A note on Terai's conjecture concerning Pythagorean numbers*)

By Xigeng CHEN**) and Maohua LE***)

(Communicated by Shokichi IYANAGA, M. J. A., May 12, 1998)

Abstract: Let (a, b, c) be a primitive Pythagorean triple with $2 \mid a$. In this note we prove that if $b \not\equiv 1 \pmod{16}$, $b^2 + 1 = 2c$, b and c are both odd primes, then the equation $x^2 + b^y = c^z$ has only the positive integer solutions $(x, y, z) = (a, 2, 2)$.

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

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

Then we have

$$(2)\quad a = 2st,\ b = s^2 - t^2,\ c = s^2 + t^2,$$

where s, t are positive integers satisfying $s > t$, $\gcd(s, t) = 1$ and $2 \mid st$. In 1993, Terai [4] conjectured that the equation

$$(3)\qquad x^2 + b^y = c^z,\ x, y, z \in \boldsymbol{N},$$

has only the solution $(x, y, z) = (a, 2, 2)$. This conjecture is not solved as yet. In [4], Terai proved that if $b \equiv 1 \pmod 4$, $b^2 + 1 = 2c$, b, c are odd primes, c splits in the imaginary quadratic field $K = \boldsymbol{Q}(\sqrt{-b})$ and the order d of a prime ideal divisor of $[c]$ in K satisfies either $d = 1$ or $2 \mid d$, then (3) has only the solution $(x, y, z) = (a, 2, 2)$. In this note we prove the following general result.

Theorem. If $b \not\equiv 1 \pmod{16}$, $b^2 + 1 = 2c$, b, c are both odd primes, then (3) has only the solution $(x, y, z) = (a, 2, 2)$.

2. Preliminaries. Lemma 1 ([2] and [3]). The equation

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

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

Lemma 2 ([1, Lemma 2]). Let k be a positive integer. All solutions (X, Y, Z) of the equation

$$X^2 + Y^2 = k^Z,\ X, Y, Z \in \boldsymbol{Z},\quad \gcd(X, Y) = 1,\ Z > 0$$

are given by

$$Z = n,\ X + Y\sqrt{-1} = \lambda_1(X_1 + \lambda_2 Y_1\sqrt{-1})^n$$
$$\text{or } \lambda_1(Y_1 + \lambda_2 X_1\sqrt{-1})^n,$$
$$n \in \boldsymbol{N},\ \lambda_1, \lambda_2 \in \{-1, 1\},$$

where X_1, Y_1 run through all positive integers satisfying

$$X_1^2 + Y_1^2 = k,\ \gcd(X_1, Y_1) = 1.$$

3. Proof of theorem. Since $b^2 + 1 = 2c$ and $2 \nmid b$, we have

$$(4)\qquad \left(\frac{b+1}{2}\right)^2 + \left(\frac{b-1}{2}\right)^2 = c.$$

Notice that c is an odd prime. We see from (4) that

$$(5)\quad (X_1, Y_1) = \left(\frac{b+1}{2}, \frac{b-1}{2}\right), \left(\frac{b-1}{2}, \frac{b+1}{2}\right)$$

are all positive integers X_1, Y_1 satisfying

$$(6)\qquad X_1^2 + Y_1^2 = c,\ \gcd(X_1, Y_1) = 1.$$

Hence, by (2) and (4), we get $s = (b+1)/2$, $t = (b-1)/2$, $s = t + 1$,

$$(7)\quad a = 2t(t+1),\ b = 2t + 1,\ c = 2t^2 + 2t + 1.$$

Let (x, y, z) be a solution of (3). Since b is an odd prime, if $2 \mid z$, then from (3) we get $c^{z/2} + x = b^y$, and $c^{z/2} - x = 1$. It implies that

$$(8)\qquad b^y + 1 = 2c^{z/2}.$$

Since $b + 1 = 2t + 2$ and $c \equiv 1 \pmod{2t + 2}$ by (7), we find from (8) that $2 \mid y$. Since $b^2 + 1 = 2c$, if $z/2 = 1$, then from (1) and (8) we get the solution $(x, y, z) = (a, 2, 2)$. If $z/2 = 2$, then we have $b^y + 1 = 2c^2 = 2((b^2 + 1)/2)^2$. It follows that $2 \equiv 1 \pmod b$, a contradiction. If $z/2 > 2$, by Lemma 1, then we get $(b, y, c, z) = (239, 2, 13, 8)$. It is impossible, by (3). Thus, (3) has only the solution $(x, y, z) = (a, 2, 2)$ with $2 \mid z$.

If $2 \mid y$ and $2 \nmid z$, then the equation

$$X^2 + Y^2 = c^Z,\ X, Y, Z \in \boldsymbol{Z},$$

1991 Mathematics Subject Classification. 11 D 61.

*) Supported by the National Natural Science Foundation of China and the Guangdong Provincial Natural Science Foundation.

**) Department of Mathematics, Maoming Education College. P. R. China.

***) Department of Mathematics, Zhanjiang Teachers College, P. R. China.

$$\gcd(X, Y) = 1, Z > 0$$

has a solution $(X, Y, Z) = (x, b^{y/2}, z)$. Recall that c is an odd prime. By Lemma 2, we get from (4), (5), (6) and (7) that

(9) $x + b^{y/2}\sqrt{-1} = \lambda_1(t + \lambda_2(t+1)\sqrt{-1})^z$ or $\lambda_1((t+1) + \lambda_2 t\sqrt{-1})^z$, $\lambda_1\lambda_2 \in \{-1, 1\}$.

Since $2 \nmid z$, we see from (9) that either $b^{y/2} \equiv 0 \pmod{t+1}$ or $b^{y/2} \equiv 0 \pmod{t}$. This is impossible, by (7).

If $2 \nmid y$ and $2 \nmid z$, then from (3) we get $(-b/c) = 1$, where $(*/*)$ is Jacobi's symbol. Since $c \equiv 1 \pmod 4$ and $c \equiv 2t^2 \pmod b$ by (7), we have $1 = (-b/c) = (b/c) = (c/b) = (2t^2/b) = (2/b)$. It implies that $b \equiv \pm 1 \pmod 8$ and

(10) $$t \equiv 0 \text{ or } 3 \pmod 4,$$

by (7). On the other hand, since $b \equiv -1 \pmod{2t+2}$ and $c \equiv 1 \pmod{2t+2}$, we get from (3) that $x^2 = c^z - b^y \equiv 1^z - (-1)^y \equiv 2 \pmod{2t+2}$. It implies that $x = 2x_1$, where x_1 is a positive integer. Then we get

(11) $$2x_1^2 \equiv 1 \pmod{t+1}.$$

If $t \equiv 3 \pmod 4$, then (11) is impossible. So we have $t \equiv 0 \pmod 4$, by (10). Further, by (11), we get $(2/t+1) = 1$. It implies that $t \equiv 0 \pmod 8$ and $b \equiv 1 \pmod{16}$. Thus, if $b \not\equiv 1 \pmod{16}$, then (3) has no solution (x, y, z) with $2 \nmid z$. The theorem is proved.

References

[1] M.-H. Le: A note on the diophantine equation $x^2 + b^y = c^z$. Acta Arith., **71**, 253–257 (1995).

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

[3] C. Störmer: L'équation m arc tan $\frac{1}{x}$ + n arc tan $\frac{1}{y}$ = $k\frac{\pi}{4}$. Bull. Soc. Math. France, **27**, 160–170 (1899).

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