A Remark on Jeśmanowicz' Conjecture

By Kei TAKAKUWA

Department of Mathematics, Gakushuin University

(Communicated by Shokichi IYANAGA, M. J. A., June 11, 1996)

1. Introduction. Let (a, b, c) be a primitive Pythagorean triple such that

(1) $a^2 + b^2 = c^2, a, b, c \in \boldsymbol{N}, (a, b) = 1, 2 \mid b.$

Then we have

(2) $a = r^2 - s^2, b = 2rs, c = r^2 + s^2$

where $r, s \in \boldsymbol{N}, (r, s) = 1, r > s, r \equiv s + 1 \pmod{2}$.

In [1], L.Jeśmanowicz conjectured that the equation

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

has then the only solution $(x, y, z) = (2, 2, 2)$. This conjecture has been proved to be true in many special cases. In particular, Maohua Le [2] proved the following theorem:

Theorem 1. *Let a, b and c be as in* (2) *with* $2 \parallel r$, $s \equiv 3 \pmod{4}$ *and* $r \geqq 81s$. *Then the only solution of* (3) *is* $(x, y, z) = (2, 2, 2)$.

The proof of this theorem in [2] is based on the following lemma:

Lemma ([3, Lemma 2]). *Let (x, y, z) be a solution of* (3) *with* $(x, y, z) \neq (2, 2, 2)$. *If* $2 \parallel r$ *and* $s \equiv 3 \pmod{4}$, *then we have* $2 \mid x, y = 1$ *and* $2 \nmid z$.

In fact, a weaker result ($r \geqq 6000$ and $s = 3$ instead of $r \geqq 81s$) had been obtained by Yongdong Guo and Maohua Le in [3] applying the Baker theory; then the above Theorem 1 was proved in [2] with the aid of a stronger result of the same theory.

In this paper, we shall show that the condition $r \geqq 81s$ can be eliminated from Theorem 1 for $s = 3, 7, 11, 15$; i.e. we shall prove the following theorem:

Theorem 2. *Let a, b and c be as in* (2) *with* $2 \parallel r$, $s = 3, 7, 11,$ *and* 15. *Then the only solution of* (3) *is* $(x, y, z) = (2,2,2)$.

2. Proof. We have to show that the existence of $(x, y, z) \neq (2, 2, 2)$ for (a, b, c) as in (2) with $2 \parallel r$, $s = 3, 7, 11, 15$ leads to a contradiction. The above Lemma says that in this hypothesis, we should have $2 \mid x, y = 1$ and $2 \nmid z$. Thus we see that the proof is reduced to that of the following Propositions 1, 2.

<u>*Notation*</u> For any integer i prime to a given prime p, let $d(i, p)$ be the order of i modulo p.

Proposition 1. *Let $a, b, c \in \boldsymbol{N}$ as in* (2) *with* $2 \parallel r$, $s \equiv 3 \pmod{4}$ *and* $x, y, z \in \boldsymbol{N}$ *with* $2 \mid x, y = 1, 2 \nmid z$. *Then the existence of* a *prime p satisfying any one of the following eight conditions is a contradiction.*

(*i*) $a \equiv \pm 1 \pmod{p}$ *and* $c^i \not\equiv 1 + b \pmod{p}$ *for any* $i (1 \leqq i \leqq p)$.

(*ii*) $c \equiv F \pmod{p}$ *and* $a^i \not\equiv F - b \pmod{p}$ *for any* $i (1 \leqq i \leqq p)$, *where* $F = \pm 1$.

(*iii*) $c \equiv 0 \pmod{p}$ *and* $a^i \not\equiv - b \pmod{p}$ *for any* $i (1 \leqq i \leqq p)$.

(*iv*) $a \equiv 0 \pmod{p}$ *and* $c^i \not\equiv b \pmod{p}$ *for any* $i (1 \leqq i \leqq p)$.

(*v*) $r \equiv 0 \pmod{p}, p \equiv 1 \pmod{4}$ *and* $4 \mid d(s, p)$.

(*vi*) $s \equiv 0 \pmod{p}, p \equiv 1 \pmod{4}$ *and* $4 \mid d(r, p)$.

(*vii*) $a \equiv \pm 1 \pmod{p}, c^m \equiv 1 + b \pmod{p}$ *for some* $m (1 \leqq m \leqq p, 2 \mid m)$ *and* $2 \mid d(c, p)$.

(*viii*) $c \equiv F \pmod{p}, a^n \equiv F - b \pmod{p}$ *for some* $n (1 \leqq n \leqq p, 2 \nmid n)$ *and* $2 \mid d(a, p)$, *where* $F = \pm 1$.

Proposition 2. *Let a, b, c, x, y, z be as above,* $2 \parallel r$, $1 < r < 81s$ *and* $s = 3, 7, 11, 15$. *Then there does exist* a *prime p satisfying one of the conditions* $(i), \ldots, (viii)$ *for each triple* (a, b, c).

Proof of Proposition 1. Case (*i*): From (3), $2 \mid x$ and $y = 1$, we have

(4) $c^z \equiv 1 + b \pmod{p}$.

From (*i*), (4) is a contradiction.

Case (*ii*): From (3), $2 \nmid z$ and $y = 1$, we have

(5) $a^x \equiv F - b \pmod{p}$.

From (*ii*), (5) is a contradiction.

Case (*iii*): From (3) and $y = 1$, we have

(6) $a^x \equiv - b \pmod{p}$.

From (*iii*), (6) is a contradiction.

Case (*iv*): From (3) and $y = 1$, we have

(7) $$c^z \equiv b(\mathrm{mod.}\ p).$$

From (*iv*), (7) is a contradiction.

Case (*v*): From (3) and $2 \mid x$, we have

$$s^{2|x-z|} \equiv 1(\mathrm{mod.}\ p).$$

Then we have $d(s, p) \,\Big|\, 2\,|x-z|$. Since $4 \,\Big|\, d(s, p)$, we see that $x \equiv z\ (\mathrm{mod.}\ 2)$, which is a contradiction.

Case (*vi*): From (3), we have

$$r^{2|x-z|} \equiv 1(\mathrm{mod.}\ p).$$

Then we have $d(r, p) \,\Big|\, 2\,|x-z|$. Since $4 \,\Big|\, d(r, p)$, we see that $x \equiv z\ (\mathrm{mod.}\ 2)$, which is a contradiction.

Case (*vii*): From (4), we have

$$c^{|z-m|} \equiv 1(\mathrm{mod.}\ p).$$

Then we have $d(c, p) \mid z - m$. Since $d(c, p) \equiv m \equiv 0\ (\mathrm{mod.}\ 2)$, we see that $2 \mid z$, which is a contradiction.

Case (*viii*): From (5), we have

$$a^{|x-n|} \equiv 1(\mathrm{mod.}\ p).$$

Then we have $d(a, p) \mid x - n$. Since $d(a, p) \equiv 0$ and $n \equiv 1\ (\mathrm{mod.}\ 2)$, we see that $2 \nmid x$, which is a contradiction. Q.E.D.

Proof of Proposition 2. We could find primes for each triple (a, b, c) as in (2) with $2 \parallel r$, $1 < r < 81s$, $s = 3, 7, 11$ and 15 using computer language system UBASIC86 (The Table below shows some of the results with larger primes).

s	r	a	b	c	p	Satisfied condition
3	70	4891	420	4909	1223	(*i*)
3	142	20155	852	20173	3359	(*i*)
11	602	362283	13244	362525	181141	(*i*)
11	842	708843	18524	709085	354421	(*i*)
15	826	682051	24780	682501	4547	(*vii*)
7	362	130995	5068	131093	2521	(*ii*)
15	622	386659	18660	387109	10753	(*ii*)
7	230	52851	3220	52949	4073	(*iii*)
7	382	145875	5348	145973	36469	(*vii*)

Thus the proof of Theorem 2 is completed.

References

[1] L.Jeśmanowicz: Kilka uwag o liczbach pitagorejwkich (Some remarks on Pythagorean numbers). Wiadom. Mat., (2) **1**, 196–202 (1955/1956) (in Polish).

[2] M.-H. Le: On Jeśmanowicz' conjecture concerning Pythagorean numbers. Proc. Japan Acad., **72A**, 97–98 (1996).

[3] Y.-D. Guo and M.-H. Le: A note on Jeśmanowicz' conjecture concerning Pythagorean numbers. Comment. Mat., Univ. St. Pauli, **44**, no. 2, 225–228 (1995).

[4] Y. Kida: UBASIC86 Ver. 8.7h (1995).