ACTA ARITHMETICA
C.1 (2001)

On Terai's conjecture concerning Pythagorean numbers

by

Maohua Le (Zhanjiang)

1. Introduction. Let $\mathbb{Z}, \mathbb{N}, \mathbb{Q}$ be the sets of integers, positive integers and rational numbers respectively. Let (a, b, c) be a primitive Pythagorean triple such that

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

Then we have

$$a = 2uv, \quad b = u^2 - v^2, \quad c = u^2 + v^2, \tag{2}$$

where u, v are positive integers satisfying

$$u > v, \quad \gcd(u, v) = 1, \quad 2 \mid uv. \tag{3}$$

In [7], Terai conjectured that the equation

$$x^2 + b^y = c^z, \quad x, y, z \in \mathbb{N}, \tag{4}$$

has only the solution $(x, y, z) = (a, 2, 2)$. This conjecture was proved for some special cases. But, in general, the problem is far from solved. In this respect, the author [3] proved that if $b > 8 \cdot 10^6$, $b \equiv \pm 5 \pmod 8$ and c is a prime power, then (4) has only the solution $(x, y, z) = (a, 2, 2)$. Afterwards, Cao and Dong [1], Yuan [8] showed that the condition $b > 8 \cdot 10^6$ can be eliminated from the result of [3]. In addition, Cao and Dong [1], Yuan and Wang [9] proved that if $b \equiv \pm 5 \pmod 8$ and either b or c is a prime, then (4) has only the solution $(x, y, z) = (a, 2, 2)$. In this paper we consider the case of $b \not\equiv \pm 5 \pmod 8$. We prove the following result.

Theorem. *If* $b \equiv 7 \pmod 8$ *and either* b *is a prime or* c *is a prime power*, *then* (4) *has only the solution* $(x, y, z) = (a, 2, 2)$.

2000 *Mathematics Subject Classification*: Primary 11D61.
Supported by the National Natural Science Foundation of China, the Guangdong Provincial Natural Science Foundation and the Natural Science Foundation of the Education Department of Guangdong Province.

2. Preliminaries

Lemma 1 ([5, pp. 12–13]). *Every solution* (X,Y,Z) *of the equation*

$$X^2+Y^2=Z^2,\qquad X,Y,Z\in\mathbb{N},\quad \gcd(X,Y)=1,\quad 2\,|\,X,$$

can be expressed as

$$X=2rs,\qquad Y=r^2-s^2,\qquad Z=r^2+s^2,$$

where r,s *are positive integers satisfying*

$$r>s,\qquad \gcd(r,s)=1,\qquad 2\,|\,rs. \tag{5}$$

Lemma 2 ([5, pp. 122–123]). *Let* n *be an odd integer with* $n\ge 1$. *Every solution* (X,Y,Z) *of the equation*

$$X^2+Y^2=Z^n,\qquad X,Y,Z\in\mathbb{Z},\quad \gcd(X,Y)=1,$$

can be expressed as

$$Z=r^2+s^2,\quad X+Y\sqrt{-1}=\lambda_1(r+\lambda_2 s\sqrt{-1})^n,\quad \lambda_1,\lambda_2\in\{1,-1\},$$

where r,s *are positive integers satisfying* (5).

Lemma 3 ([5, Theorem 4.2]). *The equation*

$$X^2+Y^4=Z^4,\qquad X,Y,Z\in\mathbb{N},\quad \gcd(X,Y)=1,$$

has no solution (X,Y,Z).

Lemma 4 ([4] and [6]). *The equation*

$$1+X^2=2Y^n,\qquad X,Y,n\in\mathbb{N},\ X>1,\ Y>1,\ n>2,$$

has only the solution $(X,Y,n)=(239,13,4)$.

Lemma 5 ([2, Lemma 1]). *Let* D *be a positive integer, and let* p *be an odd prime with* $p\nmid D$. *If the equation*

$$X^2+DY^2=p^Z,\qquad X,Y,Z\in\mathbb{Z},\quad \gcd(X,Y)=1,\quad Z>0, \tag{6}$$

has a solution (X,Y,Z), *then it has a unique solution* (X_1,Y_1,Z_1) *such that* $X_1>0$, $Y_1>0$ *and* $Z_1\le Z$, *where* Z *runs through all solutions* (X,Y,Z) *of* (6). (X_1,Y_1,Z_1) *is called the least solution of* (6). *Moreover, every solution* (X,Y,Z) *of* (6) *can be expressed as*

$$Z=Z_1t,\quad X+Y\sqrt{-D}=\lambda_1(X_1+\lambda_2Y_1\sqrt{-D})^t,\quad t\in\mathbb{N},\ \lambda_1,\lambda_2\in\{-1,1\}.$$

3. Proof of Theorem. Let (x,y,z) be a solution of (4) with $(x,y,z)\ne(a,2,2)$. Since $b\equiv 7 \pmod 8$, we see from (2), (3) and (4) that $c\equiv 1 \pmod 8$ and $2\,|\,y$.

We first consider the case that $2\,|\,y$ and $2\,|\,z$. By Lemma 1, from (4) we then get

$$x=2rs,\qquad b^{y/2}=r^2-s^2,\qquad c^{z/2}=r^2+s^2, \tag{7}$$

where r, s are positive integers satisfying (5). Since $(x, y, z) \neq (a, 2, 2)$, if $y = 2$, then $z > 2$ and $z/2 \geq 2$. By (4) and (7), we get

$$r^2 + s^2 = c^{z/2} \geq c^2 > b^2 = (r^2 - s^2)^2 \geq (r+s)^2 > r^2 + s^2, \tag{8}$$

a contradiction. Similarly, if $z = 2$, then $y > 2$ and $y/2 \geq 2$. Hence, we deduce from (2) and (4) that

$$\begin{aligned} u^2 + v^2 = c = c^{z/2} = \sqrt{x^2 + b^y} &> b^{y/2} \\ &\geq b^2 = (u^2 - v^2)^2 \geq (u+v)^2 > u^2 + v^2, \end{aligned} \tag{9}$$

a contradiction. So we have $y > 2$ and $z > 2$.

If b is a prime, then from (7) we get $r = s + 1$, $b^{y/2} = 2s + 1$ and $c^{z/2} = 2s^2 + 2s + 1$. This implies that

$$1 + b^y = 2c^{z/2}. \tag{10}$$

Since $2 \mid y$, by Lemma 4, we find from (10) that either $z/2 = 2$ or $(b, c, y, z) = (239, 13, 2, 8)$. When $z/2 = 2$, by Lemma 3, we see from (2), (4) and (10) that $y \geq 6$ and

$$\begin{aligned} 2u^4 + 4u^2v^2 + 2v^4 &= 2(u^2 + v^2)^2 = 2c^2 = 2c^{z/2} \\ &> b^y \geq b^6 = (u^2 - v^2)^6 \\ &\geq (u+v)^6 > 4u^4 + 6u^2v^2 + 4v^4, \end{aligned} \tag{11}$$

a contradiction. When $(b, c) = (239, 13)$, b and c do not satisfy (1). Thus, the Theorem holds for this case.

If c is a prime power, then

$$c = p^k, \tag{12}$$

where p is an odd prime and k is a positive integer. We see from (1), (4) and (12) that the equation

$$X^2 + b^2Y^2 = p^Z, \qquad X, Y, Z \in \mathbb{Z}, \quad \gcd(X, Y) = 1, \quad Z > 0, \tag{13}$$

has two solutions $(X, Y, Z) = (a, 1, 2k)$ and $(x, b^{(y-2)/2}, zk)$. Let (X_1, Y_1, Z_1) be the least solution of (13). By Lemma 5, if $(X_1, Y_1, Z_1) \neq (a, 1, 2k)$, then we have

$$2k = Z_1 t, \qquad t \in \mathbb{N},\ t > 1, \tag{14}$$

$$a + \sqrt{-b^2} = \lambda_1 (X_1 + \lambda_2 Y_1 \sqrt{-b^2})^t, \qquad \lambda_1, \lambda_2 \in \{-1, 1\}. \tag{15}$$

By (15), we get $2 \nmid t$. So we have $t \geq 3$. Since $X_1^2 + b^2Y_1^2 = p^{Z_1}$, we infer from (2) and (12) that

$$\begin{aligned} u^2 + v^2 = c = p^{Z_1 t/2} \geq p^{3Z_1/2} = (X_1^2 + b^2Y_1^2)^{3/2} > b^3 = (u^2 - v^2)^3 \\ \geq (u+v)^3 > u^3 + v^3, \end{aligned} \tag{16}$$

a contradiction. This implies that $(X_1, Y_1, Z_1) = (a, 1, 2k)$. Using Lemma 5 again, we get

$$zk = 2kt, \qquad t \in \mathbb{N},\ t > 1, \tag{17}$$

$$x + b^{(y-2)/2}\sqrt{-b^2} = \lambda_1(a + \lambda_2\sqrt{-b^2})^t, \qquad \lambda_1, \lambda_2 \in \{-1, 1\}. \tag{18}$$

Since $2 \nmid b$, we find from (18) that $2 \nmid t$ and

$$b^{(y-2)/2} = \lambda_1\lambda_2 \sum_{i=0}^{(t-1)/2} \binom{t}{2i+1} a^{t-2i-1}(-b^2)^i. \tag{19}$$

Since $\gcd(a, b) = 1$ and $y > 2$, we see from (19) that $b \mid t$. Further, using the same method as in the proof of [3, Theorem], we can deduce from (19) that $b^{(y-2)/2} \mid t$. So we have $t \ge b^{(y-2)/2}$. Therefore, by (7), (12) and (17), we obtain

$$\begin{aligned} b^y &= (r^2 - s^2)^2 \ge (r + s)^2 > r^2 + s^2 = c^{z/2} \\ &= p^{zk/2} = p^{kt} = c^t > b^t \ge b^{b^{(y-2)/2}}, \end{aligned} \tag{20}$$

whence we get

$$y > b^{(y-2)/2}. \tag{21}$$

However, since $y \ge 4$ and $b \ge 7$, (21) is impossible. Thus, under the hypothesis, (4) has only the solution $(z, y, z) = (a, 2, 2)$ satisfying $2 \mid y$ and $2 \mid z$.

We next consider the case that $2 \mid y$ and $2 \nmid z$. If b is a prime, then from (2) we get

$$u = v + 1, \qquad b = 2v + 1, \qquad c = 2v^2 + 2v + 1, \qquad v \equiv 3 \pmod 4. \tag{22}$$

On the other hand, by Lemma 2, we see from (4) that

$$c = r^2 + s^2, \tag{23}$$

$$x + b^{y/2}\sqrt{-1} = \lambda_1(r + \lambda_2 s\sqrt{-1})^z, \qquad \lambda_1, \lambda_2 \in \{-1, 1\}, \tag{24}$$

where r, s are positive integers satisfying (5). From (24), we get

$$b^{y/2} = \lambda_1\lambda_2 s \sum_{i=0}^{(z-1)/2} \binom{z}{2i+1} r^{z-2i-1}(-s^2)^i. \tag{25}$$

We see from (25) that s satisfies either $s = 1$ or $b \mid s$. When $s = 1$, we infer from (22) and (23) that $r^2 = 2v(v + 1)$. This implies that v is a square with $v \equiv 3 \pmod 4$, which is a contradiction. When $b \mid s$, we have $s \ge b$. Hence, by (22) and (23), we get

$$2v^2 + 2v + 1 = c = r^2 + s^2 > s^2 \ge b^2 = (2v + 1)^2 = 4v^2 + 4v + 1,$$

a contradiction.

If c is a prime power, then c can be expressed as (12). Moreover, by the above analysis, (13) then has two solutions $(X, Y, Z) = (a, 1, 2k)$ and $(x, b^{(y-2)/2}, zk)$, $(X_1, Y_1, Z_1) = (a, 1, 2k)$ is the least solution of (13) and z satisfies (17). So we have $z = 2t$ and z is even, a contradiction. Thus, under the hypothesis, (4) has no solution (x, y, z) satisfying $2 \mid y$ and $2 \nmid z$. To sum up, the Theorem is proved.

References

[1] Z. F. Cao and X. L. Dong, *On Terai's conjecture*, Proc. Japan Acad. Ser. A Math. Sci. 74 (1998), 127–129.

[2] M. H. Le, *On the number of solutions of the diophantine equation* $x^2 + D = p^n$, C. R. Acad. Sci. Paris Sér. I Math. 317 (1993), 135–138.

[3] —, *A note on the diophantine equation* $x^2 + b^y = c^z$, Acta Arith. 71 (1995), 253–257.

[4] W. Ljunggren, *Zur Theorie der Gleichung* $x^2 + 1 = Dy^4$, Avh. Norske Vid. Akad. Oslo 5 (1942), 1–27.

[5] L. J. Mordell, *Diophantine Equations*, Academic Press, London, 1969.

[6] C. Störmer, *L'équation* $m \arctan 1/x + n \arctan 1/y = k\pi/4$, Bull. Soc. Math. France 27 (1899), 160–170.

[7] N. Terai, *The Diophantine equation* $x^2 + q^m = p^n$, Acta Arith. 63 (1993), 351–358.

[8] P. Z. Yuan, *On the diophantine equation* $x^2 + b^y = c^z$, J. Sichuan Univ. Nat. Sci. Ser. 35 (1998), 5–7.

[9] P. Z. Yuan and J. B. Wang, *On the diophantine equation* $x^2 + b^y = c^z$, Acta Arith. 84 (1998), 145–147.

Department of Mathematics
Zhanjiang Normal College
Postal Code 524048
Zhanjiang, Guangdong, P.R. China

Received on 14.3.2000
and in revised form on 23.4.2001 (3773)