $a - 1 = (m^2 - 1) - n^2 = 2mt - 2(n^2 + 1)$ is divisible by both m and $2n$, hence by $b = 2mn$, where Conjecture 1 is true by [M2]. Therefore, we conclude that x is even.

In a similar manner to Section 4, we can write $x = 2X$ and $z = 2Z$ with positive odd integers X and Z, and we have the same result as Lemma 8. We can prove that y is even in a similar manner to the preceding section. Therefore, Proposition 1 completes the proof of Theorem 2 for the case $\epsilon = -1$.

7. Examples

In this section, we give some examples of Theorem 1. Note that all examples in the case $A \equiv \epsilon \pmod{b}$ have already been observed in [M2]. Here, we look at the case of $A \equiv \epsilon \pmod{b/2}$ and $A \not\equiv \epsilon \pmod{b}$.

Example 1. Let t be a positive odd integer. All the pairs (m, n) satisfying $a = \epsilon + (b/2)t$ are given as

$$m = \frac{U_\ell + tV_\ell}{2}, \qquad n = V_\ell,$$

where $\ell > 1$ is a positive integer such that ℓ is even if $\epsilon = 1$, and ℓ is odd if $\epsilon = -1$, and where $\{U_\ell\}, \{V_\ell\}$ are the sequences in t defined by

$$\begin{gathered} U_1 = t, \qquad U_2 = t^2 + 2, \qquad U_{\ell+2} = tU_{\ell+1} + U_\ell, \\ V_1 = 1, \qquad V_2 = t, \qquad V_{\ell+2} = tV_{\ell+1} + V_\ell. \end{gathered}$$

For example, we have

$$\begin{aligned} \epsilon = 1,\ \ell = 2; &\quad m = t^2 + 1,\ n = t, \\ \epsilon = 1,\ \ell = 4; &\quad m = t^4 + 3t^2 + 1,\ n = t\bigl(t^2 + 2\bigr), \\ \epsilon = -1,\ \ell = 3; &\quad m = t\bigl(t^2 + 2\bigr),\ n = t^2 + 1, \\ \epsilon = -1,\ \ell = 5; &\quad m = t^5 + 2t^3 + 2t^2 + 2t + 1,\ n = t^4 + 3t^2 + 1. \end{aligned}$$

Proof. Write $m^2 - n^2 = \epsilon + mnt$, where t is a positive odd integer. Then $(U, V) = (2m - nt, n)$ is a positive solution of the Pellian equation

$$U^2 - (t^2 + 4)V^2 = 4\epsilon.$$

By the theory of Pellian equations, we see that all positive integer solutions (U, V) are obtained from the relation that $(U + V\sqrt{t^2 + 4})/2$ is equal to a positive (even, if $\epsilon = 1$, odd if $\epsilon = -1$) power of the fundamental unit in $\mathbb{Q}(\sqrt{t^2 + 4})$, which is $\frac{t+\sqrt{t^2+4}}{2}$. From this one can easily obtain the desired conclusion. $\square$

Example 2. Let t be a positive odd integer with $t \geqslant 3$. All the pairs (m, n) satisfying $c = 1 + (b/2)t$ are given as

$$m = \frac{U_\ell + tV_\ell}{2}, \qquad n = V_\ell,$$

where $\ell > 1$ is a positive integer, and $\{U_\ell\}, \{V_\ell\}$ are the sequences in t defined by

$$U_1 = t, \qquad U_2 = t^2 - 2, \qquad U_{\ell+2} = tU_{\ell+1} - U_\ell,$$
$$V_1 = 1, \qquad V_2 = t, \qquad V_{\ell+2} = tV_{\ell+1} - V_\ell.$$

For example, we have

$$\ell = 2; \quad m = t^2 - 1, \ n = t,$$
$$\ell = 3; \quad m = t^3 - 2t, \ n = t^2 - 1,$$
$$\ell = 4; \quad m = t^4 - 3t^2 + 1, \ n = t^3 - 2t.$$

Proof. Write $m^2 + n^2 = 1 + mnt$, where t is a positive odd integer with $t \geqslant 3$. Then $(U, V) = (2m - nt, n)$ is a positive solution of the Pellian equation

$$U^2 - (t^2 - 4)V^2 = 4.$$

By the theory of Pellian equations, we see that all positive integer solutions (U, V) are obtained from the relation that $(U + V\sqrt{t^2 - 4})/2$ is equal to a positive power of the fundamental unit in $\mathbb{Q}(\sqrt{t^2 - 4})$, which is $\frac{t+\sqrt{t^2-4}}{2}$. From this one can easily obtain the desired conclusion. $\square$

Remark 1. We fail to give all (m, n) for which A is congruent to ϵ modulo $b/2^r$ with $r \geqslant 2$. Any pair (m, n) for which A is congruent to ϵ modulo b/d, where $d \neq 1, 2$ is any divisor of b, induces a positive solution $(U, V) = (dm - nt, n)$ of the Pellian equation

$$U^2 - (t^2 \pm d^2)V^2 = \epsilon d^2.$$

It seems that the above Pellian equation is very hard to handle even if d is a power of 2. We also remark that the above equation has no solutions if $(A, \epsilon) = (c, -1)$ with $d \in \{1, 2\}$.

Acknowledgments

The authors are very grateful to the referee for the many valuable comments and suggestions which enable us to improve the quality of the manuscript. The first author was supported by Grant-in-Aid for JSPS Fellows (No. 25484). The second and third authors were supported by National Natural Science Foundation of China (No. 11271142) and the Guangdong Provincial Natural Science Foundation (No. S2012010009942).

References

[D] V.A. Dem'janenko, On Jeśmanowicz' problem for Pythagorean numbers, Izv. Vyssh. Uchebn. Zaved. Mat. 48 (1965) 52–56 (in Russian).
[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.
[J] L. Jeśmanowicz, Several remarks on Pythagorean numbers, Wiadom. Mat. 1 (1955/1956) 196–202 (in Polish).
[La] M. Laurent, Linear forms in two logarithms and interpolation determinants II, Acta Arith. 133 (2008) 325–348.
[Lu] 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).
[M] T. Miyazaki, Jeśmanowicz' conjecture on exponential Diophantine equations, Funct. Approx. Comment. Math. 45 (2011) 207–229.
[M2] T. Miyazaki, Generalizations of classical results on Jeśmanowicz' conjecture concerning Pythagorean triples, J. Number Theory 133 (2013) 583–595.
[R] P. Ribenboim, Catalan's Conjecture: are 8 and 9 the only Consecutive Powers?, Academic Press, Boston, MA, 1994.
[S] W. Sierpiński, On the equation $3^x + 4^y = 5^z$, Wiadom. Mat. 1 (1955/1956) 194–195 (in Polish).