79. On a Conjecture on Pythagorean Numbers. III

By Kei TAKAKUWA

Department of Mathematics, Gakushuin University

(Communicated by Shokichi IYANAGA, M. J. A., Nov. 12, 1993)

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 $(a, y) = 1$, $2a > y$, $y \equiv 1 \pmod 4$, whence l is even, which is easily seen considering (1) mod. 4.

Proposition 1. *If a is odd, then 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,

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

where $\left(\frac{*}{*}\right)$ is the Jacobi symbol. Hence n is even.

Proposition 2. *If a is odd, then $m \neq 1$.*

Proof. Since $(4a^2 - y^2)^l \equiv 1 \pmod 8$ and $(4a^2 + y^2)^n \equiv 1 \pmod 8$, we have $(4ay)^m \equiv 0 \pmod 8$ from (1). Hence $m \neq 1$.

Proposition 3. *Let $a \equiv 2 \pmod 4$. Then*

1) *If $y \equiv 1 \pmod 8$, $m \neq 1$.*

2) *If $y \equiv 5 \pmod 8$, $m \neq 1 \Leftrightarrow n$ is even.*

Proof. 1) From (1) we have $(4ay)^m \equiv 0 \pmod{16}$. Since 4 does not divide a, we have $m \neq 1$.

2) Since $y^2 \equiv 9 \pmod{16}$, we have $(4ay)^m \equiv 9^n - 1 \pmod{16}$. Then $m \neq 1 \Leftrightarrow (4ay)^m \equiv 0 \pmod{16} \Leftrightarrow 9^n \equiv 1 \pmod{16} \Leftrightarrow n$ is even.

Proposition 4. *If $a \equiv 0 \pmod 4$ and $y \equiv 5 \pmod 8$, then n and m are even.*

Proof. From (1) we have $(2y^2)^m \equiv (2y^2)^n \pmod{2a - y}$. By $2a - y \equiv -5 \pmod 8$,

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

so $(-1)^m = (-1)^n$. Hence $n \equiv m \pmod 2$.

From (1) we have $1 \equiv 9^n \pmod{16}$, so n is even. Hence m is also even.

Theorem 1. *Let a be odd, $y = p$ odd prime, and $p \equiv 5 \pmod 8$ in (1). If m is even, 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

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

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

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

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

(2.3) $A = 2^{2m-1}b^m p^m, \quad B = 2c^m,$

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

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

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

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

which is a contradiction. Thus (2.1) does not occur. In the same way (2.2) does not occur either. (Note $\left(\frac{p}{4a^2+p^2}\right) = 1$.)

Case (2.3). $A \equiv 1 + (-1)^{l'} \equiv 0 \pmod 4$, hence l' is odd. $A \equiv 5^{n'} + 3^{l'} \equiv 0 \pmod 8$. As l' is odd, n' is odd. $A = (4a^2+p^2)^{n'} + (4a^2-p^2)^{l'} \equiv 0 \pmod p$, so $(2a)^{|l-n|} \equiv -1 \pmod p$. From $n' \equiv l' \pmod 2$ we can write $|l-n| = 4t$ with $t \in \boldsymbol{N}$, so $(2a)^t$ has order 8 (mod. p). Hence 8 divides $p-1$ i.e. $p \equiv 1 \pmod 8$, which is a contradiction. Thus (2.3) does not cccur.

Case (2.4). In the same way as in (2.3), l' and n' are odd.

Assume $m > 3$. $A \equiv 13^{n'} - 5^{l'} \equiv 0 \pmod{16}$. By $13^1 \equiv 13 \pmod{16}$, $13^3 \equiv 5 \pmod{16}$, $5^1 \equiv 5 \pmod{16}$, $5^3 \equiv 13 \pmod{16}$, we have $n' \equiv l' + 2 \pmod 4$. And n', l' are odd. Thus

(I) $l' \equiv 1 \pmod 4, \quad n' \equiv 3 \pmod 4,$

(II) $l' \equiv 3 \pmod 4, \quad n' \equiv 1 \pmod 4.$

(I): $B = 2c^m p^m \equiv (4a^2+p^2)^3 - (4a^2-p^2) \equiv 13^3 + 5 \equiv 5 + 5 = 10 \pmod{16}$. (Note that $(4a^2 \pm p^2)^4 \equiv (4 \pm 9)^4 \equiv 1 \pmod{16}$.) So $c^m p^m \equiv 5 \pmod 8$.

(II): In the same way as in (I), we have $c^m p^m \equiv 5 \pmod 8$.

Hence m is odd, which is a contradiction. Thus $m = 2$. Then $A = (4a^2+p^2)^{n'} + (4a^2-p^2)^{l'} = 2^3 b^2 \leq 8a^2 = (4a^2+p^2) + (4a^2-p^2)$, so $l' = n' = 1$. Therefore $(l, m, n) = (2,2,2)$.

Theorem 2. *Let a be odd, $y = p$ odd prime, and $p \equiv 1 \pmod 8$ in (1). In the following cases, $(l, m, n) = (2,2,2)$.*

(i) *m is even.*

(ii) *It does not occur that $a = a_1 a_2$, $(a_1, a_2) = 1$ and $a_1 \equiv 5 \pmod 8$.*

Proof. From Propositions 1,2 n is even and $m \neq 1$. Now let l', n', A, B, b and c be as above, then $(A, B) = 2$. Then there are four possibilities on choice of A, B in (2):

(2.5) $A = 2b^m p^m, \quad B = 2^{2m-1}c^m,$

(2.6) $A = 2b^m, \quad B = 2^{2m-1}c^m p^m,$

(2.7) $A = 2^{2m-1}b^m, \quad B = 2c^m p^m,$

(2.8) $A = 2^{2m-1}b^m p^m, \quad B = 2c^m.$

Case (2.5). $B \equiv 1 - (-1)^{l'} \equiv 0 \pmod 4$, hence l' is even. $B \equiv -(2p^2)^{l'} \equiv 2^{2m-1}c^m \pmod{4a^2+p^2}$. By the assumptions on a, p,

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

which is a contradiction. Thus (2.5) does not occur. In the same way (2.6) does not occur either. (Note $\left(\frac{p}{4a^2+p^2}\right) = 1$.)

Case (2.7). $A \equiv 1 + (-1)^{l'} \equiv 0 \pmod 4$, hence l' is odd. $A \equiv 5^{n'} + 3 \equiv 0 \pmod 8$, hence n' is odd.

Assume $m \geq 3$. Then $A \equiv 5^{n'} + 3^{l'} \equiv 0 \pmod{16}$. By $3^1 \equiv 3 \pmod{16}$, $3^3 \equiv -5 \pmod{16}$, $5^1 \equiv 5 \pmod{16}$, $5^3 \equiv -3 \pmod{16}$, we have $n' \equiv l' + 2 \pmod 4$. And n', l' are odd. Thus

(I) $\quad l' \equiv 1 \pmod 4, \quad n' \equiv 3 \pmod 4,$

(II) $\quad l' \equiv 3 \pmod 4, \quad n' \equiv 1 \pmod 4.$

(I): $B = 2c^m p^m \equiv (4a^2+p^2)^3 - (4a^2-p^2) \equiv 5^3 - 3 \equiv 10 \pmod{16}$. (Note that $(4a^2 \pm p^2)^4 \equiv (4 \pm 1)^4 \equiv 1 \pmod{16}$.) So $c^m \equiv 5 \pmod 8$.

(II): In the same way as in (I), we have $c^m \equiv 5 \pmod 8$.

Hence m is odd and $c \equiv 5 \pmod 8$, which is a contradiction. Therefore $m = 2$. Then $A = (4a^2+p^2)^{n'} + (4a^2-p^2)^{l'} = 2^3b^2 \leq 8a^2 = (4a^2+p^2) + (4a^2-p^2)$, so $l' = n' = 1$. Thus $(l, m, n) = (2,2,2)$.

Case (2.8). In the same way as in (2.7), we have $m = 2$. Then $(A+B)/2 = (4a^2+p^2)^{n'} = 4b^2p^2 + c^2 \leq 4a^2p^2 + a^2$.

Now $(4a^2+p^2)^3 = 64a^6 + 12a^2p^4 + 48a^4p^2 + p^6 > 4a^2p^2 + a^2 \geq (4a^2+p^2)^{n'}$, so $n' < 3$. Hence $n' = 1$. Then $4a^2 + p^2 = 4b^2c^2 + p^2 = 4b^2p^2 + c^2$, so $4b^2(c^2-p^2) = c^2 - p^2$. Therefore $4b^2 = 1$, which is a contradiction. Thus (2.8) does not occur.

Corollary 1. *Let a be odd and $y = p$ odd prime in* (1). *If $a \not\equiv 0 \pmod 3$ and $a \not\equiv p \pmod 3$, then $(l, m, n) = (2,2,2)$.*

Proof. $p \neq 3$ by $p \equiv 1 \pmod 4$. And $a^2 \equiv p^2 \equiv 1 \pmod 3$ from $a \not\equiv 0 \pmod 3$. Moreover $ap \equiv -1 \pmod 3$ from $a \not\equiv p \pmod 3$. Then from (1) we have $(-1)^m \equiv (-1)^n \pmod 3$, so $n \equiv m \pmod 2$. Since n is even from Proposition 1, m is even. Then from Theorems 1,2, we have $(l, m, n) = (2,2,2)$.

Corollary 2. *Let $y = p$ be odd prime, and $p \equiv 5 \pmod 8$ in* (1). *If $a \equiv 1 \pmod 4$, then $(l, m, n) = (2,2,2)$.*

Proof. From (1) we have $(2p^2)^m \equiv (2p^2)^n \pmod{2a-p}$. By $2a - p \equiv 5 \pmod 8$ we have

$$\left(\frac{2}{2a-p}\right) = -1,$$

so $(-1)^m = (-1)^n$ Since n is even from Proposition 1, m is even. Then from Theorem 1 we have $(l, m, n) = (2,2,2)$.

Corollary 3. *Let $y = p$ be odd prime, and $p \equiv 1 \pmod 8$ in* (1). *If $a \equiv 3 \pmod 4$, then $(l, m, n) = (2,2,2)$.*

Proof. In the same way as Corollary 2.

Theorem 3. *Let a be even, $a = 2^s a_0$ $(s \geq 1)$ with $(2, a_0) = 1$, $y = p$ odd prime, and $p \equiv 5 \pmod 8$ in* (1). *Suppose that $2a + p$, $2a - p$ are*

primes. Moreover, when $a \equiv 2 \pmod 4$, *assume the following* (i) *or* (ii).

(i) m *is even.*

(ii) $m \neq 1$. *And it does not occur that* $a_0 = a_1a_2$, $(a_1, a_2) = 1$, $a_1 \equiv 1 \pmod 4$ *and* $a_1 \neq 1$.

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

Proof. By Propositions 3, 4, n is even. Now let l', n', A and B be as in the proof of Theorem 1, then $(A, B) = 2$. Then there are four possibilities on choice of A, B in (2):

(2.9) $A = 2b^m$, $B = 2^{m(2+s)-1}c^m p^m$,

(2.10) $A = 2^{m(2+s)-1}b^m$, $B = 2c^m p^m$,

(2.11) $A = 2^{m(2+s)-1}b^m p^m$, $B = 2c^m$,

(2.12) $A = 2b^m p^m$, $B = 2^{m(2+s)-1}c^m$,

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

Case (2.9). $B \equiv 1 - (-1)^{l'} \equiv 0 \pmod 4$, hence l' is even. Then $B \equiv 9^{n'} - 1 \equiv 0 \pmod{16}$, so n' is even.

If $a \equiv 0 \pmod 4$, m is even. (Proposition 4.) Now let $a \equiv 2 \pmod 4$. Then $A \equiv 2 \equiv 2b^m \pmod{16}$, i.e. $b^m \equiv 1 \pmod 8$. If m is odd, then $b \equiv 1 \pmod 8$. And $b \neq 1$ in this case. This is a contradiction. Hence m is even.

Let $l' = 2l''$, $n' = 2n''$ and $m = 2m'$. Then

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

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 $(x, y) = 1$, $x > y$, $x \not\equiv y \pmod 2$. Also

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

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,

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

But positive integers x, y, z, w satisfying (3) do not exist by the lemma which we have proved in [1]. Thus (2.9) does not occur.

Case (2.10). $A \equiv 1 + (-1)^{l'} \equiv 0 \pmod 4$, hence l' is odd. Then $A \equiv 9^{n'} - 9 \equiv 0 \pmod{16}$, so n' is odd.

If $a \equiv 0 \pmod 4$, m is even. (Proposition 4.) Now let $a \equiv 2 \pmod 4$. Then $B \equiv 2 \equiv 2c^m p^m \pmod{16}$, i.e. $c^m p^m \equiv 1 \pmod 8$. If m is odd, then $c \equiv 5 \pmod 8$, which is a contradiction. Hence m is even. Put $m = 2m'$. $(A - B)/2 = (4a^2 - p^2)^{l'} = (2^{m'(2+s)-1}b^{m'})^2 - (c^{m'}p^{m'})^2$. 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 $2a + p$ and $2a - p$ are primes, 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) $$\begin{cases} 2^{m'(2+s)-1}b^{m'} + c^{m'}p^{m'} = (4a^2 - p^2)^{l'} \\ 2^{m'(2+s)-1}b^{m'} - c^{m'}p^{m'} = 1 \end{cases}$$

(4.2) $$\begin{cases} 2^{m'(2+s)-1}b^{m'} + c^{m'}p^{m'} = (2a + p)^{l'} \\ 2^{m'(2+s)-1}b^{m'} - c^{m'}p^{m'} = (2a - p)^{l'}. \end{cases}$$

Case (4.1). $2c^{m'}p^{m'} = (4a^2 - p^2)^{l'} - 1 \equiv -1 \pmod{4a^2 - p^2}$. By the assumptions on a, p,

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

which is a contradiction. Thus (4.1) does not occur.

Case (4.2). $(2a+p)^{l'} + (2a-p)^{l'} = 2^{m'(2+s)}b^{m'}$. Since l' is odd, we have

$$(2a+p)^{l'} + (2a-p)^{l'} = ((2a+p)+(2a-p))((2a+p)^{l'-1} - \cdots + (2a-p)^{l'-1})$$
$$= 4ax_1 = 2^{2+s}x_2,$$

where x_1, x_2 are odd. So $2^{2+s}x_2 = 2^{m'(2+s)}b^{m'}$. Thus $2+s = m'(2+s)$, so $m' = 1$. Hence $m = 2$. Then $A = (4a^2+p^2)^{n'} + (4a^2-p^2)^{l'} = 2^{3+2s}b^2 \leq 8a^2 = (4a^2+p^2) + (4a^2-p^2)$, so $l' = n' = 1$. Thus $(l, m, n) = (2,2,2)$.

Case (2.11). In the same way as in (2.10), both l' and n' are odd. So $l' \equiv n' (\text{mod. } 2)$, i.e. 4 divides $|l-n|$. Put $|l-n| = 4t$, with $t \in \boldsymbol{N}$. $A \equiv (2a)^n + (2a)^l \equiv 0 (\text{mod. } p)$, so $(2a)^{|l-n|} \equiv -1 (\text{mod. } p)$. Then $((2a)^t)^4 \equiv -1 (\text{mod. } p)$. Hence $(2a)^t$ has order 8 (mod. p). So 8 divides $p-1$, i.e. $p \equiv 1 (\text{mod. } 8)$, which is a contradiction. Thus (2.11) does not occur.

Case (2.12). In the same way as in (2.9), both l' and n' are even. So $l' \equiv n' (\text{mod. } 2)$. Hence in the same way as in (2.11), it is proved that (2.12) does not occur.

Remark. Lù Wén-duān [2] proved the conjecture of Jeśmanowicz in case $y = 1$.

References

[1] K. Takakuwa and Y. Asaeda: On a conjecture on Pythagorean numbers. Proc. Japan Acad., **69**A, 252–255 (1993).

[2] Lù Wén-duān: Lun shāng gāo shu. J. Sichuan Univ., **2**, 39–41 (1959).