BULL. AUSTRAL. MATH. SOC. 11D61
VOL. 61 (2000) [329–334]

ON TERAI'S CONJECTURE CONCERNING PYTHAGOREAN NUMBERS

MAOHU A. LE

In this paper we prove that if a, b, c, r are fixed positive integers satisfying $a^2 + b^2 = c^r$, $\gcd(a,b) = 1$, $a \equiv 3 \pmod 8$, $2 \parallel b$, $r > 1$, $2 \nmid r$, and c is a prime power, then the equation $a^x + b^y = c^z$ has only one positive integer solution $(x,y,z) = (2,2,r)$ satisfying $x > 1$, $y > 1$ and $z > 1$.

1. INTRODUCTION

Let $\mathbb{Z}$, $\mathbb{N}$ be the sets of integers and positive integers respectively. Let a, b, c, m, n, r be fixed positive integers satisfying

$$(1) \qquad a^m + b^n = c^r,\ \gcd(a,b) = 1,\ a > 1,\ b > 1,\ m > 1,\ n > 1,\ r > 1.$$

In 1994, Terai [**5**] conjectured that the equation

$$(2) \qquad a^x + b^y = c^z,\ x, y,\ z \in \mathbb{N},\ x > 1,\ y > 1,\ z > 1,$$

has only one solution $(x,y,z) = (m,n,r)$. This conjecture has been proved for some special cases (see [**3, 5, 6, 7, 8**]). But, in general, the problem is not solved as yet.

In [**7**] and [**8**], Terai proved that if $m = n = 2$, $2 \nmid r$, $a \equiv 3 \pmod 8$, $2 \parallel b$, $(b/a) = -1$ and either $a \geqslant 41b$ or r is a large prime, where $(*/*)$ denotes the Jacobi symbol, then (2) has only one solution $(x,y,z) = (2,2,r)$. The proofs of these results used a lower bound for linear forms in two logarithms due to Laurent, Mignotte and Nesterenko [**1**]. In this paper, using some elementary methods, we prove a general result as follows.

THEOREM. *If $m = n = 2$, $2 \nmid r$, $a \equiv 3 \pmod 8$, $2 \parallel b$ and c is a prime power, then (2) has ony one solution $(x,y,z) = (2,2,r)$.*

Received 19th July, 1999
Supported by the National Natural Science Foundation of China, the Guangdong Provincial Natural Science Foundation and the Natural Science Foundation of the Higher Education Department of Guangdong Province.

2. Preliminaries

Lemma 1. [**4**, pp.12–13] *Every solution (X, Y, Z) of the equation*

$$X^2 + Y^2 = Z^2,\ X, Y, Z \in \mathbb{N},\ \gcd(X, Y) = 1,\ 2 \mid Y, \tag{3}$$

can be expressed as

$$X = u^2 - v^2,\ Y = 2uv,\ Z = u^2 + v^2,$$

where u, v are positive integers satisfying $u > v$, $\gcd(u, v) = 1$ and $2 \mid uv$.

Lemma 2. [**4**, pp.122–124] *Let r be a positive integer with $2 \nmid r$. Every solution $(X, Y, Z,)$ of the equation*

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

can be expressed as

$$Z = u^2 + v^2,\ X + Y\sqrt{-1} = \lambda_1\big(u + \lambda_2 v\sqrt{-1}\big)^r,\ \lambda_1, \lambda_2 \in \{-1, 1\},$$

where u, v are coprime positive integers.

Lemma 3. [**4**, Theorem 4.2] *The equation*

$$X^4 - Y^4 = Z^2,\ X, Y, Z \in \mathbb{N},\ \gcd(X, Y) = 1 \tag{5}$$

has no solution (X, Y, Z).

Lemma 4. [**2**, Lemma 4] *Let D_1, D_2 be positive integers with $\min(D_1, D_2) > 1$. Let p be an odd prime with $p \nmid D_1 D_2$. If the equation*

$$D_1 X^2 + D_2 Y^2 = p^Z,\ X, Y, Z \in \mathbb{Z},\ \gcd(X, Y) = 1,\ Z > 0, \tag{6}$$

has solutions (X, Y, Z), then it has a unique solution (X_1, Y_1, Z_1) satisfying $X_1 > 0$, $Y_1 > 0$ and $Z_1 \leqslant Z$, 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*

$$Z = Z_1 t,\ t \in \mathbb{N},\ 2 \nmid t,$$
$$X\sqrt{D_1} + Y\sqrt{-D_2} = \lambda_1\big(X_1\sqrt{D_1} + \lambda_2 Y_1\sqrt{-D_2}\big)^t, \quad \lambda_1, \lambda_2 \in \{-1, 1\}.$$

We now show that the condition $(b/a) = -1$ can be eliminated from the results of [**7**] and [**8**].

https://doi.org/10.1017/S0004972700022334 Published online by Cambridge University Press

Lemma 5. *Let $m = n = 2$, $2 \nmid r$, $a \equiv 3 \pmod 8$ and $2 \parallel b$. If (x, y, z) is a solution of (2) with $(x, y, z) \neq (2, 2, r)$, then we have either*

$$2 \mid x,\ x \geqslant 6,\ y = 2,\ 2 \nmid z \tag{7}$$

or

$$2 \parallel x,\ x \geqslant 10,\ y = 4,\ 2 \parallel z. \tag{8}$$

Proof: Since $m = n = 2$, we get from (1) that

$$a^2 + b^2 = c^r,\ \gcd(a, b) = 1,\ a > 1,\ b > 1,\ r > 1. \tag{9}$$

Further, since $a \equiv 3 \pmod 8$, $2 \parallel b$ and $2 \nmid r$, we see from (9) that $c \equiv 5 \pmod 8$. Hence, by Lemma 2, we find from (9) that

$$a + b\sqrt{-1} = \lambda_1 \left(u + \lambda_2 v\sqrt{-1}\right)^r,\ \lambda_1, \lambda_2 \in \{-1, 1\}, \tag{10}$$

where u, v are positive integers satisfying

$$u^2 + v^2 = c,\ \gcd(u, v) = 1. \tag{11}$$

Since $2 \nmid r$, by (10) and (11), we get

$$\begin{aligned} a &= \lambda_1 u \sum_{i=0}^{(r-1)/2} \binom{r}{2i} u^{r-2i-1} \left(-v^2\right)^i \equiv 2^{r-1} \lambda_1 u^r \pmod c, \\ b &= \lambda_1 \lambda_2 v \sum_{i-0}^{(r-1)/2} \binom{r}{2i+1} u^{r-2i-1} \left(-v^2\right)^i \equiv 2^{r-1} \lambda_1 \lambda_2 u^{r-1} v \pmod c. \end{aligned} \tag{12}$$

Further, since $2 \parallel b$, we see from (12) that $2 \nmid u$ and $2 \parallel v$.

Let (x, y, z) be a solution of (2) with $(x, y, z) \neq (2, 2, r)$. If $2 \nmid x$ and $2 \nmid y$, then we have

$$\left(\frac{-ab}{c}\right) = 1, \tag{13}$$

by (2). However, by (11) and (12), we get

(14)

$$\begin{aligned} &\left(\frac{-1}{c}\right) = 1,\ \left(\frac{a}{c}\right) = \left(\frac{2^{r-1}\lambda_1 u^r}{c}\right) = \left(\frac{u}{c}\right) = \left(\frac{c}{u}\right) = \left(\frac{u^2+v^2}{u}\right) = \left(\frac{v^2}{u}\right) = 1, \\ &\left(\frac{b}{c}\right) = \left(\frac{2^{r-1}\lambda_1\lambda_2 u^{r-1} v}{c}\right) = \left(\frac{v}{c}\right) = \left(\frac{2}{c}\right)\left(\frac{v/2}{c}\right) = \left(\frac{2}{c}\right)\left(\frac{c}{v/2}\right) = \left(\frac{2}{c}\right) = -1. \end{aligned}$$

https://doi.org/10.1017/S0004972700022334 Published online by Cambridge University Press

This implies that $(-ab/c) = -1$, a contradiction with (13). Similarly, by (14), we can prove that (2) has no solution (x, y, z) satisfying $2 \mid x$ and $2 \nmid y$. So we have $2 \mid y$. Further, if $2 \nmid x$ and $2 \mid y$, then we get $c^z = z^x + b^y \equiv 3(\mathrm{mod}\, 4)$. This is impossible. Thus, we obtain $2 \mid x$ and $2 \mid y$.

If $2 \mid x$, $2 \mid y$ and $2 \nmid z$, then $b^y = c^z - a^x \equiv 4(\mathrm{mod}\, 8)$. This implies that $y = 2$. Since $(x, y, z) \neq (2, 2, r)$, we get $x \geqslant 4$. Further, if $x = 4$, then $x > r$ and $a^4 \equiv -b^2(\mathrm{mod}\, c^z)$ by (2). Since $a^2 \equiv -b^2(\mathrm{mod}\, c^r)$ by (9), we get $a^2 \equiv 1(\mathrm{mod}\, c^r)$. It follows that $a^2 - 1 \geqslant c^r = a^2 + b^2 > a^2 - 1$, a contradiction. So we have $x \geqslant 6$ and (7) holds.

If $2 \mid x$, $2 \mid y$ and $2 \mid x$, then $(X, Y, Z) = \left(a^{x/2}, b^{y/2}, c^{z/2}\right)$ is a solution of the equation (3). Hence, by Lemma 1, we get

$$a^{x/2} = u^2 - v^2, \; b^{y/2} = 2uv, \; c^{z/2} = u^2 + v^2, \tag{15}$$

where u, v are positive integers satisfying

$$u > v, \; \gcd(u, v) = 1, \; 2 \mid uv. \tag{16}$$

Further, if $2 \mid x/2$, then from (15) and (16) we obtain $2 \nmid u$, $4 \mid v$ and $2 \mid z/2$. This implies that the equation (5) has a solution $(X, Y, Z) = \left(c^{z/4}, a^{x/4}, b^{y/2}\right)$. However, by Lemma 3, that is impossible. So we have $2 \parallel x$. Then, by (15) and (16), we get $2 \parallel u$, $2 \nmid u$, $y = 4$ and $2 \parallel x$. On the other hand, if $x = 2$ or 6, then from (2) and (9) we get $z > r$ and $a^2 + 1 \equiv 0(\mathrm{mod}\, c^r)$. This is impossible. So we have $x \geqslant 10$ and (8) holds. Thus, the lemma is proved. ∎

3. Proof of Theorem

Since $r > 1$ and c is a prime power, by (9), we have $c = p^s$ where p is an odd prime, s is a positive integer. Let (x, y, z) be a solution of (2) with $(x, y, z) \neq (2, 2, r)$. By Lemma 5, the solution satisfies either (7) or (8).

If (8) holds, then from (15) and (16) we get $u = 2u_1^2$ and $v = v_1^2$, where u_1, v_1 are positive odd integers with $\gcd(u_1, v_1) = 1$. Hence, by (15), we get

$$c^{z/2} = p^{sz/2} = 4u_1^4 + v_1^4 = \left(2u_1^2 + 2u_1v_1 + v_1^2\right)\left(2u_1^2 - 2u_1v_1 + v_1^2\right). \tag{17}$$

Since $\gcd\left(2u_1^2 + 2u_1v_1 + v_1^2,\; 2u_1^2 - 2u_1v_1 + v_1^2\right) = 1$, we see from (17) that $2u_1^2 - 2u_1v_1 + v_1^2 = u_1^2 + (u_1 - v_1)^2 = 1$. This implies that $u_1 = v_1 = 1$ and $(a, b, c) = (3, 2, 5)$. However, then (9) does not hold. Thus, (2) has no solution (x, y, z) satisfying (8).

If (7) holds, then $(X, Y, Z) = \left(a^{(x-2)/2}, 1, sz\right)$ is a solution of the equation

$$a^2X^2 + b^2Y^2 = p^Z, \; X, Y, Z, \in \mathbb{Z}, \; \gcd(X, Y) = 1, \; Z > 0. \tag{18}$$

On the other hand, we see from (9) that (18) has another solution $(X, Y, Z) = (1, 1, sr)$. Further, by the definitions of Lemma 4, the least solution of (18) is $(X_1, Y_1, Z_1) = (1, 1, sr)$. Therefore, by Lemma 4, we get

(19) $$sz = srt,\ t \in \mathbb{N},\ 2 \nmid t,\ t > 1,$$

(20) $$a^{(x-2)/2}\sqrt{a^2} + \sqrt{-b^2} = \lambda_1\big(\sqrt{a^2} + \lambda_2\sqrt{-b^2}\big)^t,\ \lambda_1, \lambda_2 \in \{-1, 1\}.$$

By (20), we get

(21) $$\begin{aligned} a^{(x-2)/2} &= \lambda_1 a \sum_{i=0}^{(t-1)/2} \binom{t}{2i} a^{t-2i-1}\big(-b^2\big)^i \\ &= \lambda_1 a \sum_{j=0}^{(t-1)/2} \binom{t}{2j+1} a^{2j}\big(-b^2\big)^{(t-1)/2-j}. \end{aligned}$$

Since $x \geqslant 6$ and $\gcd(a, b) = 1$, we find from (21) that $a \mid t$.

Let q be a prime factor of a. Further let $q^\alpha \parallel a$, $q^\beta \parallel t$ and $q^{\gamma_j} \parallel 2j+1$ for $j = 1, \ldots, (t-1)/2$. Then we have

(22) $$\gamma_j \leqslant \frac{\log(2j+1)}{\log q} \leqslant j,\ j = 1, \ldots, \frac{t-1}{2}.$$

By (22), we obtain

(23) $$\binom{t}{2j+1} a^{2j}\big(-b^2\big)^{(t-1)/2-j} = t\binom{t-1}{2j}\frac{a^{2j}}{2j+1}\big(-b^2\big)^{(t-1)/2-j} \equiv 0 \pmod{q^{\beta+1}}$$

for $j = 1, \ldots, (t-1)/2$. This implies that

(24) $$q^{\alpha+\beta} \parallel \lambda_1 a \sum_{j=0}^{(t-1)/2} \binom{t}{2j+1} a^{2j}\big(-b^2\big)^{(t-1)/2-j}.$$

The combination of (21) and (24) yields

(25) $$\beta = \left(\frac{x-4}{2}\right)\alpha.$$

Let q run through all prime factors of a. We see from (25) that

(26) $$t \geqslant a^{(x-4)/2} > 1.$$

Therefore, by (2), (7), (9), (19) and (26), we get

(27) $$a^x + b^2 = c^z = c^{rt} = \big(a^2 + b^2\big)^t > a^{2t} + b^{2t} > a^{2a^{(x-4)/2}} + b^2.$$

From (27), we obtain

(28) $$x > 2a^{(x-4)/2}.$$

However, since $x \geqslant 6$ and $a \geqslant 3$, (28) is impossible. Thus, (2) has no solution (x, y, z) satisfying (7). The theorem is proved. $\square$

References

[1] M. Laurent, M. Mignotte and Y. Nesterenko, 'Formes linéaries en deux logarithmes et déterminants d'interpolation', *J. Number Theory* **55** (1995), 285–321.

[2] M.-H. Le, 'A note on the generalized Ramanujan-Nagell equation', *J. Number Theory* **50** (1995), 193–201.

[3] M.-H. Le, 'A note on the diophantine equation $(m^3 - 3m)^x + (3m^2 - 1)^y = (m^2 + 1)^z$', *Proc. Japan Acad. Ser. A Math. Sci.* **73** (1997), 148–149.

[4] L.J. Mordell, *Diophantine equations* (Academic Press, New York, 1969).

[5] N. Terai, 'The diophantine equation $a^x + b^y = c^z$', *Proc. Japan Acad. Ser. A. Math. Sci.* **70** (1994), 22-26.

[6] N. Terai, 'The diophantine equation $a^x + b^y = c^z$ II', *Proc. Japan Acad. Ser. A. Math. Sci.* **71** (1995), 109–110.

[7] N. Terai, 'The diophantine equation $a^x + b^y = c^z$ III', *Proc. Japan Acad. Ser. A. Math. Sci.* **72** (1996), 20–22.

[8] N. Terai, 'Applications of a lower bound for linear forms in two logarithms to exponential diophantine equations' (to appear).

Department of Mathematics
Zhanjiang Normal College
Postal Code 524048
Zhanjiang, Guangdong
People's Republic of China