ACTA ARITHMETICA
138.2 (2009)

A note on Jeśmanowicz' conjecture concerning primitive Pythagorean triplets

by

Maohua Le (Zhanjiang)

1. Introduction. Let $\mathbb{N},\mathbb{R}$ be the sets of all positive integers and real numbers respectively. Let (a,b,c) be a primitive Pythagorean triplet such that

$$(1)\qquad a^2+b^2=c^2,\quad a,b,c\in\mathbb{N},\quad \gcd(a,b,c)=1,\quad 2\mid b.$$

Then we have

$$(2)\qquad a=s^2-t^2,\quad b=2st,\quad c=s^2+t^2,$$

where s,t are positive integers satisfying $s>t, 2\mid st$ and $\gcd(s,t)=1$. In 1956, L. Jeśmanowicz [5] conjectured that the equation

$$(3)\qquad a^x+b^y=c^z,\quad x,y,z\in\mathbb{N},$$

has only the solution $(x,y,z)=(2,2,2)$. This problem was solved for some special cases (see [6] and its references). For example, V. A. Dem'yanenko [3] proved that if $s-t=1$, then the conjecture is true. But, in general, this problem is not solved yet. Because the equation (3) relates to a generalization of Fermat's last theorem (see Problem B19 of [4]), it seems that the conjecture is a very difficult problem.

Since $\gcd(a,c)=1$ by (1), there exists some positive integers n such that

$$(4)\qquad a^n\equiv\lambda \pmod{c},\quad \lambda\in\{-1,1\}.$$

Let d denote the least positive integer n satisfying (4). In this paper we deal with the case where

$$(5)\qquad \gcd\left(c,\frac{a^d-\lambda}{c}\right)=1.$$

In fact, there are many primitive Pythagorean triplets (a,b,c) which have the property (5). For example, if $s-t=1$, then $a=2t+1$, $c=2t^2+2t+1$ and

---

2000 *Mathematics Subject Classification*: Primary 11D61.
Key words and phrases: exponential diophantine equation, primitive Pythagorean triplet, Jeśmanowicz' conjecture.

DOI: 10.4064/aa138-2-3

$a^2 = 2c-1$. This implies that $d = 2$ and (5) holds. Using the Gel'fond–Baker method, we prove a general result as follows.

THEOREM. *Let* (a, b, c) *be a positive Pythagorean triplet satisfying* (5). *If* $c > 4 \cdot 10^9$, *then* (3) *has only the solution* $(x, y, z) = (2, 2, 2)$.

2. Preliminaries. Let (a, b, c) be a primitive Pythagorean triplet with (1). Then a solution (x, y, z) of (3) will be called *exceptional* if $(x, y, z) \neq (2, 2, 2)$.

LEMMA 1. *Let* $f(X) \in \mathbb{R}[X]$ *be a polynomial of degree* n. *If there exist a real number* α_0 *such that* $\alpha_0 > \max(0, f(\log \alpha_0), f^{(1)}(\log \alpha_0), \ldots, f^{(n)}(\log \alpha_0))$, *where* $f^{(j)}(X)$ $(j = 1, \ldots, n)$ *is the* j*th derivative of* $f(X)$, *then* $\alpha > f(\log \alpha)$ *for any real number* α *with* $\alpha \geq \alpha_0$.

Proof. For a real variable X, let

$$g(X) = X - f(\log X), \qquad X > 0, \tag{6}$$

and

$$g_m(X) = X - f^{(m)}(\log X), \quad X > 0,\ m = 1, \ldots, n+1. \tag{7}$$

Then $g(X)$ and $g_m(X)$ $(m = 1, \ldots, n+1)$ are continuous and differentiable functions. Further let $g'(X)$ and $g'_m(X)$ denote the derivatives of $g(X)$ and $g_m(X)$ respectively. We see from (6) and (7) that

$$g'(X) = \frac{g_1(X)}{X}, \qquad X > 0, \tag{8}$$

and

$$g'_{m-1}(X) = \frac{g_m(X)}{X}, \quad X > 0,\ m = 2, \ldots, n+1. \tag{9}$$

Since $f(X)$ is a polynomial of degree n, we have $f^{(n+1)}(X) = 0$. Hence, by (7), we get $g_{n+1}(X) = X > 0$, and by (9), we obtain $g'_n(X) > 0$ for $X > 0$. This implies that $g_n(X)$ is an increasing function. Further, since $\alpha_0 > f^{(n)}(\log \alpha_0)$, we see from (7) that $g_n(\alpha_0) > 0$. Therefore, we get $g_n(X) > 0$ for $X \geq \alpha_0$. By the same method, we can successively prove that $g_{n-1}(X) > 0, \ldots, g_1(X) > 0$ and $g(X) > 0$ for $X \geq \alpha_0$. Thus, by (6), we get $X > f(\log X)$ for $X \geq \alpha_0$. The lemma is proved.

LEMMA 2. $a > \sqrt{c}$ *and* $b > \sqrt{2c}$.

Proof. By (2), we get

$$a = s^2 - t^2 = (s+t)(s-t) \geq s + t > \sqrt{s^2 + t^2} = \sqrt{c}.$$

Since $s > t \geq 1$, we have $(2s^2 - 1)(2t^2 - 1) > 1$. This implies that $b^2 = 4s^2t^2 > 2(s^2 + t^2) = 2c$ and $b > \sqrt{2c}$. The lemma is proved.

Lemma 3. *If* (x,y,z) *is an exceptional solution of* (3), *then* $x \neq y$ *and* $z > 2$.

Proof. If $x = y$, then from (1) and (3) we get $a^2 \equiv -b^2 \pmod{c}$ and $a^x \equiv -b^x \pmod{c}$ respectively. Hence, we have $a^{2x} \equiv (-1)^x b^{2x} \equiv b^{2x} \pmod{c}$. Since $\gcd(b,c) = 1$, x must be even. Let $x = 2t$, where t is a positive integer. Then we have $a^{2t} \equiv (-1)^t b^{2t} \equiv -b^{2t} \pmod{c}$. This implies that t must be odd. Further, since $(x,y,z) \neq (2,2,2)$, we get $t \geq 3$. Therefore, by Lemma 2, we obtain $c^z \geq a^6 + b^6 > 3c^3$ and $z \geq 4$. By (1) and (3), we get

$$0 \equiv c^{z-2} \equiv \frac{a^{2t} + b^{2t}}{a^2 + b^2} \equiv a^{2t-2} t \pmod{c^2}. \tag{10}$$

Since $\gcd(a,c) = 1$, we see from (10) that $c^2 \mid t$ and

$$t \geq c^2 \geq 25. \tag{11}$$

On the other hand, let $X = a^2$ and $Y = -b^2$. We see from (1) and (3) that $X - Y = a^2 + b^2 = c^2$ and $X^t - Y^t = a^{2t} + b^{2t} = c^z$. This implies that $X^t - Y^t$ has no primitive divisor. Therefore, by an earlier result of G. D. Birkhoff and H. S. Vandiver [1], we have $t \leq 6$, a contradiction with (11). Thus, we obtain $x \neq y$.

By Lemma 2, if $\max(x,y) > 1$, then $z > 1$. This implies that (3) has no solution (x,y,z) with $z = 1$. Similarly, if $z = 2$, then we have $\min(x,y) = 1$ and $\max(x,y) = 3$. When $(x,y) = (1,3)$, since $c^2 = a^2 + b^2 = a + b^3$, we get

$$a(a-1) = b^2(b-1). \tag{12}$$

Since $\gcd(a,b) = 1$, by (12), we obtain $b^2 \mid a-1$ and $c > a > a-1 \geq b^2 > 2c$, a contradiction. By the same method, we can eliminate the case where $(x,y) = (3,1)$. Thus, we get $z > 2$. The lemma is proved.

Lemma 4 ([8, Lemma 1]). *If* (5) *holds and* $a^n \equiv \lambda' \pmod{c^r}$ *for some positive integers* n *and* r, *where* $\lambda' \in \{-1,1\}$, *then* $dc^{r-1} \mid n$.

Lemma 5. *If* (5) *holds and* (x,y,z) *is an exceptional solution*, *then* $|x-y| \geq c$.

Proof. By (1) and (3), we get $a^2 \equiv -b^2 \pmod{c^2}$ and $a^x \equiv -b^y \pmod{c^z}$ respectively. Since $z > 2$ by Lemma 3, we have $a^{2y} \equiv (-1)^y b^{2y} \equiv (-1)^y a^{2y} \pmod{c^z}$. Further, since $\gcd(a,c) = 1$ by (1), we obtain

$$a^{2|x-y|} \equiv (-1)^y \pmod{c^z}. \tag{13}$$

Furthermore, since $x \neq y$ by Lemma 3, $|x-y|$ is a positive integer. Therefore, by Lemma 4, we see from (13) that $dc \mid 2|x-y|$ and $2|x-y| \geq dc$. Since $c > a$ by (2), we have $d \geq 2$ by (4). Thus, we obtain $|x-y| \geq dc/2 \geq c$. The lemma is proved.

LEMMA 6 ([7, Lemma 5]). *Let $\alpha_1, \alpha_2, \beta_1, \beta_2$ be positive integers with* $\min(\alpha_1, \alpha_2) > 10^3$, *and let $\Lambda = \beta_1 \log \alpha_1 - \beta_2 \log \alpha_2$. If $\Lambda \neq 0$, then*

$$\log |\Lambda| > -17.61(\log \alpha_1)(\log \alpha_2)(1.7735 + B)^2,$$

where

$$B = \max\left(8.445, 0.2257 + \log\left(\frac{\beta_1}{\log \alpha_2} + \frac{\beta_2}{\log \alpha_2}\right)\right).$$

LEMMA 7 ([2, Theorem 2]). *Let α_1, α_2 be positive odd integers, and let β_1, β_2 be positive integers. Further, let $\Lambda' = \alpha_1^{\beta_1} - \alpha_2^{\beta_2}$. If $\Lambda' \neq 0$ and $\alpha_1 \equiv 1$* (mod 4), *then*

$$\operatorname{ord}_2 \Lambda' \leq 208(\log \alpha_1)(\log \alpha_2)(\log \beta')^2,$$

where $\operatorname{ord}_2 \Lambda'$ *is the order of* 2 *in* Λ',

$$\log B' = \max\left(10, 0.04 + \log\left(\frac{\beta_1}{\log \alpha_2} + \frac{\beta_2}{\log \alpha_1}\right)\right).$$

LEMMA 8. *Let* $\min(a, b, c) > 10^3$. *If $a^x > b^{2y}$ or $b^y > a^{2x}$, then $x < 4500 \log c$ or $y < 4500 \log c$.*

Proof. We first consider the case of $a^x > b^{2y}$. Then, by (3), we get

$$z \log c = \log(a^x + b^y) = \log a^x + \frac{2b^y}{2a^x + b^y} \sum_{i=0}^{\infty} \frac{1}{2i+1}\left(\frac{b^y}{2a^x + b^y}\right)^{2i} \tag{14}$$

$$= x \log a + \frac{2b^y}{a^x + c^z} \sum_{i=0}^{\infty} \frac{1}{2i+1}\left(\frac{b^y}{a^x + c^z}\right)^{2i}$$

$$< x \log a + \frac{b^y}{a^x} \sum_{i=0}^{\infty} \frac{1}{2i+1}\left(\frac{b^y}{a^x}\right)^{2i}$$

$$< x \log a + \frac{1}{a^{x/2}} \sum_{i=0}^{\infty} \frac{1}{2i+1}\left(\frac{1}{a^x}\right)^{i} < x \log a + \frac{2}{a^{x/2}}.$$

Let $\alpha_1 = c$, $\alpha_2 = a$, $\beta_1 = z$, $\beta_2 = x$ and $\Lambda = z \log c - x \log a$. We see from (14) that

$$0 < \Lambda < \frac{2}{a^{x/2}}. \tag{15}$$

On the other hand, since $\min(a, c) > 10^3$, by Lemma 6, we have

$$\log \Lambda > -17.61(\log c)(\log a)(1.7735 + B)^2, \tag{16}$$

where

$$B = \max\left(8.445, 0.2257 + \log\left(\frac{z}{\log a} + \frac{x}{\log c}\right)\right). \tag{17}$$

The combination of (15) and (16) yields

$$\log 2 + 17.61(\log c)(\log a)(1.7735 + B)^2 > \frac{x}{2}\log a. \tag{18}$$

Further, since $\min(a, c) > 10^3$, and $B \geq 8.445$ by (17), we get

$$17.61(\log c)(\log a)(1.7735 + B)^2 > 3360.$$

Therefore, by (18), we obtain

$$\frac{x}{\log c} < 35.24(1.7735 + B)^2. \tag{19}$$

When $8.445 \geq 0.2257 + \log(z/\log a + x/\log c)$, we deduce from (19) that $x < 3680 \log c$, so the assertion of the lemma holds in this case.

When $8.445 < 0.2557 + \log(z/\log a + x/\log c)$, we have

$$\frac{x}{\log c} < 35.25\biggl(1.9992 + \log\biggl(\frac{z}{\log a} + \frac{x}{\log c}\biggr)\biggr)^2. \tag{20}$$

By (14), we get

$$\frac{z}{\log a} < \frac{x}{\log c} + \frac{2}{a^{x/2}(\log a)(\log c)} < \frac{6x}{5\log c}. \tag{21}$$

Hence, by (20) and (21), we obtain

$$\frac{x}{\log c} < 35.25\biggl(2.7878 + \log\frac{x}{\log c}\biggr)^2. \tag{22}$$

Let $f(X) = 35.25(2.7878+X)^2$. Then $f(X) \in \mathbb{R}[X]$ is a polynomial of degree two, $f^{(1)}(X) = 70.5(2.7878 + X)$ and $f^{(2)}(X) = 70.5$. Let $\alpha_0 = 4500$. Since $\alpha_0 > \max(0, f(\log\alpha_0), f^{(1)}(\log\alpha_0), f^{(2)}(\log\alpha_0))$, by Lemma 1, we have

$$\alpha > 35.25(2.7878 + \log\alpha)^2, \qquad \alpha \in \mathbb{R}, \alpha \geq 4500. \tag{23}$$

Therefore, we see from (22) and (23) that $x < 4500 \log c$. Thus, the assertion of the lemma holds for $a^x > b^{2y}$.

By using the same method, we can prove that if $b^y > a^{2x}$, then $y < 4500 \log c$. This completes the proof.

3. Proof of Theorem. We now suppose that (3) has an exceptional solution (x, y, z). We will reach a contradiction in each of the following four cases.

Case I: $a^x > b^{2y}$. Since $a^x > b^{2y}$, by Lemma 2, if $y \geq x$, then $a^x > b^{2y} \geq b^{2x} > c^x > a^x$, a contradiction. So we have $y < x$ and $|x - y| = x - y < x$. Hence, by Lemma 5, we obtain

$$c < x. \tag{24}$$

On the other hand, by Lemma 8, we have

$$x < 4500 \log c. \tag{25}$$

The combination of (24) and (25) yields

$$c < 4500 \log c. \tag{26}$$

Let $f[X] = 4500X$. Then $f(X) \in \mathbb{R}[X]$ is a polynomial of degree one, and $f^{(1)}(X) = 4500$. Let $\alpha_0 = 37000$. Since $\alpha_0 > \max(0, f(\log \alpha_0), f^{(1)}(\log \alpha_0))$, by Lemma 1, we see from (26) that $c < 37000$, a contradiction with $c > 4{\cdot}10^9$.

Case II: $b^{2y} > a^x > b^y$. Since $b^{2y} > a^x$, by Lemma 2, we have $c^{2y} > b^{2y} > a^x > c^{x/2}$. This implies that $y > x/4$ and $|x - y| < 4y$. Hence, by Lemma 5, we get

$$c < 4y. \tag{27}$$

Let $\alpha_1 = c$, $\alpha_2 = a$, $\beta_1 = z$, $\beta_2 = x$ and $\Lambda' = c^z - a^x$. Then, by (1) and (2), we have $\Lambda' = b^x$, $\mathrm{ord}_2 \Lambda' = y \,\mathrm{ord}_2 b$, $\mathrm{ord}_2 b \geq 2$ and

$$\mathrm{ord}_2 \Lambda' \geq 2y. \tag{28}$$

On the other hand, since $c \equiv 1 \pmod 4$, by Lemma 7, we have

$$\mathrm{ord}_2 \Lambda' \leq 208(\log c)(\log a)(\log B')^2, \tag{29}$$

where

$$\log B' = \max\left(10, 0.04 + \log\left(\frac{z}{\log a} + \frac{x}{\log c}\right)\right). \tag{30}$$

The combination of (28) and (29) yields

$$2y \leq 208(\log c)(\log a)(\log B')^2. \tag{31}$$

When $10 \geq 0.04 + \log(z/\log a + x/\log c)$, we infer from (27), (30) and (31) that

$$c < 41600(\log c)(\log a) < 41600(\log c)^2. \tag{32}$$

Let $f[X] = 41600X^2$. Then $f(X) \in \mathbb{R}[X]$, $f^{(1)}(X) = 83200X$ and $f^{(2)}(X) = 83200$. Let $\alpha_0 = 1.2 \cdot 10^7$. Since

$$\alpha_0 > \max(0, f(\log \alpha_0), f^{(1)}(\log \alpha_0), f^{(2)}(\log \alpha_0)),$$

by Lemma 1, we see from (32) that $c < 1.2 \cdot 10^7$, a contradiction.

When $10 < 0.04 + \log(z/\log a + x/\log c)$, we have

$$y < 104(\log c)(\log a)\left(0.04 + \log\left(\frac{z}{\log a} + \frac{x}{\log c}\right)\right)^2. \tag{33}$$

Since $a^x > b^y$, we have $2a^x > c^z$ by (3). Further, since $b^{2y} > a^x$, we get $c^{2y+1} > b^{2y+1} > a^x b > 2a^x > c^z$. This implies that $2y \geq z$. Therefore, by (33), we obtain

$$(34)\qquad \frac{z}{\log a} < 208(\log c)\left(0.04+\log\left(\frac{z}{\log a}+\frac{x}{\log c}\right)\right)^2$$
$$< 208(\log c)\left(0.04+\log\frac{2z}{\log a}\right)^2 < 208(\log c)\left(0.7332+\log\frac{z}{\log a}\right)^2.$$

Let $f[X]=208(\log c)(0.7332+X)^2$. Then $f^{(1)}(X)=416(\log c)(0.7332+X)$ and $f^{(2)}(X)=416\log c$. Let $\alpha_0=2080(\log c)^3$. Since $c>4\cdot 10^9$, we have $\alpha_0>\max(0, f(\log\alpha_0), f^{(1)}(\log\alpha_0), f^{(2)}(\log\alpha_0))$. Therefore, by Lemma 1, we see from (34) that

$$(35)\qquad \frac{z}{\log a} < 2080(\log c)^3,$$

whence we get

$$(36)\qquad z < 2080(\log c)^4.$$

By Lemma 2, we see from (3) that $c^z > b^y > c^{y/2}$ and $z > y/2$. Therefore, by (27) and (36), we obtain

$$(37)\qquad c < 16640(\log c)^4.$$

Let $f[X]=16640X^4$ and $\alpha_0=4\cdot 10^9$. Then we have $\alpha_0>\max(0, f(\log\alpha_0), f^{(1)}(\log\alpha_0), f^{(2)}(\log\alpha_0), f^{(3)}(\log\alpha_0), f^{(4)}(\log\alpha_0))$. Thus, we see from (37) that $c<4\cdot 10^9$, a contradiction.

Case III: $a^{2x} > b^y > a^x$. By Lemma 2, we have $c^y > b^y > a^x > c^{x/2}$ and $y > x/2$. This implies that $|x-y| < 2y$. Further, by Lemma 5, we get

$$(38)\qquad c < 2y.$$

Thus, by Lemma 7, using the same method as in the proof of Case II, we can deduce from (38) that $c < 4\cdot 10^9$, a contradiction.

Case IV: $b^y > a^{2x}$. By Lemma 2, we have $c^y > b^y > a^{2x} > c^x$ and $y > x$. This implies that $|x-y| < y$. Further, by Lemma 5, we get

$$(39)\qquad c < y.$$

On the other hand, by Lemma 8, we have

$$(40)\qquad y < 4500\log c.$$

The combination of (39) and (40) yields (26). Thus, using the same method as in the proof of Case I, we can deduce from (36) that $c < 37000$, a contradiction.

To sum up, the theorem is proved.

Acknowledgements. This research was supported by the National Natural Science Foundation of China (No. 10771186) and the Guangdong Provincial Natural Science Foundation (No. 06029035).

References

[1] G. D. Birkhoff and H. S. Vandiver, *On the integral divisors of* $a^n - b^n$, Ann. of Math. (2) 5 (1904), 173–180.

[2] Y. Bugeaud, *Linear forms in p-adic logarithms and the diophantine equation* $(x^n - 1)/(x - 1) = y^q$, Math. Proc. Cambridge Philos. Soc. 127 (1999), 373–381.

[3] V. A. Dem'yanenko, *On Jeśmanowicz' problem for Pythagorean numbers*, Izv. Vyssh. Uchebn. Zaved. Mat. 1965, no. 5, 52–56 (in Russian).

[4] R. K. Guy, *Unsolved Problems in Number Theory*, 3rd ed., Springer, New York, 2004.

[5] L. Jeśmanowicz, *Several remarks in Pythagorean numbers*, Wiadom. Mat. (2) 1 (1955/1956), 196–202 (in Polish).

[6] M. H. Le, *A note on Jeśmanowicz' conjecture*, Colloq. Math. 64 (1995), 47–51.

[7] —, *On the exponential diophantine equation* $(m^3 - 3m)^x + (3m^2 - 1)^y = (m^2 + 1)^z$, Publ. Math. Debrecen 58 (2001), 461–466.

[8] K. Möller, *Untere Schranke für die Anzahl der Primzahlen*, *aus denen* x, y, z *der Fermatschen Gleichung* $x^n + y^n = z^n$ *bestehen muss*, Math. Nachr. 14 (1955), 25–28.

Department of Mathematics
Zhanjiang Normal College
Zhanjiang, Guangdong 524048, P.R. China
E-mail: lemaohua2008@163.com

Received on 31.3.2008
and in revised form on 18.9.2008 (5679)