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 $l, m, n \in \boldsymbol{N}$

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

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

$$2^{2m}a^m p^m = AB. \tag{2}$$

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

$(2a)^{2|n'-l'|} \equiv -1 \pmod{p}$. Then $(2a)^{|n'-l'|}$ has order $4 \bmod p$. This contradicts the assumption $p \equiv 3 \pmod 4$. Therefore $B \equiv 0 \pmod{p}$.

Now there are two possibilities on choice of A, B in (2):

$$A = 2b^m, \qquad B = 2^{2m-1}c^m p^m \tag{2.1}$$

$$A = 2^{2m-1}b^m, \quad B = 2c^m p^m, \tag{2.2}$$

where $a = bc$, $(b, c) = 1$.

Case (2.1). $B \equiv 1 - (-1)^{l'} \equiv 0 \pmod 4$, hence l' is even. $B \equiv -(-2p^2)^{l'} \equiv 2^{2m-1}c^m p^m \pmod{4a^2 + p^2}$. By the assumptions on a, p,

$$\left(\frac{-(-2p^2)^{l'}}{4a^2 + p^2}\right) = 1 = \left(\frac{2^{2m-1}c^m p^m}{4a^2 + p^2}\right) = -1,$$

which is a contradiction. Thus (2.1) does not occur.

Case (2.2). $A \equiv 1 + (-1)^{l'} \equiv 0 \pmod 4$, hence l' is odd. $A \equiv 5^{n'} + 3^{l'} \equiv 0 \pmod 8$. As l' is odd, n' is odd. $A \equiv (2p^2)^{n'} \equiv 2c^m p^m \pmod{4a^2 - p^2}$. By the assumptions on a, p.

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

Therefore m is even. Assume $m \geq 4$. $(A + B)/2 = (4a^2 + p^2)^{n'} = 2^{2m-2}b^m + c^m p^m$. Then $5^{n'} \equiv 1 \pmod 8$ as c, p are odd. Since n' is odd, $4 \equiv 0 \pmod 8$, which is a contradiction, hence $m = 2$. Then $A = (4a^2 + p^2)^{n'} + (4a^2 - p^2)^{l'} = 8b^2 \leq 8a^2 = (4a^2 + p^2) + (4a^2 - p^2)$. Therefore $n' = l' = 1$. Thus $(l, m, n) = (2,2,2)$.

Theorem 2. *Let a be even, $y = p$ odd prime, and $p \equiv 3 \pmod 8$ in (1). If $2a + p$ is prime and $2a - p$ is prime or 1, then $(l, m, n) = (2,2,2)$.*

Proof. By Props. 2, 3, both m and n are even. Now let l', n', A and B be as the proof of Theorem 1, then $(A, B) = 2$ and $B \equiv 0 \pmod{p}$. Let $a = 2^s a_0$ $(s \geq 1)$, $(2, a_0) = 1$, then there are two possibilities on choice of A, B in (2):

$$A = 2b^m, \qquad B = 2^{m(2+s)-1}c^m p^m, \tag{2.3}$$

$$A = 2^{m(2+s)-1}b^m, \quad B = 2c^m p^m, \tag{2.4}$$

where $a_0 = bc$, $(b, c) = 1$.

Case (2.3). $B \equiv 1 - (-1)^{l'} \equiv 0 \pmod 4$, hence l' is even, then $(4a^2 - p^2)^{l'} \equiv 1 \pmod{16}$. Therefore $B \equiv 9^{n'} - 1 \equiv 0 \pmod{16}$, hence n' is even. Let $l' = 2l''$, $n' = 2n''$, $m = 2m'$.

$$(A + B)/2 = ((4a^2 + p^2)^{n''})^2 = (b^{m'})^2 + (2^{m'(2+s)-1}c^{m'}p^{m'})^2.$$

Then we have $b^{m'} = x^2 - y^2$, $2^{m'(2+s)-1}c^{m'}p^{m'} = 2xy$, $(4a^2 + p^2)^{n''} = x^2 + y^2$, where $x, y \in \boldsymbol{N}$, with $(x, y) = 1$, $x > y$, $x \not\equiv y \pmod 2$.

$$(A - B)/2 = ((4a^2 - p^2)^{l''})^2 = (b^{m'})^2 - (2^{m'(2+s)-1}c^{m'}p^{m'})^2.$$

Then we have $b^{m'} = z^2 + w^2$, $2^{m'(2+s)-1}c^{m'}p^{m'} = 2zw$, $(4a^2 - p^2)^{l''} = z^2 - w^2$, where $z, w \in \boldsymbol{N}$, with $(z, w) = 1$, $z > w$, $z \not\equiv w \pmod 2$. Accordingly,

$$x^2 - y^2 = z^2 + w^2 \tag{3}$$
$$xy = zw.$$

But positive integers x, y, z, w satisfying (3) do not exist by the Lemma which we prove later. Thus (2.3) does not occur.

Case (2.4). $A \equiv 1 + (-1)^{l'} \equiv 0 \pmod 4$, hence l' is odd. $(A-B)/2 = (4a^2 - p^2)^{l'} = (2^{m'(2+s)-1}b^{m'})^2 - (c^{m'}p^{m'})^2$. So

$(4)(2a+p)^{l'}(2a-p)^{l'} = (2^{m'(2+s)-1}b^{m'} + c^{m'}p^{m'})(2^{m'(2+s)-1}b^{m'} - c^{m'}p^{m'})$.

Since $2a+p$ is prime, $2a-p$ is prime or 1, and $(2a+p, 2a-p) = (2^{m'(2+s)-1}b^{m'} + c^{m'}p^{m'}, 2^{m'(2+s)-1}b^{m'} - c^{m'}p^{m'}) = 1$, we have either of two cases:

$$(4.1) \qquad 2^{m'(2+s)-1}b^{m'} + c^{m'}p^{m'} = (4a^2 - p^2)^{l'}, \quad 2^{m'(2+s)-1}b^{m'} - c^{m'}p^{m'} = 1,$$

$$(4.2) \qquad 2^{m'(2+s)-1}b^{m'} + c^{m'}p^{m'} = (2a+p)^{l'}, \quad 2^{m'(2+s)-1}b^{m'} - c^{m'}p^{m'} = (2a-p)^{l'}.$$

Case (4.1). $2c^{m'}p^{m'} = (4a^2-p^2)^{l'} - 1 \equiv 7^{l'} - 1 \equiv 6 \pmod{16}$, as l' is odd. Hence $c^{m'}p^{m'} \equiv 3 \pmod 8$. Then $1 = 2^{m'(2+s)-1}b^{m'} - c^{m'}p^{m'} \equiv 2^{m'(2+s)-1}b^{m'} - 3 \pmod 8$, that is, $2^{m'(2+S)-1}b^{m'} \equiv 4 \pmod 8$. As b is odd and $m'(2+s) - 1 \geq 2$, $m'(2+S) - 1 = 2$, i.e. $m' = 1$, $s = 1$. Then (4.1) becomes

$$4b + cp = (2a+p)^{l'}(2a-p)^{l'}, \quad 4b - cp = 1.$$

Then $8b - 1 = (2a+p)^{l'}(2a-p)^{l'}$. This is possible only when $2a - p = 1$. Thus (4.1) occurs only in the case $2a - p = 1$ which is a subcase of (4.2).

Case (4.2). $(2a+p)^{l'} - (2a-p)^{l'} = 2c^{m'}p^{m'}$, and l' is odd, then $2p^{l'} \equiv 0 \pmod c$. As $(p, c) = (2, c) = 1$, $c = 1$. Accordingly $b = a_0$, and (4.2) becomes

$$2^{m'(2+s)-1}a_0^{m'} + p^{m'} = (2a+p)^{l'}, \quad 2^{m'(2+s)-1}a_0^{m'} - p^{m'} = (2a-p)^{l'}.$$

Then $2^{m'(2+s)}a_0^{m'} = (2a+p)^{l'} + (2a-p)^{l'}$. Since l' is odd, $(2a+p)^{l'} + (2a-p)^{l'} = 4ad = 2^{2+s}a_0 d$, where $d = (2a+p)^{l'-1} - (2a+p)^{l'-2}(2a-p) + \cdots + (2a-p)^{l'-1}$ is odd. Hence $m' = 1$. By (4.2) $2a + p = (2a+p)^{l'}$, hence $l' = 1$, then $n' = 1$. Thus $(l, m, n) = (2,2,2)$.

Lemma. *Let* $x, y, z, w \in \boldsymbol{N}$, $(x, y) = (z, w) = 1$, $x > y$, $z > w$, $x \not\equiv y \pmod 2$, $z \not\equiv w \pmod 2$. *Then one of the following equations is not satisfied.*

$$(3) \qquad x^2 - y^2 = z^2 + w^2, \quad xy = zw.$$

Proof. Suppose that x, y, z, w satisfy (3). As $z \not\equiv w \pmod 2$, $z^2 + w^2 \equiv 1 \pmod 4$, that is, $x^2 - y^2 \equiv 1 \pmod 4$, hence x is odd and y is even. Let $(x, z) = a$. Put $x = ab$, $z = ac$, so $(b, c) = 1$. By $xy = zw$, we can put $y = cd$, $w = bd$. As y is even, we can assume that c is even. (The proof is essentially the same for d being even.) By $x^2 - y^2 = z^2 + w^2$, $a^2(b^2 - c^2) = d^2(b^2 + c^2)$. $(x, y) = 1$ and $(b, c) = 1$ mean $(a, d) = 1$ and $(b^2 - c^2, b^2 + c^2) = 1$. Hence $b^2 + c^2 = a^2$, $d^2 + c^2 = b^2$. As c is even, we have

$$b = x'^2 - y'^2, \quad c = 2x'y', \quad a = x'^2 + y'^2$$
$$d = z'^2 - w'^2, \quad c = 2z'w', \quad b = z'^2 + w'^2,$$

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

$$x'^2 - y'^2 = z'^2 + w'^2$$
$$x'y' = z'w'.$$

Hence x', y', z', w' satisfy (3). And $x \geq a > x'$, $y \geq c > y'$, $z \geq c \geq z'$, $w \geq b > w'$. This means that $x, y, z, w \in \boldsymbol{N}$ satisfying (3) become infinitely small, which is a contradiction.

Theorem 3. *Let a be odd, $y = p$ odd prime, and $p \equiv 3 \pmod 4$ in* (1). *If a prime divisor q of a satisfies $q \equiv 1 \pmod 4$ and*

$$\left(\frac{p}{q}\right) = -1,$$

then $(l, m, n) = (2,2,2)$.

Proof. Let r be a primitive root modulo q. Then r has order $q-1$ mod q. Let $p \equiv r^t \pmod q$. Since

$$-1 = \left(\frac{p}{q}\right) = \left(\frac{r}{q}\right)^t,$$

t is odd. Then order of $p \bmod q =$ order of $r^t \bmod q = (q-1)/(t, q-1) \equiv 0 \pmod 4$. From (1) $(-p^2)^l \equiv p^{2n} \pmod q$, so $p^{2|l-n|} \equiv 1 \pmod q$. Hence order of $p \bmod q$ divides $2(l-n)$. So 2 divides $l-n$. Since l is even, n is even. By Prop.1, $m \neq 1$. Thus $(l, m, n) = (2,2,2)$ from Theorem 1.

Remark. Thus we could prove that the conjecture of Jeśmanowicz holds in special cases as shown in Theorems 1-3. We could prove also that this conjecture holds in case $y = 3$, a is odd and (i) $a \equiv 0,2,3,4 \pmod 7$, $a \equiv 4,5 \pmod 9$, $a \equiv 4 \pmod{11}$, $a \equiv 0,10 \pmod{13}$, or $a \equiv 6,7,11 \pmod{17}$, or (ii) a prime divisor q of a satisfies $q \equiv 1 \pmod 3$, and the order of 3 mod q is divisible by 3. (For all primes $q \equiv 1 \pmod 3$, $7 \leq q \leq 199$ except 61,67,103,151,193, the order of 3 mod q is divisible by 3.) But we omit here the detailed proof which runs in a similar way as in our proof of Theorems 1, 3 respectively.

References

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

[2] N. Terai: The diophantine equation $x^2 + q^m = p^n$. Acat Arith., **LXIII.4**, 351–358 (1993).