On Terai's conjecture*)

By Zhenfu CAO and Xiaolei DONG

Department of Mathematics, Harbin Institute of Technology, Harbin 150001, P. R. China

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

Abstract: Terai presented the following conjecture: If $a^2 + b^2 = c^2$ with $a > 0$, $b > 0$, $c > 0$, gcd $(a, b, c) = 1$ and a even, then the diophantine equation $x^2 + b^m = c^n$ has the only positive integral solution $(x, m, n) = (a, 2, 2)$. In this paper we prove that if (i) b is a prime power, $c \equiv 5 \pmod 8$, or (ii) $c \equiv 5 \pmod 8$ is a prime power, then Terai's conjecture holds.

1. Introduction. In 1956, Jeśmanowicz [4] conjectured that if a, b, c are Pythagorean triples, i.e. positive integers a, b, c satisfying $a^2 + b^2 = c^2$, then the Diophantine equation

$$a^x + b^y = c^z$$

has the only positive integral solution $(x, y, z) = (2, 2, 2)$. When a, b, c take some special Pythagorean triples, it was discussed by Sierpinski [14], C. Ko [5-10], J. R. Chen [2], Dem'janenko [3] and others.

In 1993, as an analogue of above conjecture, Terai [16] presented the following:

Conjecture. If $a^2 + b^2 = c^2$ with gcd $(a, b, c) = 1$ and a even, then the Diophantine equation

$$x^2 + b^m = c^n \tag{1}$$

has the only positive integral solution $(x, m, n) = (a, 2, 2)$.

Terai proved that if b and c are primes such that (i) $b^2 + 1 = 2c$, (ii) $d = 1$ or even if $b \equiv 1 \pmod 4$, where d is the order of a prime divisor of $[c]$ in the ideal class group of $\boldsymbol{Q}(\sqrt{-b})$, then the conjecture holds. Further, he proved that if $b^2 + 1 = 2c$, $b < 20$, $c < 200$, then conjecture holds. Recently, X. Chen and M. Le [11] proved that if $b \not\equiv 1 \pmod{16}$, $b^2 + 1 = 2c$, b and c are both odd primes, then the conjecture holds, and P. Yuan and J. Wang [17] proved that if $b \equiv \pm 3 \pmod 8$ is a prime, then Terai's conjecture holds.

In this paper, we consider Terai's conjecture when b or c is prime power. Then we prove the following:

Theorem 1. If b is a prime power, $c \equiv 5 \pmod 8$, then Terai's conjecture holds.

Corollary. If $2k + 1$ is a prime, $k \equiv 1$ or $2 \pmod 4$, then the Diophantine equation

$$x^2 + (2k + 1)^m = (2k^2 + 2k + 1)^n$$

has the only positive integral solution $(x, m, n) = (2k^2 + 2k, 2, 2)$.

Theorem 2. If $c \equiv 5 \pmod 8$ is a prime power, then Terai's conjecture holds.

2. Some lemmas. We use the following lemmas to prove our theorems.

Lemma 1. If a, b, c are positive integers satisfying $a^2 + b^2 = c^2$, where $2 \mid a$, gcd $(a, b, c) = 1$, then

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

where $s > t > 0$, gcd $(s, t) = 1$ and $s \not\equiv t \pmod 2$.

Lemma 2 (Störmer [15]). The Diophantine equation

$$x^2 + 1 = 2y^n$$

has no solutions in integers $x > 1$, $y \geq 1$ and n odd ≥ 3.

Lemma 3 (Ljunggren [12]). The Diophantine equation

$$x^2 + 1 = 2y^4$$

has the only positive integral solutions $(x, y) = (1, 1)$ and $(239, 13)$.

Lemma 4 (Cao [1]). If p is an odd prime and the Diophantine equation

$$x^p + 1 = 2y^2 (|y| > 1)$$

has integral solution x, y, then $2p \mid y$.

Now, we assume that a, b, c are Pythagorean triples with gcd $(a, b, c) = 1$ and $2 \mid a$.

Lemma 5. If $c \equiv 5 \pmod 8$, then we have

$$(b/c) = (c/b) = -1,$$

where $(*/*)$ denotes Jacobi's symbol.

---

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

1991 Mathematics Subject Classification: 11D61.

Proof. From Lemma 1, we have

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

where $s > t > 0$, gcd $(s, t) = 1$ and $s \not\equiv t \pmod 2$. Since $c \equiv 5 \pmod 8$, we have

$$(c/b) = (b/c) = (s^2 - t^2/s^2 + t^2) = ((s^2 + t^2) - 2t^2/s^2 + t^2).$$
$$= (-2t^2/s^2 + t^2) = (-1/s^2 + t^2)(2/s^2 + t^2)(t^2/s^2 + t^2) = -1.$$

Thus, the proof is completed. □

Lemma 6. If $c \equiv 5 \pmod 8$, then the integral solutions of equation (1) satisfy $2 \mid m$, $2 \mid n$.

Proof. Suppose equation (1) has positive integral solution (x, m, n). We have

$$x^2 \equiv c^n \pmod b,\ x^2 \equiv -b^m \pmod c.$$

Thus, by Lemma 5 we have

$$1 = (c^n/b) = (c/b)^n = (-1)^n,$$
$$1 = (-b^m/c) = (-1/c)(b/c)^m = (-1)^m,$$

and so $2 \mid m$, $2 \mid n$. The lemma is proved. □

3. Proof of theorems. Proof of Theorem 1. Suppose (x, m, n) is a positive integral solution of equation (1). By Lemma 6, put $m = 2m_1$, $n = 2n_1$, where m_1 and n_1 are some positive integers. Then equation (1) gives

$$x^2 + b^{2m_1} = c^{2n_1}. \tag{2}$$

Since gcd $(a, b, c) = 1$, $a^2 + b^2 = c^2$, $2 \mid a$, we have gcd $(b, c) = 1$ and $2 \nmid bc$. Thus from (2) and Lemma 1, we have

$$x = 2uv,\ b^{m_1} = u^2 - v^2,\ c^{n_1} = u^2 + v^2, \tag{3}$$

where $u > v > 0$, gcd $(u, v) = 1$ and $u \not\equiv v \pmod 2$. From $b^{m_1} = u^2 - v^2$ in (3), we have

$$u - v = 1,\ u + v = b^{m_1} \tag{4}$$

since b is a prime power and gcd $(u - v, u + v) = 1$. From (4) we have

$$u = (b^{m_1} + 1)/2,\ v = (b^{m_1} - 1)/2.$$

Substituting these into $c^{n_1} = u^2 + v^2$ in (3), we have

$$2c^{n_1} = b^{2m_1} + 1,\ c > b > 1. \tag{5}$$

If $n_1 > 2$, then without loss of generality, we may assume that $4 \mid n_1$, or $p \mid n_1$ (p is an odd prime). By Lemma 2, (5) is impossible if $p \mid n_1$. If $4 \mid n_1$, then by Lemma 3, (5) gives

$$c^{n_1/4} = 13,\ b^{m_1} = 239$$

so $m_1 = 1$, $b = 239$, $c = 13$, a contradiction since $c > b$.

If $n_1 = 2$, then by Lemma 4, (5) gives $m_1 = 2^e$, $e \geq 0$. When $e = 0$, from $2c^2 = b^2 + 1$ we have $b > c$, a contradiction. When $e > 0$, equation (5) gives

$$2c^2 = (b^{m_1/2})^4 + 1,\ c > b > 1,$$

which is impossible (see [13], p. 18).

If $n_1 = 1$, then (5) gives $2c = b^{2m_1} + 1$. On the other hand, since b is a prime power, from $a^2 + b^2 = c^2$, gcd $(a, b, c) = 1$ and $2 \mid a$, we have

$$c - a = 1,\ c + a = b^2$$

and so $2c = b^2 + 1$. Thus $m_1 = 1$. The Theorem 1 is proved. □

Proof of Theorem 2. Suppose (x, m, n) is a positive integral solution of equation (1). From Lemma 6, we have $m = 2m_1$, $n = 2n_1$, where m_1 and n_1 are some positive integers. By Lemma 1, we have $b = u^2 - v^2$, $c = u^2 + v^2$, and (1) gives

$$x = 2st,\ (u^2 - v^2)^{m_1} = s^2 - t^2,\quad (u^2 + v^2)^{n_1} = s^2 + t^2, \tag{6}$$

where $u > v > 0$, gcd $(u, v) = 1$, $u \not\equiv v \pmod 2$, and $s > t > 0$, gcd $(s, t) = 1$ and $s \not\equiv t \pmod 2$. From $(u^2 - v^2)^{m_1} = s^2 - t^2$, we see that

$$s + t = b_1^{m_1},\ s - t = b_2^{m_1},\ u^2 - v^2 = b_1 b_2,$$

where gcd $(b_1, b_2) = 1$, b_1 and b_2 are some positive integers. Hence

$$s = (b_1^{m_1} + b_2^{m_1})/2,\ t = (b_1^{m_1} - b_2^{m_1})/2.$$

Substituting these into $(u^2 + v^2)^{n_1} = s^2 + t^2$ in (6), we have

$$2(u^2 + v^2)^{n_1} = b_1^{2m_1} + b_2^{2m_1},\ \gcd(b_1, b_2) = 1. \tag{7}$$

When $2 \mid n_1$, from (7) we see that $b_1^{2m_1} + b_2^{2m_1} \equiv 2 \pmod{16}$ since $(u^2 + v^2)^{n_1} \equiv 1 \pmod 8$. But $b_1 b_2 = u^2 - v^2 \equiv \pm 3 \pmod 8$ since $u^2 + v^2 \equiv 5 \pmod 8$. If $2 \nmid m_1$ then $b_1^{2m_1} + b_2^{2m_1} \equiv 1 + 9 \equiv 10 \pmod{16}$, a contradiction. If $2 \mid m_1$, then equation (7) gives that the equation

$$2z^2 = x^4 + y^4,\ \gcd(x, y) = 1$$

has positive integral solution $z = (u^2 + v^2)^{n_1/2} > 1$, which is impossible (see [13], p. 18).

When $2 \nmid n_1$, from (7) we have $b_1^{2m_1} + b_2^{2m_1} \equiv 10 \pmod{16}$. So $2 \nmid m_1$. If $m_1 > 1$, then $p \mid m_1$, p is an odd prime. From (7), we have

$$(u^2 + v^2)^{n_1} = \frac{(b_1^{2m_1/p})^p + (b_2^{2m_1/p})^p}{2}$$
$$= \frac{b_1^{2m_1/p} + b_2^{2m_1/p}}{2} \cdot \frac{(b_1^{2m_1/p})^p + (b_2^{2m_1/p})^p}{b_1^{2m_1/p} + b_2^{2m_1/p}}.$$

Since $u^2 + v^2$ is a prime power, gcd

$$\left(\frac{b_1^{2m_1/p} + b_2^{2m_1/p}}{2},\ \frac{(b_1^{2m_1/p})^p + (b_2^{2m_1/p})^p}{b_1^{2m_1/p} + b_2^{2m_1/p}}\right) = 1 \text{ or}$$

p, and $p \,\Big\|\, \dfrac{(b_1^{2m_1/p})^p + (b_2^{2m_1/p})^p}{b_1^{2m_1/p} + b_2^{2m_1/p}}$ if $u^2 + v^2$ is a power of p. Thus we have $(b_1^{2m_1/p} + b_2^{2m_1/p})/2 = 1$, which is impossible.

Thus $m_1 = 1$. Then we show that $n_1 = 1$. If $b_1, b_2 > 1$, then we have

$$u^{2n_1} < 2(u^2 + v^2)^{n_1} = b_1^2 + b_2^2 \leq b_1^2 b_2^2 = (u^2 - v^2)^2 < u^4.$$

Since $2 \nmid n_1$, we obtain $n_1 = 1$.

If $b_1 = 1$ or $b_2 = 1$, then we have

$$u^{2n_1} < 2(u^2 + v^2)^{n_1} = (u^2 - v^2)^2 + 1 < u^4.$$

Since $2 \nmid n_1$, we obtain $n_1 = 1$.

This completes the proof of Theorem2. $\square$

Acknowledgements. This paper was finished two years ago. The proof of "$n_1 = 1$" in proof of Theorem 2 was more complex at that time. Now the proof is simplified according to referee's report. The authors would like to thank the referee for his valuable suggestions.

References

[1] Z. Cao: On the Diophantine equation $x^{2n} - Dy^2 = 1$. Proc. Amer. Math. Soc., **98(1)**, 11–16 (1986).

[2] J. R. Chen: On Jeśmanowicz' conjecture Sichuan Daxue Xuebao, **2**, 19–25 (1962) (in Chinese).

[3] V. A. Dem'janenko: On Jeśmanowicz' problem for Pythagorean numbers. Izv. Vysš. Učebn. Zaved. Matematika, **48(5)**, 52–56 (1965) (in Russian).

[4] L. Jeśmanowicz': Some remarks on Pythagorean numbers. Wiakom. Mat., ser. 2, **1(2)**, 196–202 (1956).

[5] C. Ko: On Pythagorean numbers. Sichuan Daxue Xuebao, **1**, 73–80 (1958) (in Chinese).

[6] C. Ko: On Jeśmanowicz' conjecture. Sichuan Daxue Xuebao, **2**, 31–40 (1958) (in Chinese).

[7] C. Ko: On Pythagorean numbers $2n + 1$, $2n(n + 1)$, $2n(n + 1) + 1$. Sichuan Daxue Xuebao, **3**, 9–13 (1963) (in Chinese).

[8] C. Ko: On Pythagorean numbers $2n + 1$, $2n(n + 1)$, $2n(n + 1) + 1$ (III). Sichuan Daxue Xuebao, **4**, 11–24 (1964) (in Chinese).

[9] C. Ko: On Diophantine equation $(a^2 - b^2)^x + (2ab)^y = (a^2 + b^2)^z$. Sichuan Daxue Xuebao, **3**, 25–34 (1959) (in Chinese).

[10] C. Ko and Q. Sun: On Pythagorean numbers $2n + 1$, $2n(n + 1)$, $2n(n + 1) + 1$ (II). Sichuan Daxue Xuebao, **3**, 1–6 (1964) (in Chinese).

[11] X. Chen and M. Le: A note on Terai's conjecture concerning Pythagorean numbers. Proc. Japan Acad., **74A**, 80–81 (1998).

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

[13] L. J. Mordell: Diophantine Equations. Academic Press (1969).

[14] W. Sierpinski: On the equation $3^x + 4^y = 5^z$. Wiakom. Mat., ser. 2, **1(2)**, 194–195 (1956).

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

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

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