X. ZHANG
KODAI MATH. J.
41 (2018), 413–420

ON TERAI'S CONJECTURE

Xin Zhang

Abstract

Let p be an odd prime such that $b^r + 1 = 2p^t$, where r, t are positive integers and $b \equiv 3, 5 \pmod 8$. We show that the Diophantine equation $x^2 + b^m = p^n$ has only the positive integer solution $(x, m, n) = (p^t - 1, r, 2t)$. We also prove that if b is a prime and $r = t = 2$, then the above equation has only one solution for the case $b \equiv 3, 5, 7 \pmod 8$ and the case d is not an odd integer greater than 1 if $b \equiv 1 \pmod 8$, where d is the order of prime divisor of ideal (p) in the ideal class group of $\mathbf{Q}(\sqrt{-q})$.

1. Introduction and main results

In 1956, Jeśmanowicz [5] conjectured that if positive integers satisfying a, b, c are Pythagorean numbers, i.e. $a^2 + b^2 = c^2$, then the Diophantine equation

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

has only the positive integer solution $(x, y, z) = (2, 2, 2)$. As an analogue of Jeśmanowicz's conjecture, Terai proposed the following conjecture.

Conjecture 1.1 (Terai's conjecture [10]). *If (a, b, c) is primitive Pythagorean triple such that*

$$a^2 + b^2 = c^2, \quad a, b, c \in \mathbf{N}, \quad \gcd(a, b) = 1, \quad a \equiv 0 \pmod 2,$$

then the Diophantine equation

$$x^2 + b^m = c^n$$

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

In [10], Terai proved that if p and q are primes such that (i) $q^2 + 1 = 2p$ and (ii) d is not an odd integer greater than 1 if $q \equiv 1 \pmod 4$, then the Diophantine equation $x^2 + q^m = p^n$ has only the positive integer solution

---

Mathematics Subject Classification. 11D41; 11D61.

Key words and phrases. Diophantine equation; Terai's conjecture; integer solution.

This work was supported by National Natural Science Foundation of China (Grant Nos. 11401330, 11471162).

Received March 22, 2017; revised July 18, 2017.

$(x, m, n) = (p-1, 2, 2)$, where d is the order of a prime divisor of (p) in the ideal class group of $\mathbf{Q}(\sqrt{-q})$.

Terai's conjecture has been verified to be true in many special cases:

- $b > 8 \cdot 10^6$, $b \equiv 5 \pmod 8$, c is a prime power (Le [6]);
- $b^2 + 1 = 2c$, $b \not\equiv 1 \pmod{16}$, both b and c are odd primes (Chen and Le [3]);
- $b \equiv 7 \pmod 8$, either b is a prime or c is a prime (Le [7]);
- $c \equiv 5 \pmod 8$, b or c is a prime power (Cao and Dong [2]);
- $b \equiv \pm 5 \pmod 8$, c is a prime (Yuan and Wang [12]).

In 2014, Terai [11] proved that if $q \equiv 3, 5 \pmod 8$ is a prime such that $q^t + 1 = 2c$, then the Diophantine equation $x^2 + q^m = c^n$ has only the positive integer solution $(x, m, n) = (c-1, t, 2)$. In 2015, Deng [4] proved that if q is a prime such that $q^t + 1 = 2c^2$, then the Diophantine equation $x^2 + q^m = c^{2n}$ has only the positive integer solution $(x, m, n) = (c^2 - 1, t, 2)$.

In this note, using elementary methods, we mainly prove the following theorems.

Theorem 1.2. *Let b be a positive integer with $b \equiv 3, 5 \pmod 8$. Let p be a prime such that $b^r + 1 = 2p^t$, where r, t are positive integers. Then the Diophantine equation*

$$x^2 + b^m = p^n \tag{1.1}$$

has only the positive integer solution $(x, m, n) = (p^t - 1, r, 2t)$.

Example 1.3. The only positive integral solution of each of the equations

(1) $x^2 + (5 \times 137)^m = 7^n$, (2) $x^2 + (319 \times 43)^m = 19^n$,

(3) $x^2 + (15 \times 2083)^m = 5^n$, (4) $x^2 + 21^m = 97241^n$,

(5) $x^2 + 35^m = 750313^n$, (6) $x^2 + (23 \times 353)^m = 5741^n$

is given by $(x, m, n) = (342, 1, 6), (6858, 1, 6), (3124, 1, 10), (97240, 4, 2), (750312, 4, 2), (32959080, 2, 4)$, respectively.

Remark 1.4. All of these cases can be obtained by Theorem 1.2 directly.

Theorem 1.5. *Let p and q be primes such that*

(i) $q^2 + 1 = 2p^2$,

(ii) *d is not an odd integer greater than 1 if $q \equiv 1 \pmod 8$, where d is the order of a prime divisor of (p) in the ideal class group of $\mathbf{Q}(\sqrt{-q})$.*

Then the Diophantine equation

$$x^2 + q^m = p^n$$

has only the positive integer solution $(x, m, n) = (p^2 - 1, 2, 4)$.

Example 1.6. There are exactly three pairs (p,q) in the range $q < 10^{12}$ satisfying conditions (i) and (ii) in Theorem 1.5:

$$(p,q) = (5,7), (29,41), (44560482149, 63018038201),$$

which were obtained by using Pari/GP.

Remark 1.7. Our proofs of Theorem 1.2 and Theorem 1.5 are mainly based on Bugeaud's result [1].

2. Some lemmas

We need the following lemmas to prove the main results.

Lemma 2.1 (Störmer [9]). *The Diophantine equation*

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

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

Lemma 2.2 (Ljunggren [8]). *The Diophantine equation*

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

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

Lemma 2.3 (Bugeaud [1]). *Let* $D > 2$ *be an integer and let* p *be an odd prime which does not divide* D. *If there exists a positive integer* a *with* $D = 3a^2 + 1$ *and* $p = 4a^2 + 1$, *then the Diophantine equation*

$$x^2 + D^m = p^n,$$

in positive integer x, m *and* n *has at most three solutions* (x,m,n), *namely*

$$(a,1,1), \quad (8a^2 + 3a, 1, 3), \quad (x_3, m_3, n_3),$$

with m_3 (*if the third solution exists*) *even. Otherwise, the Diophantine equation*

$$x^2 + D^m = p^n,$$

in positive integer x, m *and* n *has at most two solutions. If these are* (x_1, m_1, n_1) *and* (x_2, m_2, n_2), *then* $m_1 \not\equiv m_2 \pmod 2$.

Lemma 2.4. *Let* p *be an odd prime and* c *a positive integer. If* (m_0, n_0) *is a positive integer solution of*

$$2p^m = c^n + 1,$$

then $n_0 = 2^s$ *for some nonnegative integer* s.

Proof. It's obvious that the equation has no solution satisfying $m_0, n_0 > 0$ when $c = 1, 2$. So we consider $c \geq 3$. Let (m_0, n_0) be a solution of $2p^m - c^n$

$= 1$. Supposing that there exists an odd prime l dividing n_0, we have $n_0 = kl$ for some integer $k \geq 1$. Then

$$2p^{m_0} = c^{n_0} + 1 = c^{kl} + 1 = (c^k + 1)(c^{k(l-1)} - c^{k(l-2)} + \cdots + 1).$$

Hence we have

$$\frac{c^{kl} + 1}{c^k + 1} = c^{k(l-1)} - c^{k(l-2)} + \cdots + 1 > l, \tag{2.1}$$

and

$$c^k + 1 = 2p^{m_1},$$

for some $1 \leq m_1 < m_0$. Therefore,

$$p^{m_0 - m_1} = \frac{c^{kl} + 1}{c^k + 1} = \frac{(2p^{m_1} - 1)^l + 1}{2p^{m_1}} = \sum_{i=1}^{l} \binom{l}{i} (2p^{m_1})^{i-1} (-1)^{l-i}. \tag{2.2}$$

Modulo p in both sides of the equation (2.2), we obtain

$$0 \equiv \sum_{i=1}^{l} \binom{l}{i} (2p^{m_1})^{i-1} (-1)^{l-i} \equiv l \pmod{p}.$$

Hence $l = p$. Then by equation (2.1) and equation (2.2) we have $p^{m_0 - m_1} > p$.

On the other hand, modulo p^2 in both sides of the equation (2.2), we have

$$p^{m_0 - m_1} = \sum_{i=1}^{l} \binom{l}{i} (2p^{m_1})^{i-1} (-1)^{l-i} \equiv p \pmod{p^2}.$$

Hence $p^{m_0 - m_1} = p$, a contradiction. So $n_0 = 2^s$ for some nonnegative integer s. Thus the proof of Lemma 2.4 is finished. □

3. Proofs of main results

Proof of Theorem 1.2. Let

$$b = b_1^2 \prod_{i=1}^{l} p_i \prod_{j=1}^{k} q_j,$$

where p_i, q_j are different primes such that $p_i \equiv 3, 5 \pmod{8}$, $q_j \equiv 1, 7 \pmod{8}$. We show that if $b \equiv 3$ or $5 \pmod{8}$, then l is odd. Otherwise, we have

$$\prod_{i=1}^{l} p_i \equiv \pm 1 \pmod{8}, \quad \prod_{j=1}^{k} q_j \equiv \pm 1 \pmod{8}.$$

Thus $b \equiv \pm 1 \pmod{8}$, a contradiction. According to $b^r + 1 = 2p^t$ and Lemma 2.4, we obtain $r = 2^s$ for some nonnegative integer s.

If $s = 0$, that is $r = 1$, then $b + 1 = 2p^t$. Thus $\left(\frac{2p^t}{p_i}\right) = 1$ for $i = 1, \ldots, l$. In view of $p_i \equiv 3, 5 \pmod 8$, we see that $\left(\frac{2}{p_i}\right) = -1$. Hence $\left(\frac{p}{p_i}\right) = -1$ for $i = 1, \ldots, l$ and t odd. Similarly, we have $\left(\frac{p}{q_j}\right) = 1$ for $j = 1, \ldots, k$. It's easy to see $\gcd(b, p) = 1$ and

$$\left(\frac{b}{p}\right) = \left(\frac{-1}{p}\right). \tag{3.1}$$

If $p \equiv 1 \pmod 4$ then we have

$$1 = \left(\frac{-1}{p}\right) = \left(\frac{b}{p}\right) = \prod_{i=1}^{l}\left(\frac{p_i}{p}\right)\prod_{j=1}^{k}\left(\frac{q_j}{p}\right) = \prod_{i=1}^{l}\left(\frac{p}{p_i}\right)\prod_{j=1}^{k}\left(\frac{p}{q_j}\right) = -1,$$

which is impossible. So

$$p \equiv 3 \pmod 4. \tag{3.2}$$

Hence there doesn't exist a positive integer a such that $p = 4a^2 + 1$. It is obvious that $(p^t - 1, 1, 2t)$ is a solution of (1.1). Assume that (x_0, m_0, n_0) is another solution of (1.1). Then $x_0^2 + b^{m_0} = p^{n_0}$. Hence

$$x_0^2 \equiv -b^{m_0} \pmod p.$$

Thus $\left(\frac{-b^{m_0}}{p}\right) = 1$. Then by (3.1) and (3.2) we have m_0 is odd. By Lemma 2.3, this is impossible. Hence the equation (1.1) has no other solution in this case.

If $s \geq 1$, then $r = 2^s$ is even. By $b^r + 1 = 2p^t$, we have

$$p \equiv 1 \pmod 4$$

and

$$\left(\frac{2p^t}{p_i}\right) = 1 \quad \text{for } i = 1, \ldots, l.$$

In view of $p_i \equiv 3, 5 \pmod 8$, we see that $\left(\frac{2}{p_i}\right) = -1$. Hence $\left(\frac{p}{p_i}\right) = -1$ for $i = 1, \ldots, l$ and t odd. Similarly, we have $\left(\frac{p}{q_j}\right) = 1$ for $j = 1, \ldots, k$. Then we have

$$\left(\frac{b}{p}\right) = \prod_{i=1}^{l}\left(\frac{p_i}{p}\right)\prod_{j=1}^{k}\left(\frac{q_j}{p}\right) = \prod_{i=1}^{l}\left(\frac{p}{p_i}\right)\prod_{j=1}^{k}\left(\frac{p}{q_j}\right) = -1. \tag{3.3}$$

It is obvious that $(p^t - 1, r, 2t)$ is a solution of equation (1.1). Let (x_0, m_0, n_0) be another solution of the equation (1.1). Then $x_0^2 + b^{m_0} = p^{n_0}$. Hence

$$x_0^2 \equiv -b^{m_0} \pmod p.$$

Thus $\left(\dfrac{-b^{m_0}}{p}\right) = 1$. Then by equation (3.3) and $p \equiv 1 \pmod 4$ we obtain m_0 is even. So we have $m_0 \equiv r \pmod 2$. By Lemma 2.3, this is impossible. Hence the equation (1.1) has no other solution in this case.

This completes the proof of Theorem 1.2.

Proof of Theorem 1.5. Assume that (x_0, m_0, n_0) is a solution of the equation

$$x^2 + q^m = p^n. \tag{3.4}$$

Then we have

$$x_0^2 + q^{m_0} = p^{n_0}. \tag{3.5}$$

The proof is divided into two cases depending on the parity of n_0 as follows.

Case 1. n_0 is even. Let $n_0 = 2k$. Then we obtain

$$q^{m_0} = (p^k + x_0)(p^k - x_0).$$

Because $q^2 + 1 = 2p^2$, we have $\gcd(2p, q) = 1$. So $\gcd(p^k + x_0, p^k - x_0) = 1$. Hence $p^k - x_0 = 1$ and $p^k + x_0 = q^{m_0}$. Then

$$q^{m_0} + 1 = 2p^k.$$

By Lemma 2.4 we know that $m_0 = 2^s$ for some nonnegative integer s. Now we show that $s > 0$. Otherwise, we have $q + 1 = 2p^k$ and $q^2 + 1 = 2p^2$. This forces $q + 1 | q^2 + 1$, which is impossible. Hence $s \geq 1$ and m_0 is even. By using Lemmas 2.1 and 2.2, we have $k = 1$ or 2. Then we obtain that the equation (3.4) has the only solution $(m_0, n_0) = (2, 4)$.

Case 2. n_0 is odd. Assume $(q, p) = (3s^2 + 1, 4s^2 + 1)$. Then we have

$$s^2 + q = p.$$

Hence

$$q^2 + 1 = 2p^2 = 2(s^2 + q)^2 \geq 2(1 + q)^2.$$

This is impossible. Thus $(q, p) \neq (3s^2 + 1, 4s^2 + 1)$. It's easy to see $(p^2 - 1, 2, 4)$ is a solution of the equation (3.4). By using Lemma 2.3, m_0 is odd.

We note that $q^2 + 1 = 2p^2$ implies $p \equiv 1 \pmod 4$ and $q \equiv 1, 7 \pmod 8$. If $q \equiv 7 \pmod 8$, then by (3.5) we have $3 \equiv 3^{m_0} \equiv 1 \pmod 4$, which is impossible. This forces $q \equiv 1 \pmod 8$.

Let $K = \mathbf{Q}(\sqrt{-q})$ and $\mathcal{O}_K$ its integer ring. Then $\mathcal{O}_K = \mathbf{Z}[\sqrt{-q}]$. By (3.5) we have $\left(\dfrac{-q}{p}\right) = 1$. So (p) is completely split in $\mathcal{O}_K$. Hence $p\mathcal{O}_K = \mathfrak{p}\bar{\mathfrak{p}}$, where $\mathfrak{p}$, $\bar{\mathfrak{p}}$ are distinct prime ideals. Therefore we obtain the ideal decomposition:

$$(x_0 - q^{(m_0-1)/2}\sqrt{-q})(x_0 + q^{(m_0-1)/2}\sqrt{-q}) = \mathfrak{p}^{n_0}\bar{\mathfrak{p}}^{n_0}$$

in $\mathcal{O}_K$. Note that the ideals $(x_0 - q^{(m_0-1)/2}\sqrt{-q})$ and $(x_0 + q^{(m_0-1)/2}\sqrt{-q})$ are relatively prime and the fact that $\mathcal{O}_K$ is a Dedekind domain. We have either $(x_0 + q^{(m_0-1)/2}\sqrt{-q}) = \mathfrak{p}^{n_0}$ or $\bar{\mathfrak{p}}^{n_0}$. We may assume that

$$(x_0 + q^{(m_0-1)/2}\sqrt{-q}) = \mathfrak{p}^{n_0}.$$

Then $\mathfrak{p}^{n_0}$ is a principal ideal and so $n_0 = dt$ for some integer t. By the assumption that d is 1 or even and n_0 is odd, we have $d = 1$. So $\mathfrak{p}$ is a principal ideal. Let

$$\mathfrak{p} = (a + b\sqrt{-q}), \tag{3.6}$$

with integers a, b. Then we obtain

$$x_0 + q^{(m_0-1)/2}\sqrt{-q} = \pm(a + b\sqrt{-q})^{n_0}.$$

Thus we have

$$q^{(m_0-1)/2} = \pm b \sum_{j=0}^{(n_0-1)/2} \binom{n_0}{2j+1} a^{n_0-2j-1} b^{2j} (-q)^j.$$

Therefore $b = \pm q^t$ for some integer $0 \le t \le \dfrac{m_0 - 1}{2}$. By (3.6), we have

$$N_{K/\mathbf{Q}}(\mathfrak{p}) = a^2 + b^2 q.$$

That is

$$p = a^2 + q^{2t+1}.$$

Hence

$$q^2 + 1 = 2p^2 = 2(a^2 + q^{2t+1})^2 \ge 2(1 + q)^2,$$

a contradiction. This completes the proof of Theorem 1.5.

Acknowledgments. The author would like to thank the referee for helpful comments and valuable suggestions.

References

[1] Y. Bugeaud, On some exponential Diophantine equations (English summary), Monatsh. Math. **132** (2001), 93–97.

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

[3] X. Chen and M. Le, A note on Terai's conjecture concerning Pythagorean numbers (English summary), Proc. Japan Acad. Ser. A. Math. Sci. **74** (1998), 80–81.

[4] M. Deng, A note on the Diophantine equation $x^2 + q^m = c^{2n}$, Proc. Japan Acad. Ser. A. Math. Sci. **91** (2015), 15–18.

[5] L. Jeśmanowicz, Several remarks on Pythagorean numbers, Wiadom. Mat. (2) **1** (1955/1956), 196–202.

[6] M. Le, A note on the Diophantine equation $x^2 + b^y = c^z$, Acta Arith. **71** (1995), 253–257.
[7] M. Le, On Terai's conjecture concerning Pythagorean numbers, Acta Arith. **100** (2001), 41–45.
[8] W. Ljunggren, Zur Theorie der Gleichung $x^2 + 1 = Dy^4$ (in German), Avh. Norske Vid. Akad. Oslo. I. (1942).
[9] C. Störmer, Solution complète en nombres entiers de l'equation $m \arctan \frac{1}{x} + n \arctan \frac{1}{y} = k\frac{\pi}{4}$ (in French), Bull. Soc. Math. France **27** (1899), 160–170.
[10] N. Terai, The Diophantine equation $x^2 + q^m = p^n$, Acta Arith. **63** (1993), 351–358.
[11] N. Terai, A note on the Diophantine equation $x^2 + q^m = c^n$, Bull. Aust. Math. Soc. **90** (2014), 20–27.
[12] P. Yuan and J. Wang, On the Diophantine equation $x^2 + b^y = c^z$, Acta Arith. **84** (1998), 145–147.

Xin Zhang
School of Mathematical and Physics
Qingdao University of Science and Technology
Qingdao 266000
P. R. China
E-mail: Xin_zw_Zhang@126.com