57. *On a Conjecture on Pythagorean Numbers*

By Kei TAKAKUWA and You ASAEDA

Department of Mathematics, Gakushuin University

(Communicated by Shokichi IYANAGA, M. J. A., Sept. 13, 1993)

L. Jeśmanowicz [1] conjectured that if u, v, w are Pythagorean numbers, i.e. positive integers with $(u, v) = (v, w) = (w, u) = 1$ satisfying $u^2 + v^2 = w^2$, then the diophantine equation on $l, m, n \in \boldsymbol{N}$

$$u^l + v^m = w^n$$

has the only solution $(l, m, n) = (2,2,2)$. (Cf. [2].) Since u, v, w are Pythagorean numbers, we have

$$u = x^2 - y^2,\ v = 2xy,\ w = x^2 + y^2,$$

where $x, y \in \boldsymbol{N}$, with $(x, y) = 1$, $x > y$, $x \not\equiv y \pmod 2$.

We shall consider here the following diophantine equation on $l, m, n \in \boldsymbol{N}$

(1) $$(4a^2 - y^2)^l + (4ay)^m = (4a^2 + y^2)^n$$

where $a, y \in \boldsymbol{N}$ *with* $(a, y) = 1$, $2a > y$, $y \equiv 3 \pmod 4$, whence l is even, which is easily seen considering (1) mod 4.

Proposition 1. *If a is odd, then* $m \equiv n \pmod 2$ *and* $m \neq 1 \Leftrightarrow n$ *is even.*

Proof. From (1) we have $(4ay)^m \equiv (2y^2)^n \pmod{4a^2 - y^2}$. By the assumptions on a, y,

$$\left(\frac{2^{2m}a^m y^m}{4a^2 - y^2}\right) = (-1)^m = \left(\frac{2^n y^{2n}}{4a^2 - y^2}\right) = (-1)^n,$$

where $\left(\frac{*}{*}\right)$ is the Jacobi symbol. Hence $m \equiv n \pmod 2$. If n is even, $m \neq 1$. If n is odd, $(4a^2 + y^2)^n \equiv 5 \pmod 8$ and $(4a^2 - y^2)^l \equiv 1 \pmod 8$. Then we have $(4ay)^m \equiv 4 \pmod 8$ from (1), hence $m = 1$.

Proposition 2. *If a is even, then* m *is even.*

Proof. From (1) we have $(4ay)^m \equiv (2y^2)^n \pmod{4a^2 - y^2}$. By the assumptions on a, y,

$$\left(\frac{2^{2m}a^m y^m}{4a^2 - y^2}\right) = (-1)^m = \left(\frac{2^n y^{2n}}{4a^2 - y^2}\right) = 1.$$

Hence m is even.

Proposition 3. *If a is even and* $y \equiv 3 \pmod 8$, *then* n *is even.*

Proof. By Prop. 2, m is even. From (1) we have $1 \equiv 9^n \pmod{16}$ Hence n is even.

Theorem 1. *Let a be odd,* $y = p$ *odd prime, and* $p \equiv 3 \pmod 4$ *in* (1). *If* $m \neq 1$, *then* $(l, m, n) = (2,2,2)$.

Proof. By Prop.1, n is even. Put $l = 2l'$, $n = 2n'$, and $(4a^2 + p^2)^{n'} + (4a^2 - p^2)^{l'} = A$, $(4a^2 + p^2)^{n'} - (4a^2 - p^2)^{l'} = B$. Clearly $(A, B) = 2$. From (1) we have

(2) $$2^{2m}a^m p^m = AB.$$

Assume $A \equiv 0 \pmod p$, then we have $(2a)^{2n'} + (2a)^{2l'} \equiv 0 \pmod p$, so