COLLOQUIUM MATHEMATICUM

VOL. 128 2012 NO. 2

JEŚMANOWICZ' CONJECTURE WITH CONGRUENCE RELATIONS

BY

YASUTSUGU FUJITA (Chiba) and TAKAFUMI MIYAZAKI (Tokyo)

Abstract. Let a, b and c be relatively prime positive integers such that $a^2 + b^2 = c^2$. We prove that if $b \equiv 0 \pmod{2^r}$ and $b \equiv \pm 2^r \pmod{a}$ for some non-negative integer r, then the Diophantine equation $a^x + b^y = c^z$ has only the positive solution $(x, y, z) = (2, 2, 2)$. We also show that the same holds if $c \equiv -1 \pmod{a}$.

1. Introduction. Let a, b and c be relatively prime positive integers such that $a^2+b^2 = c^2$. Such a triple (a, b, c) is called a *primitive Pythagorean triple*. We consider the positive solutions (x, y, z) of the exponential Diophantine equation

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

The first non-trivial result on the Diophantine equation (1.1) is due to Sierpiński ([12]), who showed that the Diophantine equation $3^x + 4^y = 5^z$ has only the positive solution $(x, y, z) = (2, 2, 2)$. Jeśmanowicz ([5]) further showed that the same is true for

$$(a, b, c) \in \{(5, 12, 13), (7, 24, 25), (9, 40, 41), (11, 60, 61)\},$$

and proposed the following conjecture.

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

There are various kinds of triples (a, b, c) for which Conjecture 1.1 is known to be valid. When we parameterize a, b and c by

$$a = m^2 - n^2, \quad b = 2mn, \quad c = m^2 + n^2, \tag{1.2}$$

where m and n are positive integers with $m > n$, $\gcd(m, n) = 1$ and $m \not\equiv n \pmod 2$, it was shown that Conjecture 1.1 is true for $n = 1$ by Lu ([8]) and for $n = m - 1$ by Dem'janenko ([2]). In [10], the second author showed that Conjecture 1.1 is true if $a \equiv -1 \pmod{b}$, $a \equiv 1 \pmod{b}$ or $c \equiv 1 \pmod{b}$, where the results for $a \equiv -1 \pmod{b}$ and $c \equiv 1 \pmod{b}$ generalize the ones

2010 *Mathematics Subject Classification*: Primary 11D61; Secondary 11D09.

Key words and phrases: exponential Diophantine equations, Pythagorean triples, Pell equations.

in [8] and [2], respectively. For other results supporting Conjecture 1.1, see for example [1], [3], [6] and [7]. In this paper, we show that Conjecture 1.1 is true under a certain assertion on b mod a.

THEOREM 1.2. *Let a, b and c be a primitive Pythagorean triple such that $a^2+b^2=c^2$. Let r be a non-negative integer such that $b \equiv 0 \pmod{2^r}$. If $b \equiv \epsilon 2^r \pmod{a}$ with $\epsilon \in \{\pm 1\}$, then Conjecture 1.1 is true.*

Note that in Theorem 1.2 one can take any integer $r \geq 0$ as long as $b \equiv 0 \pmod{2^r}$. Moreover, if b is odd, then $r=0$ and $b \equiv \pm 1 \pmod{a}$, where Conjecture 1.1 is true by [10]. Thus, we may assume (1.2).

Note that Theorem 1.2 contains the results of Lu ([8]) and Dem'janenko ([2]) whenever m is a power of 2. Indeed, if we put $m = 2^s$, then $n = m-1$ implies that $a = 2^{s+1}-1$ and $b = 2^{s+1}(2^s-1) \equiv -2^s \pmod{a}$ (it is obvious for the result of Lu).

The second main theorem asserts that Conjecture 1.1 holds under the assumption $c \equiv -1 \pmod{a}$.

THEOREM 1.3. *Let a, b and c be a primitive Pythagorean triple such that $a^2+b^2=c^2$. If $c \equiv -1 \pmod{a}$, then Conjecture 1.1 is true.*

If $c \equiv -1 \pmod{a}$ with a even, then $m^2+n^2 = -1+2mnt$ for some integer t, which does not hold modulo 4. Hence, we may assume (1.2) in this case, too. For the cases of $c \equiv \epsilon 2^r \pmod{a}$ with $(\epsilon, r) \neq (-1, 0)$, see the end of Section 5, where, in particular, it is shown that Conjecture 1.1 is true if $c \equiv 2 \pmod{a}$, which can be regarded as a paraphrase of the result of Lu ([8]).

2. Preliminaries to the proof of Theorem 1.2. By the assumptions $b \equiv \epsilon 2^r \pmod{a}$, $b \equiv 0 \pmod{2^r}$ and $a \equiv 1 \pmod{2}$, we may write

$$b = \epsilon 2^r + 2^r at$$

with some integer $t \geq 0$. If $t=0$, then ($\epsilon = 1$ and) $b = 2^r$, which implies $n=1$, and then Conjecture 1.1 holds by [8]. Hence, we may assume that $t \geq 1$. Putting $M = m+n$ and $N = m-n$, we see from (1.2) that

$$(M - 2^r Nt)^2 - ((2^r t)^2+1)N^2 = \epsilon 2^{r+1}. \tag{2.1}$$

If $t \geq 2$, then the Pell equation $U^2 - ((2^r t)^2+1)V^2 = \epsilon 2^{r+1}$ has no primitive solution (cf., e.g., [4, Lemma 2.3]), and the Diophantine equation (2.1) has no solution, since $\gcd(M,N)=1$. Hence, $t=1$ and

$$m^2 - n^2 = m_0 n_0 - \epsilon, \tag{2.2}$$

where m_0 and n_0 are positive divisors of m and n, respectively, such that $2^r m_0 n_0 = 2mn$, that is,

$$(m_0, n_0) = \begin{cases} (m/2^{r-1},\, n) & \text{if } m \text{ is even,} \\ (m,\, n/2^{r-1}) & \text{if } m \text{ is odd.} \end{cases}$$

If $r = 0$, then $m^2 - n^2 = 2mn - \epsilon$, which means $a = b - \epsilon$. In this case, we know that Conjecture 1.1 is true by [10]. Thus, we may assume that

$$r \geq 1.$$

Moreover, equation (2.2) immediately shows that $m_0 n_0$ is even. If $m_0 = 1$, then $m = m_0 = 1$, which contradicts $m > n$. If $n_0 = 1$, then $n = n_0 = 1$, where Conjecture 1.1 is true by [8]. Furthermore, if $m_0 = 2$, then $\epsilon = -1$ and $m^2 = (n+1)^2$, and if $n_0 = 2$, then $\epsilon = 1$ and $n^2 = (m-1)^2$; in either case, we have $n = m - 1$ and Conjecture 1.1 is true by [2]. Thus, we may assume that

$$m_0, n_0 \geq 3.$$

By (2.2) we have the following congruences:

$$m^2 \equiv -\epsilon \pmod{n_0} \quad \text{and} \quad n^2 \equiv \epsilon \pmod{m_0}. \tag{2.3}$$

Lemma 2.1. *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 (2.3) 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 of $\epsilon = 1$. Consider the case of $\epsilon = 1$. By Lemma 2.1, we may write $x = 2X$ and $z = 2Z$ with positive integers X and Z, which, together with (1.1), enables us to write

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

where

$$D = (m^2 + n^2)^Z + (m^2 - n^2)^X, \qquad E = (m^2 + n^2)^Z - (m^2 - n^2)^X. \tag{3.1}$$

It is easy to see that $\gcd(D, E) = 2$. Also, $y > Z$, in particular, $y > 1$. Indeed,

$$(2mn)^y = DE > D > (m^2 + n^2)^Z > (2mn)^Z.$$

Recall that $m_0 n_0$ is even. If $m_0 n_0 \equiv 0 \pmod{4}$, then $m^2 - n^2 \equiv -1 \pmod{4}$, which implies that m is even, so $m_0 \equiv 0 \pmod{4}$. If $m_0 n_0 \equiv 2 \pmod{4}$, then $m^2 - n^2 \equiv 1 \pmod{4}$, which implies that n is even, so $n_0 \equiv 2 \pmod{4}$.

To sum up, it suffices to consider the case of either

$$\text{(i) } m_0 \equiv 0 \pmod 4 \text{ and } n_0 = n,$$

or

$$\text{(ii) } n_0 \equiv 2 \pmod 4 \text{ and } m_0 = m.$$

LEMMA 3.1. *If* $m_0 \equiv 0 \pmod 4$*, then* X *and* Z *are odd. If* $n_0 \equiv 2 \pmod 4$*, then* X *is odd.*

Proof. Suppose that X is even. Then from (2.3) and (3.1) we see that $D \equiv 2 \pmod 4$, $D \equiv 2 \pmod{m_0}$, $E \equiv 0 \pmod 4$ and $E \equiv 0 \pmod{m_0}$. Hence, in each case of (i) and (ii) we have $E \equiv 0 \pmod{2^{y-1}m^y}$. However, this implies that $2^{y-1}m^y \le E < D \le 2n^y$, which contradicts $y > 1$ and $m > n$. Therefore, X is odd.

Suppose that Z is even in the case of $m_0 \equiv 0 \pmod 4$. Then $E \equiv 2 \pmod{m_0}$, $E \equiv 2 \pmod n$ and we have $E = 2$, so $D = 2^{y-1}m^y n^y$. Thus, $2^{y-2}m^y n^y = AB$, where $A = (m^2+n^2)^{Z/2}+1$, $B = (m^2+n^2)^{Z/2}-1$. Since $A \equiv 2 \pmod{m_0}$, we see that $B \equiv 0 \pmod{2^{y-3}m^y}$. But this implies that $2^{y-3}m^y \le B < A \le 2n^y$, so $y \le 3$. Since $y > Z$, we have $y = 3$ and $Z = 2$. Hence, $B = m^2+n^2-1 \equiv 0 \pmod{m^3}$, a contradiction. Therefore, if $m_0 \equiv 0 \pmod 4$, then Z is also odd. ■

In case (i), we need the following lemma in order to show that y is even.

LEMMA 3.2. *If* $m_0 \equiv 0 \pmod 4$*, then* $m_0 \equiv 0 \pmod{2^{r+2}}$.

Proof. Put $m_1 = m_0/2$. Equation (2.2) implies

$$(n+m_1)^2 - (2^{2r}+1)m_1^2 = 1.$$

Since any positive solution of the Pell equation $U^2 - (2^{2r}+1)V^2 = 1$ has the form

$$U + V\sqrt{2^{2r}+1} = \left(2^{2r+1}+1+2^{r+1}\sqrt{2^{2r}+1}\,\right)^j$$

with a positive integer j, we easily see that $m_1 \equiv 0 \pmod{2^{r+1}}$, that is, $m_0 \equiv 0 \pmod{2^{r+2}}$. ■

By Lemma 3.1, we see that $E \equiv 2 \pmod{m_0}$ and $E \equiv 0 \pmod n$, so

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

Hence,

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

Since $y \ge 2$, we see from (2.3) that

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

LEMMA 3.3. *If* $m_0 \equiv 0 \pmod 4$*, then* y *is even.*

Proof. Suppose that y is odd. Congruences (2.3) and (3.2) together imply that $n \equiv 1 \pmod{m_0}$. Putting $n = 1 + hm_0$ with a positive integer h, we see from (2.2) that

$$(2^{2r-2} - h^2 - h)\, m_0 = 2h + 1.$$

Hence, $2^{2r-2} - h^2 - h \geq 1$, yielding $h < 2^{r-1}$. This implies that $m_0 \leq 2h + 1 < 2^r + 1 < 2^{r+1}$, which contradicts Lemma 3.2. ∎

Thus, we have shown that all three x, y and z are even in case (i), where it is not difficult to prove Theorem 1.2.

Proof of Theorem 1.2 in the case of $\epsilon = 1$ and $m_0 \equiv 0 \pmod 4$. Putting $y = 2Y$, one may write

$$(3.3) \qquad (m^2 - n^2)^X = k^2 - l^2, \quad (2mn)^Y = 2kl, \quad (m^2 + n^2)^Z = k^2 + l^2,$$

where k and l are positive integers with $k > l$, $\gcd(k, l) = 1$ and $k \not\equiv l \pmod 2$. Since $y = 2Y > Z$ and

$$(m^2 - n^2)^{2Z} > (m^2 + n^2)^Z = k^2 + l^2 > k^2 - l^2 = (m^2 - n^2)^X,$$

we have

$$(3.4) \qquad |X - Z| < Z < 2Y.$$

Since $(k + l)(k - l) = (m^2 - n^2)^X$ and $\gcd(k + l, k - l) = 1$, we may write

$$(3.5) \qquad k + l = u^X, \quad k - l = v^X$$

for some positive odd integers u and v satisfying $u > v$, $\gcd(u, v) = 1$ and $uv = m^2 - n^2$. Then we see that

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

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

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

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

$$u \pm v \leq u + v \leq uv + 1 = m^2 - n^2 + 1 \leq m^2 = 2^{2r-2} m_0^2$$

and $m = 2^{r-1} m_0 \equiv 0 \pmod{2^{2r+1}}$ by Lemma 3.2, we find that

$$(3.6) \qquad Y = \frac{\nu_2(u \pm v)}{\nu_2(2mn)} \leq \frac{(2r-2)\log 2 + 2\log m_0}{(2r+2)\log 2} < \frac{\log m_0}{2\log 2} + 1.$$

On the other hand, equation (1.1) implies that $n^{4X} \equiv n^{4Z} \pmod{m^2}$, which together with (2.2) yields $(1 - m_0 n)^{2X} \equiv (1 - m_0 n)^{2Z} \pmod{m^2}$. Hence,

$$2m_0 nX \equiv 2m_0 nZ \pmod{m_0^2}.$$

Similarly, we see that $m^{4X} \equiv m^{4Z} \pmod{n^2}$ and

$$2m_0nX \equiv 2m_0nZ \pmod{n^2}.$$

Since $\gcd(m_0, n) = 1$, we have $2m_0nX \equiv 2m_0nZ \pmod{m_0^2n^2}$, that is,

$$X \equiv Z \pmod{m_0n/2}. \tag{3.7}$$

If $X \neq Z$, then (3.4), (3.6) and (3.7) together imply that

$$m_0n/2 \le |X - Z| \le 2Y - 2 < \frac{\log m_0}{\log 2},$$

which contradicts $n \ge 3$ and $m_0 \ge 8$. Therefore, $X = Z$. Since X is odd by Lemma 3.1, we see that

$$(2mn)^{2Y} = DE = (m^2 + n^2)^{2X} - (m^2 - n^2)^{2X} = (2mn)^2w',$$

where w' is an odd integer. Hence, $\nu_2((2mn)^{2Y}) = \nu_2((2mn)^2)$. This implies that $Y = 1$, so $X = Z = 1$ by (3.4). ∎

Secondly, consider the case of (ii) $n_0 \equiv 2 \pmod 4$. We begin by examining m and $n_1 = n_0/2$ modulo 2^{r+1}.

LEMMA 3.4. *If $n_0 \equiv 2 \pmod 4$, then*

$$m \equiv 2^r + 1 \pmod{2^{r+1}} \quad \text{and} \quad n_1 \equiv 1 \pmod{2^{r+1}},$$

where $n_1 = n_0/2$.

Proof. From (2.2) we see that $(m - n_1)^2 - (2^{2r} + 1)n_1^2 = -1$. Since any positive solution of the Pell equation $U^2 - (2^{2r} + 1)V^2 = -1$ has the form

$$U + V\sqrt{2^{2r} + 1} = \left(2^r + \sqrt{2^{2r} + 1}\,\right)\left(2^{2r+1} + 1 + 2^{r+1}\sqrt{2^{2r} + 1}\,\right)^j$$

with a non-negative integer j, we have $m - n_1 \equiv 2^r \pmod{2^{r+1}}$ and $n_1 \equiv 1 \pmod{2^{r+1}}$, which immediately implies the assertion. ∎

LEMMA 3.5. *If $n_0 \equiv 2 \pmod 4$, then y is even.*

Proof. We know from Lemma 3.1 that X is odd. Assume first that Z is even. By (3.1), we see that $D \equiv 0 \pmod m$, $D \equiv 0 \pmod{n_0}$ and $E \equiv 0 \pmod 4$, so

$$D = 2m^yn_1^y, \quad E = 2^{(r+1)y-1}.$$

Hence,

$$(m^2 + n^2)^Z = (D + E)/2 = m^yn_1^y + 2^{(r+1)y-2}.$$

Since $y \ge 2$, $n = 2^{r-1}n_0 = 2^rn_1$ and Z is even, we see from Lemma 3.4 that

$$1 \equiv (1 + 2^r)^y \pmod{2^{r+1}},$$

which implies that y is even.

Assume secondly that Z is odd. By (3.1), we see that $D \equiv 0 \pmod{m}$, $D \equiv -2 \pmod{n_0}$ and $E \equiv 0 \pmod{4}$, so

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

Hence,

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

Since $y \geq 2$, $m^2 \equiv -1 \pmod{n_0}$ and Z is odd, we obtain $m^y \equiv -1 \pmod{n_0}$. 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. ∎

Proof of Theorem 1.2 in the case of $\epsilon = 1$ *and* $n_0 \equiv 2 \pmod{4}$. Put $y = 2Y$. Then, we may write equation (3.3), and we have (3.4) and (3.5). Similarly to the case of $\epsilon = 1$ and $m_0 \equiv 0 \pmod{4}$, we find

$$Y \leq \frac{\log m}{\log 2}.$$

Also, in the same way as in the proof of (3.7), we have

$$X \equiv Z \pmod{mn_0/2}.$$

If $X \neq Z$, then

$$mn_0/2 \leq |X - Z| \leq 2Y - 2 \leq \frac{2\log m}{\log 2} - 2.$$

This contradicts $m \geq 3$ and $n_0 \geq 3$. Hence, $X = Z$, which implies $X = Y = Z = 1$, as we observed in case (i). ∎

4. The case of $\epsilon = -1$. In the case of $\epsilon = -1$, considering (2.2) modulo 4, we see that either

$$\text{(i) } m_0 \equiv 2 \pmod{4} \text{ and } n = n_0,$$

or

$$\text{(ii) } n_0 \equiv 0 \pmod{4} \text{ and } m = m_0.$$

Consider first the case of $m_0 \equiv 2 \pmod{4}$. Since m is even, reducing equation (1.1) modulo 4, we find that $(-1)^x \equiv 1 \pmod{4}$, that is, x is even. Since we already know by Lemma 2.1 that z is even, we can put $x = 2X$ and $z = 2Z$ with positive integers X and Z, so we obtain $(2mn)^y = DE$ with equations (3.1).

LEMMA 4.1. *If* $m_0 \equiv 2 \pmod{4}$, *then* X *and* Z *are odd.*

Proof. Suppose that X is even. Then, $D \equiv 2 \pmod{4}$ and $D \equiv 2 \pmod{n}$. If Z is even, then $D \equiv 2 \pmod{m_0}$ and $D = 2$, which contradicts $D > E$. If Z is odd, then $D \equiv 0 \pmod{m_0}$ and

$$D = 2m_1^y, \quad E = 2^{(r+1)y-1}n^y,$$

where $m_1 = m_0/2$. However, by (2.2), $n^2 - 2m_1 n + 1 - m^2 = 0$ and

$$n = -m_1 + \sqrt{m_1^2 + m^2 - 1} > m_1(2^r - 1) \geq m_1,$$

which shows that $D = 2m_1^y < 2n^y \leq E$, a contradiction. Hence, X is odd.

Suppose that Z is even. Then $D \equiv 0 \pmod 4$, $D \equiv 2 \pmod{m_0}$, $D \equiv 2 \pmod n$ and

$$D = 2^{(r+1)y-1}, \quad E = 2m_1^y n^y.$$

However, by (2.2), we have

$$n = -m_1 + \sqrt{m_1^2 + m^2 - 1} > m_1(2^r - 1) \geq 2^r - 1,$$

that is, $n \geq 2^r$. Since $m_1 \geq 3$ by $m_0 \geq 6$, we obtain

$$E = 2m_1^y n^y \geq 2 \cdot 3^y 2^{ry} > 2^{(r+1)y} > D,$$

which is a contradiction. Therefore, Z is odd. ∎

By Lemma 4.1, $D = 2^{y-1}m^y$ and $E = 2n^y$. It is clear that $y \geq 2$ and

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

Since $n^2 \equiv -1 \pmod{m_0}$ by (2.3), we have $n^y \equiv -1 \pmod{m_0}$. If y is odd, then $n \equiv \pm 1 \pmod{m_0}$, and hence $n^2 \equiv 1 \pmod{m_0}$, which contradicts $n^2 \equiv -1 \pmod{m_0}$ and $m_0 \geq 3$. Therefore, y is even.

Proof of Theorem 1.2 *in the case of* $\epsilon = -1$ *and* $m_0 \equiv 2 \pmod 4$. Similarly to the case of $\epsilon = 1$ and $m_0 \equiv 0 \pmod 4$, we can show that

$$(y/2 =)\ Y < \frac{\log m_0}{\log 2} + 2, \qquad X \equiv Z \pmod{m_0 n},$$

and this leads to the desired conclusion. ∎

Consider now the case of $n_0 \equiv 0 \pmod 4$. We may write

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

where α, β, i, j are positive integers with i, j odd, and with $\alpha \geq 2$, $\beta \geq 2$ and $e \in \{\pm 1\}$. By (2.2), we have

$$\begin{aligned} \beta + 1 &= \nu_2(m^2 - 1) = \nu_2(n^2 + mn_0) = \nu_2(n_0(2^{2r-2}n_0 + m)) \\ &= \nu_2(n_0) \leq \nu_2(n) = \alpha < 2\alpha. \end{aligned} \tag{4.1}$$

It follows from Lemma 3.1 in [9] that if $y > 1$, then $x \equiv z \pmod 2$; since z is even by Lemma 2.1, x is also even. If $y = 1$, then by (1.1) and (2.2), we have

$$(mn_0 + 1)^x + 2mn \equiv (mn_0 + 1)^z \pmod{n^2},$$

which yields $x + 2^r \equiv z \pmod{n_0}$, in particular, $x \equiv z \pmod 2$ (since $r \geq 1$). Hence, in any case, x and z are even. Put $x = 2X$ and $z = 2Z$.

LEMMA 4.2. *If* $n_0 \equiv 0 \pmod 4$, *then* X *and* Z *are odd.*

Proof. By (4.1) and Lemma 2 in [10], we have $X \equiv Z \pmod 2$. We may write $(2mn)^y = DE$ with (3.1). Suppose that X and Z are even. Then, $D \equiv 2 \pmod 4$, $D \equiv 2 \pmod m$, $D \equiv 2 \pmod{n_0}$, so $D = 2$, which contradicts $D > E$. Hence, X and Z are odd. ∎

By (2.2), we have $(m - n_1)^2 - (2^{2r} + 1)n_1^2 = 1$, where $n_1 = n_0/2$, and we see that

$$n_0 \equiv 0 \pmod{2^{r+2}} \tag{4.2}$$

in the same way as in Lemma 3.2. On the other hand, by Lemma 4.2, $D = 2m^y$ and $E = 2^{y-1}n^y$. We see that $(m^2 + n^2)^Z = (D + E)/2 = m^y + 2^{y-2}n^y$. Hence,

$$m^y \equiv 1 \pmod{n_0}. \tag{4.3}$$

These arguments lead to the following lemma.

LEMMA 4.3. *If* $n_0 \equiv 0 \pmod 4$, *then* y *is even.*

Proof. The proof is similar to the proof of Lemma 3.3 and therefore we omit it. ∎

Proof of Theorem 1.2 *in the case of* $\epsilon = -1$ *and* $n_0 \equiv 0 \pmod 4$. Similarly to the case of $\epsilon = 1$ and $n_0 \equiv 2 \pmod 4$, we can show that

$$(y/2 =)\ Y \le \frac{\log m}{2\log 2}, \quad X \equiv Z \pmod{mn_0/2},$$

and this leads to the desired conclusion. ∎

5. Proof of Theorem 1.3. Assume that $c \equiv -1 \pmod a$. Then, by (1.1) there exists an integer $t > 1$ such that

$$m^2 + n^2 = -1 + (m^2 - n^2)t. \tag{5.1}$$

Putting $M = m + n$ and $N = m - n$, we can rewrite this as

$$(M - Nt)^2 - (t^2 - 1)N^2 = -2. \tag{5.2}$$

Since the fundamental solution (p, q) of the Pell equation $P^2 - (t^2 - 1)Q^2 = 1$ is $(p, q) = (t, 1)$, the fundamental solution (u, v) of the Pell equation $U^2 - (t^2 - 1)V^2 = -2$ satisfies

$$0 < v \le \frac{1}{\sqrt{2(t-1)}} \cdot \sqrt{2} = \frac{1}{\sqrt{t-1}}$$

(cf. [11, Theorem 108a]). Hence, we must have $v = 1$ and $t = 2$. Substituting this into (5.2), we obtain

$$M^2 + N^2 = -2 + 4MN, \tag{5.3}$$

which implies that

$$M^2 \equiv -2 \pmod N, \quad N^2 \equiv -2 \pmod M. \tag{5.4}$$

Lemma 5.1. *y and z are even.*

Proof. By (1.1) and (5.3), we have

$$(MN)^x + (2MN - N^2 - 1)^y = (2MN - 1)^z,$$

which together with (5.4) implies

$$1 \equiv (-1)^z \pmod{M}.$$

Since $M = m+n \geq 3$, z is even. Similarly, we have $(-1)^y \equiv (-1)^z \pmod{N}$, that is, $(-1)^y \equiv 1 \pmod{N}$. If $N = m - n = 1$, then it is known by [2] that $(x, y, z) = (2, 2, 2)$. Hence, we may assume that $N \geq 3$ and y is even. ∎

Putting $y = 2Y$ and $z = 2Z$, we may write

$$(MN)^x = DE,$$

where

$$\begin{aligned} D &= (2MN - 1)^Z + (2MN - N^2 - 1)^Y, \\ E &= (2MN - 1)^Z - (2MN - N^2 - 1)^Y. \end{aligned} \tag{5.5}$$

Lemma 5.2. *Y and Z are odd.*

Proof. Suppose that Z is even. Then, by (5.4) and (5.5), we have $D \equiv 2 \pmod{M}$ and $E \geq M^x > N^x \geq D$, a contradiction. Thus, Z is odd.

Suppose that Y is even. Then, we similarly have $E \equiv -2 \pmod{M}$, $E \equiv -2 \pmod{N}$ and $E = 1$, which implies that $3 \equiv 0 \pmod{M}$. This contradicts $M > N \geq 3$. Hence, Y is odd. ∎

By Lemma 5.2, we have $D \equiv 0 \pmod{M}$, $D \equiv -2 \pmod{N}$ and

$$D = M^x, \quad E = N^x,$$

that is,

$$(m^2 + n^2)^Z + (2mn)^Y = (m + n)^x, \quad (m^2 + n^2)^Z - (2mn)^Y = (m - n)^x.$$

Suppose that x is odd. Then, considering $D + E$ modulo $2m$, we see that $2(n^2)^Z \equiv 0 \pmod{2m}$, that is, $n^{2Z} \equiv 0 \pmod{m}$, which contradicts $\gcd(m, n) = 1$. Hence, x is even. We are now ready to prove Theorem 1.3.

Proof of Theorem 1.3. Putting $x = 2X$, we may write equations (3.3) and we have inequalities (3.4). Then

$$\begin{aligned} k^2 &= \frac{1}{2}\{(m^2 - n^2)^X + (m^2 + n^2)^Z\} \\ &= \frac{1}{2}\left\{(MN)^X + \frac{1}{2}(D + E)\right\} = \left\{\frac{1}{2}(M^X + N^X)\right\}^2, \end{aligned}$$

in other words, $k = (M^X + N^X)/2$. Similarly, we have $l = (M^X - N^X)/2$.

Suppose now that X is even. Then, $k \equiv n^X \pmod{m}$ and $k \equiv m^X \pmod{n}$. This implies that k is prime to mn. But, since k is a divisor of $(2mn)^Y$, we must have $k = 1$, which is clearly absurd. Therefore, X is odd. Since $M = m + n$ and $N = m - n$, as we observed in the case of $\epsilon = 1$ and $m_0 \equiv 0 \pmod 4$, we see that

$$Y\nu_2(2mn) = \nu_2(M^2 - N^2) - 1 = \nu_2(2mn).$$

It follows that $Y = 1$, and, by (3.4), we obtain $X = Z = 1$. ■

We conclude this paper by considering the cases of $c \equiv \epsilon 2^r \pmod a$ with $(\epsilon, r) \neq (-1, 0)$. By (1.2), we may write

$$m^2 + n^2 = \epsilon 2^r + (m^2 - n^2)t$$

for some positive integer t, and putting $M = m+n$ and $N = m-n$ we have

$$(M - Nt)^2 - (t^2 - 1)N^2 = \epsilon 2^{r+1}. \tag{5.6}$$

If $(\epsilon, r) = (1, 0)$, then, since the fundamental solution (u, v) of the Pell equation

$$U^2 - (t^2 - 1)V^2 = 2 \tag{5.7}$$

satisfies $0 \le v \le 1/\sqrt{t+1}$ by [11, Theorem 108], we have $v = 0$, which does not give a solution of (5.7). Hence, $c \not\equiv 1 \pmod a$.

If $(\epsilon, r) = (1, 1)$, then the fundamental solution (u, v) of the Pell equation $U^2 - (t^2 - 1)V^2 = 4$ satisfies $0 \le v \le \sqrt{2/(t+1)}$. If $t \ge 2$, then $v = 0$, which means that N is even, a contradiction. Thus, $t = 1$ and $n = 1$, where $(x, y, z) = (2, 2, 2)$ by [8].

In all other cases, (1.1) and (5.6) together imply that

$$M^2 \equiv \epsilon 2^{r+1} \pmod N, \quad N^2 \equiv \epsilon 2^{r+1} \pmod M,$$
$$(MN)^x + (MNt + \epsilon 2^r - N^2)^y = (MNt + \epsilon 2^r)^z,$$

and

$$(-\epsilon 2^r)^y \equiv (\epsilon 2^r)^z \pmod M, \quad (\epsilon 2^r)^y \equiv (\epsilon 2^r)^z \pmod N.$$

It seems difficult to deduce the evenness of y and z from these congruences. This is why we did not treat the cases of $c \equiv \epsilon 2^r \pmod a$, other than $c \equiv -1 \pmod a$.

Acknowledgements. The authors are grateful to the referee for the helpful comments. The second author is supported by JSPS Research Fellowships for Young Scientists.

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] Y. Fujita, *The non-extensibility of $D(4k)$-triples $\{1, 4k(k-1), 4k^2+1\}$ with $|k|$ prime*, Glas. Mat. Ser. III 41 (2006), 205–216.
[5] L. Jeśmanowicz, *Several remarks on Pythagorean numbers*, Wiadom. Mat. 1 (1955/1956), 196–202 (in Polish).
[6] M.-H. Le, *A note on Jeśmanowicz conjecture*, Colloq. Math. 69 (1995), 47–51.
[7] M.-H. Le, *A note on Jeśmanowicz' conjecture concerning primitive Pythagorean triplets*, Acta Arith. 138 (2009), 137–144.
[8] 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).
[9] T. Miyazaki, *On the conjecture of Jeśmanowicz concerning Pythagorean triples*, Bull. Austral. Math. Soc. 80 (2009), 413–422.
[10] T. Miyazaki, *Generalizations of classical results on Jeśmanowicz' conjecture concerning Pythagorean triples*, in: Diophantine Analysis and Related Fields 2010, AIP Conf. Proc. 1264, Amer. Inst. Phys., Melville, NY, 2010, 41–51.
[11] T. Nagell, *Introduction to Number Theory*, Almqvist, Stockholm, and Wiley, New York, 1951.
[12] W. Sierpiński, *On the equation $3^x + 4^y = 5^z$*, Wiadom. Mat. 1 (1955/1956), 194–195 (in Polish).

Yasutsugu Fujita
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

Takafumi Miyazaki
Department of Mathematics and Information Sciences
Tokyo Metropolitan University
1-1 Minami-Ohsawa
Hachioji, Tokyo, Japan
E-mail: miyazaki-takafumi@tmu.ac.jp

Received 1 April 2012;
revised 17 September 2012 (5658)