

On the Terai–Jeśmanowicz conjecture

ZHENFU CAO and XIAOLEI DONG (Shanghai)

Abstract. Let $a, b, c \in \mathbb{N}$ be fixed satisfying $a^2 + b^2 = c^r$ with $\gcd(a, b) = 1$ and r odd ≥ 3 . In this paper, we prove that (A) if $b \equiv 3 \pmod{4}$, $2 \parallel a$ and $b \geq 25.1a$, then the Diophantine equation (1) $a^x + b^y = c^z$ has only the positive integer solution $(x, y, z) = (2, 2, r)$; (B) if $a = |V_r|$, $b = |U_r|$, $c = m^2 + 1$, where the integers U_r, V_r satisfy $(m + \sqrt{-1})^r = V_r + U_r\sqrt{-1}$, and $b \equiv 3 \pmod{4}$, $2 \parallel a$ and b is a prime, then equation (1) has only the positive integer solution $(x, y, z) = (2, 2, r)$.

§1. Introduction

Let $\mathbb{Z}$ and $\mathbb{N}$ be the sets of integers and positive integers respectively. In [16], [17], N. TERAJ conjectured that if $a, b, c, p, q, r \in \mathbb{N}$ are fixed, and $a^p + b^q = c^r$, where $p, q, r \geq 2$, and $\gcd(a, b) = 1$, then the Diophantine equation

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

has only the solution $(x, y, z) = (p, q, r)$. In [2], we point out that the condition $\max(a, b, c) > 7$ should be added to the hypotheses of the conjecture. In fact, we see that the equation $(2^n - 1)^x + 2^y = (2^n + 1)^z$ has two solutions $(x, y, z) = (1, 1, 1)$ and $(2, n + 2, 2)$ for any $1 < n \in \mathbb{N}$. So, we suggest that the conjecture should be modified as follows.

Mathematics Subject Classification: 11D61.

Key words and phrases: exponential diophantine equation.

This project was supported by China Postdoctoral Science Foundation and the National Natural Science Foundation of China.

Conjecture. *If $a, b, c, p, q, r \in \mathbb{N}$ with $a^p + b^q = c^r$, $a, b, c, p, q, r \geq 2$ and $\gcd(a, b) = 1$, then Diophantine equation (1) has only the solution $(x, y, z) = (p, q, r)$ with $x, y, z > 1$.*

For $p = q = r = 2$ the above statement was conjectured previously by JEŚMANOWICZ [6]. We shall use the term Terai–Jeśmanowicz conjecture for the above conjecture. Some recent results on the Terai–Jeśmanowicz conjecture are as follows:

(A) TERAİ [16], LE [8] and the authors [2], [5] considered the case $p = q = 2$, $r = 3$, and for

$$(2) \quad a = m^3 - 3m, \quad b = 3m^2 - 1, \quad c = m^2 + 1,$$

where $2 \mid m \in \mathbb{N}$, they proved that

(A1) if b is an odd prime, and there is a prime l such that $m^2 - 3 \equiv 0 \pmod{l}$ and $e \equiv 0 \pmod{3}$, where e is the order of 2 modulo l , then the Terai–Jeśmanowicz conjecture holds (see [16]).

(A2) if b is an odd prime and $4 \nmid m$, then the Terai–Jeśmanowicz conjecture holds (see [8]).

(A3) if b is an odd prime, then the Terai–Jeśmanowicz conjecture holds (see [5]). And if c is a prime, then the Terai–Jeśmanowicz conjecture also holds (see [2], [5]).

(B) TERAİ [17] and the authors [2], [5] also considered the case $p = q = 2$, $r = 5$, and for

$$(3) \quad a = m|m^4 - 10m^2 + 5|, \quad b = 5m^4 - 10m^2 + 1, \quad c = m^2 + 1,$$

where $2 \mid m \in \mathbb{N}$, they proved that

(B1) if b is an odd prime and there is an odd prime l such that $ab \equiv 0 \pmod{l}$ and $e \equiv 0 \pmod{5}$, where e is the order of c modulo l , then the Terai–Jeśmanowicz conjecture holds (see [17]).

(B2) if b is an odd prime, then the Terai–Jeśmanowicz conjecture holds (see [5]). And if c is a prime, then the Terai–Jeśmanowicz conjecture holds (see [2], [5]).

(C) One of the authors [2] also proved that if $p = q = 2$, $2 \nmid r$, $c \equiv 5 \pmod{8}$, $b \equiv 3 \pmod{4}$ and c is a prime power, then the Terai–Jeśmanowicz conjecture holds. In a recent paper of LE [9], we see that Le only got a special case of the result of [2].

Recently, TERAJ [18] also considered the case $p = q = 2$, $2 \nmid r \geq 3$, he proved that if $b \equiv 3 \pmod{8}$, $2 \parallel a$, $(\frac{a}{l}) = -1$ and $b \geq 30a$, where $l > 1$ is a divisor of b and $(\frac{*}{*})$ denotes the Jacobi symbol, then the Terai-Jeśmanowicz conjecture holds.

In this paper, we prove the following further results.

Theorem 1. *Let $p = q = 2$ and r odd ≥ 3 . Suppose that $b \equiv 3 \pmod{4}$, $2 \parallel a$ and $b \geq 25.1a$, then the Terai-Jeśmanowicz conjecture holds.*

This is an improvement of Theorem 1 of TERAJ [18].

From Lemma 1 of [16], we know that $a = n(3m^2 - n^2)$, $b = m \times (m^2 - 3n^2)$, $c = m^2 + n^2$ are all primitive solutions of $a^2 + b^2 = c^3$, where $m, n \in \mathbb{N}$ with $\gcd(m, n) = 1$.

Corollary to Theorem 1. *Suppose that $a = n(3m^2 - n^2)$, $b = m \times (m^2 - 3n^2)$, $c = m^2 + n^2$, where $m, n \in \mathbb{N}$ with $\gcd(m, n) = 1$. If $m \equiv 3 \pmod{4}$, $2 \parallel n$ and $m > 71.68n$, then equation (1) has only the solution $(x, y, z) = (2, 2, 3)$.*

Theorem 2. *Let $m, r \in \mathbb{N}$ with $2 \nmid r$, $r > 1$, define the integers U_r , V_r by $(m + \sqrt{-1})^r = V_r + U_r\sqrt{-1}$. If $a = |V_r|$, $b = |U_r|$, $c = m^2 + 1$ and if $m \equiv 2 \pmod{4}$, $b \equiv 3 \pmod{4}$ and b is a prime, then equation (1) has only the solution $(x, y, z) = (2, 2, r)$.*

In Theorem 2, taking $r = 3$, we obtain the result of LE [8]. If $r = 7$, then we have from Theorem 2 that

Corollary to Theorem 2. *Let*

$$\begin{aligned} a &= m |m^6 - 21m^4 + 35m^2 - 7|, \\ b &= 7m^6 - 35m^4 + 21m^2 - 1, \quad c = m^2 + 1, \end{aligned}$$

where $2 < m \in \mathbb{N}$. If $m \equiv 2 \pmod{4}$ and b is a prime, then equation (1) has only the solution $(x, y, z) = (2, 2, 7)$.

In addition, we have also the following two results.

Theorem 3. *If $m \in \mathbb{N}$ with $m > 1$, then the Diophantine equation*

$$(4) \quad A^{2m} + B^2 = C^4, \quad A, B, C \in \mathbb{Z}, \quad \gcd(A, B) = 1, \quad 2 \mid A$$

has no solution with $AB \neq 0$.

Theorem 4. *If $m \in \mathbb{N}$ with $m > 3$, then the Diophantine equation*

$$(5) \quad A^{2m} + B^4 = C^2, \quad A, B, C \in \mathbb{Z}, \gcd(A, B) = 1, 2 \mid B$$

has no solution with $AB \neq 0$.

Clearly, Theorems 3 and 4 can be applied to Terai–Jesmanowicz conjecture.

§2. Proof of Theorem 1 and its corollary

We will use the following lemmas to prove Theorem 1 and its corollary.

Lemma 1. *Let $a, b, c, p, q, r \in \mathbb{N}$ satisfy the hypotheses of the Terai–Jesmanowicz conjecture. If $p = q = 2$, $2 \nmid r$, $c \equiv 5 \pmod{8}$ and $b \equiv 3 \pmod{4}$, then $2 \mid x$, $2 \mid y$ in equation (1).*

PROOF. See [2]. □

Lemma 2. *Let $a, b, c \in \mathbb{N}$ be fixed satisfying $a^2 + b^2 = c^r$ with $\gcd(a, b) = 1$ and r odd ≥ 3 . Suppose that $b \equiv 3 \pmod{4}$, $2 \parallel a$. If equation (1) has solutions (x, y, z) , then $x = 2$, $2 \mid y$, $2 \nmid z$.*

PROOF. Lemma 2 uses Theorem 3 and 4, whose proofs will be given in the last Section.

From $b \equiv 3 \pmod{4}$, $2 \parallel a$, $a^2 + b^2 = c^r$ and r odd, we see that $c \equiv 5 \pmod{8}$. So, if equation (1) has solutions (x, y, z) then we get from Lemma 1 that $2 \mid x$, $2 \mid y$.

Case (i): z is odd. Then, by arguing mod 8, we have from (1) that $a^x + 1 \equiv 5 \pmod{8}$, and so $x = 2$ since $2 \parallel a$.

Case (ii): z is even. We can assume that $x = 2X$, $y = 2Y$, $z = 2Z$, where $X, Y, Z \in \mathbb{N}$. Then from (1), we have

$$a^X = 2uv, \quad b^Y = u^2 - v^2, \quad c^Z = u^2 + v^2,$$

where $u, v \in \mathbb{N}$ with $\gcd(u, v) = 1$, $2 \nmid u + v$.

Since $2 \parallel a$, we have $X > 1$. If $X > 2$, then $uv \equiv 0 \pmod{4}$ and so $c^Z \equiv 1 \pmod{8}$, we get $2 \mid Z$. Then equation (1) leads to $a^{2X} + (b^Y)^2 = (c^{Z/2})^4$, which is impossible by Theorem 3. Hence $X = 2$, and by Theorem 4, we get $Y \leq 3$.

If $Y = 1$, then from (1), we have $a^4 + b^2 = c^{2Z}$. So, we get

$$a^2(a^2 - 1) = (a^4 + b^2) - (a^2 + b^2) = c^{2Z} - c^r = c^r(c^{2Z-r} - 1).$$

Hence, we see that $c^r \mid a^2 - 1$ since $\gcd(a, c) = 1$. And so

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

a contradiction.

If $Y = 2$, then (1) gives $a^4 + b^4 = c^{2Z}$, which is impossible (see [14], p. 37).

If $Y = 3$, then (1) gives $a^4 + b^6 = c^{2Z}$. So, we get

$$(6) \quad b^2(2a^2 + b^2 - b^4) = (a^2 + b^2)^2 - (a^4 + b^6) = c^{2r} - c^{2Z}.$$

Clearly, $r \neq Z$. Hence, if $r > Z$ then we see from (6) that $b^2 \mid c^{2r-2Z} - 1$. So, (6) gives

$$2a^2 + b^2 - b^4 = c^{2Z} \cdot \frac{c^{2r-2Z} - 1}{b^2} \geq c^{2Z} = a^4 + b^6$$

which is impossible. If $r < Z$, then (6) gives

$$b^4 - 2a^2 - b^2 = c^{2r} \cdot \frac{c^{2Z-2r} - 1}{b^2} \geq c^{2r} > a^4 + b^4$$

which is also impossible. The proof is complete. $\square$

Lemma 3. *Let $a, b, c, p, q, r \in \mathbb{N}$ satisfy the hypotheses of the Terai-Jeśmanowicz conjecture, $b > a > 1$, $c \geq 3$ and $q \geq p$. Let n be a given positive integer with $p \leq n \leq 1722$. If $b \geq \mu a^{p/q}$ and the equation*

$$a^n + b^y = c^z, \quad y, z \in \mathbb{N}$$

has solutions y, z with $(y, n) \neq (q, p)$, then $y < n + q - p$, where

$$\begin{aligned} \mu &= \left\{ \exp \left(\frac{\delta}{\frac{n}{\log c} + M} \right) - 1 \right\}^{-1/q}, \\ M &= 1060.29 + 105.53 \left(\frac{1}{\log b} + \frac{1}{\log c} \right) + 765.39 (\log b \log c)^{-1/2} \\ &\quad + \frac{\log 81 + 12.26}{\log b \log c} + \frac{\log(\log b \log c)}{\log b \log c} \end{aligned}$$

and $\delta = 1$ or 2 according as $ry - qz$ is odd or even.

PROOF. Using a corollary to a theorem of Laurent–Mignotte–Nesterenko [12], the lemma follows from the proof of main theorem of TERAJ [18]. $\square$

A Lucas pair (resp. a Lehmer pair) is a pair (α, β) of algebraic integers such that $\alpha + \beta$ and $\alpha\beta$ (resp. $(\alpha + \beta)^2$ and $\alpha\beta$) are non-zero coprime rational integers and α/β is not a root of unity. For a given Lucas pair (α, β) , one defines the corresponding sequence of Lucas numbers by

$$u_n = u_n(\alpha, \beta) = \frac{\alpha^n - \beta^n}{\alpha - \beta} \quad (n = 0, 1, 2, \dots).$$

For a given Lehmer pair (α, β) , one defines the corresponding sequence of Lehmer numbers by

$$\tilde{u}_n = \tilde{u}_n(\alpha, \beta) = \begin{cases} \frac{\alpha^n - \beta^n}{\alpha - \beta} & \text{if } n \text{ is odd,} \\ \frac{\alpha^n - \beta^n}{\alpha^2 - \beta^2} & \text{if } n \text{ is even.} \end{cases}$$

It is clear that every Lucas pair (α, β) is also a Lehmer pair, and

$$u_n = \begin{cases} \tilde{u}_n & \text{if } n \text{ is odd,} \\ (\alpha + \beta)\tilde{u}_n & \text{if } n \text{ is even.} \end{cases}$$

Let (α, β) be a Lucas (resp. Lehmer) pair. The prime number p is a primitive divisor of the Lucas (resp. Lehmer) number $u_n(\alpha, \beta)$ (resp. $\tilde{u}_n(\alpha, \beta)$) if p divides u_n but does not divide $(\alpha - \beta)^2 u_1 \cdots u_{n-1}$ (resp. if p divides $\tilde{u}_n$ but does not divide $(\alpha^2 - \beta^2)^2 \tilde{u}_1 \cdots \tilde{u}_{n-1}$). Recently, Y. BILU, G. HANROT and P. VOUTIER [1] proved the following

Lemma 4. *For any integer $n > 30$, every n -th term of any Lucas or Lehmer sequence has a primitive divisor.*

In [1], for any positive integer $n \leq 30$, all Lucas sequences and all Lehmer sequences whose n -th term has no primitive divisor are explicitly determined. See Tables 1–4 of [1].

Lemma 5. *If $2 \nmid r$ and $r > 1$, then all solutions (X, Y, Z) of the equation*

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

are given by

$$X + Y\sqrt{-1} = \lambda_1(X_1 + \lambda_2 Y_1 \sqrt{-1})^r, \quad Z = X_1^2 + Y_1^2,$$

where $\lambda_1, \lambda_2 \in \{-1, 1\}$, $X_1, Y_1 \in \mathbb{N}$ and $\gcd(X_1, Y_1) = 1$.

Lemma 5 follows directly from a theorem in book of MORDELL [13] pp. 122–123.

PROOF of Theorem 1. From the theorem of [2], we see that if c is a prime power, then our theorem holds. Hence, we may suppose that $c \geq 85$. It follows from Lemma 2 that $x = 2$, $2 \mid y$ and $2 \nmid z$. In Lemma 3, let $p = q = 2$, $n = 2$ and $\delta = 2$. Then by Lemma 3, if equation (1) has solutions with $(y, n) \neq (2, 2)$, then $y < n + q - p = 2$ under the condition

$$(7) \quad b \geq \left\{ \exp \left(\frac{2}{\frac{n}{\log c} + M} \right) - 1 \right\}^{-1/2} a.$$

Now, we prove that

$$(8) \quad b \geq 251.$$

Using Lemma 5, from $a^2 + b^2 = c^r$, $\gcd(a, b) = 1$, $2 \mid a$ and r odd ≥ 3 , we get

$$(9) \quad b + a\sqrt{-1} = \lambda_1(u + \lambda_2 v \sqrt{-1})^r, \quad c = u^2 + v^2,$$

where $\lambda_1, \lambda_2 \in \{-1, 1\}$, $u, v \in \mathbb{N}$ with $\gcd(u, v) = 1$ and $2 \nmid u + v$. Let $\alpha = u + v\sqrt{-1}$, $\beta = u - v\sqrt{-1}$. Then (9) gives

$$(10) \quad a = \left| \frac{\alpha^r - \beta^r}{\alpha - \beta} \right| v.$$

Since $2 \nmid \frac{\alpha^r - \beta^r}{\alpha - \beta}$ and $2 \parallel a$, (10) implies that $2 \parallel v$. By Lemma 4 and Tables 1 and 3 of [1], we see that $\frac{\alpha^r - \beta^r}{\alpha - \beta}$ has a primitive divisor. Also, if $3 \nmid v$ and $3 \mid \frac{\alpha^r - \beta^r}{\alpha - \beta}$, then from $b^2 + a^2 = c^r$ we see that $c = u^2 + v^2 \equiv 1 \pmod{3}$ and so $3 \mid u$. On the other hand, from $3 \mid \frac{\alpha^r - \beta^r}{\alpha - \beta}$ we know that $3 \nmid u$, a contradiction. If $3 \mid v$, then $a \geq 18$, $b > 251$, i.e. (8) holds. If $3 \nmid \frac{\alpha^r - \beta^r}{\alpha - \beta}$, then from (10), we get $a \geq 10$ and so $b \geq 251$, i.e. (8) also holds.

From $b \geq 251$ and $c \geq 85$, we have $\frac{n}{\log c} < 0.2251n$ and

$$\begin{aligned} M &= 1060.29 + 105.53 \left(\frac{1}{\log b} + \frac{1}{\log c} \right) + 765.39 (\log b \log c)^{-1/2} \\ &\quad + \frac{\log 81 + 12.26}{\log b \log c} + \frac{\log(\log b \log c)}{\log b \log c} < 1258.434. \end{aligned}$$

Therefore, we get that

$$\begin{aligned} \left\{ \exp \left(\frac{2}{\frac{n}{\log c} + M} \right) - 1 \right\}^{-1/2} &< \left\{ \exp \left(\frac{2}{0.2251 \cdot 2 + 1258.434} \right) - 1 \right\}^{-1/2} \\ &< 25.1. \end{aligned}$$

From this, we have $b \geq 25.1a > \left\{ \exp \left(\frac{2}{\frac{n}{\log c} + M} \right) - 1 \right\}^{-1/2} a$, i.e. (7) holds.

Hence, $y < 2$, but which is impossible since $2 \mid y$.

Thus, $y = 2$, and from $c^z = a^x + b^y = a^2 + b^2 = c^r$, we get $z = r$.

This proves Theorem 1. $\square$

PROOF of Corollary to Theorem 1. Clearly, $a^2 + b^2 = c^3$ and $b \equiv 3 \pmod{4}$, $2 \parallel a$. Notice that $m > 71.68n$. We get

$$23.88 \left(3 + \frac{8}{\left(\frac{m}{n} \right)^2 - 3} \right) < 71.68 < \frac{m}{n}.$$

It implies that $m(m^2 - 3n^2) > 23.88n(3m^2 - n^2)$, that is $b > 23.88a$. Since $n \geq 2$, $m > 71.68n > 143$, i.e. $m \geq 145$. We get

$$a = n^3 \left(3 \left(\frac{m}{n} \right)^2 - 1 \right) > 8(3 \cdot 71.68^2 - 1) = 123304.53 \dots,$$

i.e. $a \geq 123306$. Hence,

$$\begin{aligned} (11) \quad b &> 23.88 \cdot 123306 > 2944547 \text{ (i.e. } b \geq 2944549), \\ c &\geq 145^2 + 2^2 = 21029. \end{aligned}$$

By the proof of Theorem 1, it suffices to prove

$$(12) \quad \left\{ \exp \left(\frac{2}{\frac{n}{\log c} + M} \right) - 1 \right\}^{-1/2} < 23.88.$$

From (11), we have $\frac{n}{\log c} < 0.1004656n$ and

$$M = 1060.29 + 105.53 \left(\frac{1}{\log b} + \frac{1}{\log c} \right) + 765.39(\log b \log c)^{-1/2} \\ + \frac{\log 81 + 12.26}{\log b \log c} + \frac{\log(\log b \log c)}{\log b \log c} < 1141.003342.$$

From this, we easily get that (12) holds.

The corollary is proved. $\square$

Remark 1. Using TERAİ's method (see [18]), we can prove that if $a = 2(3m^2 - 4)$, $b = m(m^2 - 12)$, $c = m^2 + 4$, where $m \in \mathbb{N}$ with $m \equiv 3 \pmod{4}$ and $m > 3$, then equation (1) has only the solution $(x, y, z) = (2, 2, 3)$.

§3. Proof of Theorem 2

We need Lemma 2, Lemma 5 and the following result.

Let u_n be Lucas sequence, i.e. $u_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}$, where α, β are two roots of the equation

$$x^2 - Px + Q = 0, \quad P, Q \in \mathbb{Z}, \quad P > 0, \quad \gcd(P, Q) = 1.$$

It is well known fact that

Lemma 6. *If m, n are odd, then $\gcd(u_m, u_n) = u_{\gcd(m, n)}$.*

PROOF. For example, see D. H. LEHMER [10]. $\square$

PROOF of Theorem 2. It is clear that $2 \parallel a$ when $m \equiv 2 \pmod{4}$. Then from Lemma 2, we get $x = 2$, $y = 2y_1$ and $2 \nmid z$, where $y_1 \in \mathbb{N}$. If $y_1 = 1$, then we have from (1) that $z = r$, that is, Theorem 2 holds. Otherwise, we assume that $y_1 > 1$.

By Lemma 5, we have from (1) that

$$(13) \quad a + b^{y_1} \sqrt{-1} = \lambda_1 (X + \lambda_2 Y \sqrt{-1})^z, \quad c = X^2 + Y^2,$$

where $\lambda_1, \lambda_2 \in \{-1, 1\}$, $X, Y \in \mathbb{N}$ and $\gcd(X, Y) = 1$. It follows from (13) that

$$(14) \quad \lambda_1 \lambda_2 b^{y_1} = Y \left(\binom{z}{1} X^{z-1} - \binom{z}{3} X^{z-3} Y^2 + \cdots + (-1)^{\frac{z-1}{2}} \binom{z}{z} Y^{z-1} \right).$$

Clearly, (14) gives that $Y = b^l$, $0 \leq l \leq y_1$. If $l > 0$, then $m^2 + 1 = c = X^2 + Y^2 \geq b^2 + 1$ and so

$$(15) \quad m \geq b.$$

On the other hand, let

$$A = \binom{r}{1} m^{r-3} - \binom{r}{3} m^{r-5} + \cdots + (-1)^{\frac{r-3}{2}} \binom{r}{r-2}.$$

Then $b = |U_r| = |m^2 A + (-1)^{\frac{r-1}{2}}|$. Therefore, by b is a prime, we see that $A \neq 0$. It implies that

$$b = |U_r| = |m^2 A + (-1)^{\frac{r-1}{2}}| \geq m^2 |A| - 1 \geq m^2 - 1 > m,$$

which contradicts (15). Therefore $l = 0$, that is, $Y = 1$. From $c = m^2 + 1 = X^2 + 1$, we get that $X = m$. Now, we get from (14) that

$$(16) \quad \lambda_1 \lambda_2 b^{y_1} = \frac{\alpha^z - \beta^z}{\alpha - \beta} = U_z,$$

where $\alpha = m + \sqrt{-1}$, $\beta = m - \sqrt{-1}$ are two roots of the equation $x^2 - 2mx + (m^2 + 1) = 0$. By Lemma 6, we get that $\gcd(b, U_z) = \gcd(U_r, U_z) = U_{\gcd(r, z)}$. Since $b = |U_r|$ is a prime, $U_r \mid U_z$, we get $r \mid z$. Let $z = rz_1$, $z_1 \in \mathbb{N}$. We have

$$V_{rz_1} + U_{rz_1} \sqrt{-1} = (m + \sqrt{-1})^{rz_1} = (V_r + U_r \sqrt{-1})^{z_1}.$$

It follows from (16) that

$$(17) \quad b^{y_1-1} = \left| \frac{U_{rz_1}}{U_r} \right| = \left| \binom{z_1}{1} V_r^{z_1-1} - \binom{z_1}{3} V_r^{z_1-3} U_r^2 + \cdots + (-1)^{\frac{z_1-1}{2}} \binom{z_1}{z_1} U_r^{z_1-1} \right|.$$

Clearly, $b \mid z_1$. Let $b^{l_j} \parallel \binom{z_1}{2j+1} V_r^{z_1-(2j+1)} U_r^{2j}$, $0 \leq j \leq \frac{z_1-1}{2}$ and let $b^{t_j} \parallel 2j+1$. Then we have $2j - t_j > 0$ for $j > 0$. So from

$$\binom{z_1}{2j+1} V_r^{z_1-(2j+1)} U_r^{2j} = \frac{z_1}{2j+1} \binom{z_1-1}{2j} V_r^{z_1-(2j+1)} b^{2j}$$

we see that $l_0 < l_0 + 2j - t_j \leq l_j$ for $j > 0$. Hence, we get from (17) that $b^{y_1-1} \mid z_1$, and so $z_1 \geq b^{y_1-1}$. It follows from (1) that

$$a^2 + b^{2y_1} = c^{rz_1} = (a^2 + b^2)^{z_1} \geq (a^2 + b^2)^{b^{y_1-1}} > a^2 + b^{2y_1},$$

a contradiction.

This proves Theorem 2. $\square$

Remark 2. In the proof of Theorem 2, not using Lemma 2, we can also get that $x = 2$, $y = 2y_1$ and $2 \nmid z$. In fact, using some results on the equations $x^2 - y^n = 1$, $x^2 - 2y^n = -1$ and $x^{2n} - 2y^2 = -1$ (see CHAO KO [7], LJUNGGREN [11], STÖRMER [15] and ZHENFU CAO [3]), we can get an elementary proof of it.

§4. Proof of Theorems 3 and 4

Proof of Theorems 3 and 4 need two important results on the Diophantine equations

$$(18) \quad x^p + 2y^p + z^p = 0, \quad x, y, z \in \mathbb{Z}, \quad xyz \neq 0, \quad p \in \mathbb{P},$$

and

$$(19) \quad x^n + y^n = z^2, \quad x, y, z \in \mathbb{Z}, \quad xyz \neq 0, \quad n \in \mathbb{N}.$$

Lemma 7. *Equation (18) has no solution with $x \neq z$.*

Lemma 8. *If $n \geq 4$, then equation (19) has no solution.*

For the proofs of Lemmas 7 and 8, see DARMON and MEREL [4]. Now, using Lemma 7, we can obtain the proof of Theorem 3.

PROOF of Theorem 3. Suppose that equation (4) has a solution with $AB \neq 0$. From RIBENBOIM [14], p. 38, we can assume that $2 \nmid m$. Therefore, we get from (4) that

$$(20) \quad |A|^m = 2uv, \quad C^2 = u^2 + v^2,$$

where $u, v \in \mathbb{N}$ with $\gcd(u, v) = 1$, $2 \nmid u + v$. Without loss of generality, we may assume that $2 \mid u$, $2 \nmid v$. Then from the second equality of (20), we get

$$(21) \quad u = 2u_1v_1, \quad v = u_1^2 - v_1^2,$$

where $u_1, v_1 \in \mathbb{N}$ with $\gcd(u_1, v_1) = 1, 2 \nmid u_1 + v_1$. From the first equality of (20), we have

$$(22) \quad u = 2^{m-1}A_1^m, \quad v = A_2^m, \quad |A| = 2A_1A_2,$$

where $A_1, A_2 \in \mathbb{N}$ with $\gcd(A_1, A_2) = 1$. Hence, we get from (21) and (22) that

$$(23) \quad u_1v_1 = 2^{m-2}A_1^m, \quad u_1^2 - v_1^2 = A_2^m.$$

Clearly, the second equality of (23) implies

$$u_1 + v_1 = A_3^m, \quad u_1 - v_1 = A_4^m, \quad A_2 = A_3A_4,$$

and so

$$(24) \quad 2u_1 = A_3^m + A_4^m, \quad 2v_1 = A_3^m - A_4^m,$$

where $A_3, A_4 \in \mathbb{N}$ with $\gcd(A_3, A_4) = 1$. From the first equality of (23), we see that $u_1 = A_5^m$ or $v_1 = A_5^m$. By Lemma 7, we know that (24) gives $A_3 = A_4$ and so $v_1 = 0$, which is impossible since $v_1 \in \mathbb{N}$. The theorem is proved. $\square$

Using similar method and Lemma 8, we easily prove that Theorem 4 holds.

Acknowledgements. The authors would like to thank the referee for his valuable suggestions.

References

- [1] Y. BILU, G. HANROT and P. VOUTIER (with an appendix by M. Mignotte), Existence of primitive divisors of Lucas and Lehmer numbers, *J. reine angew. Math.* (to appear).
- [2] ZHENFU CAO, A note on the Diophantine equation $a^x + b^y = c^z$, *Acta Arith.* **91** no. 1 (1999), 85–93.
- [3] ZHENFU CAO, On the Diophantine equation $x^{2n} - Dy^2 = 1$, *Proc. Amer. Math. Soc.* **98** (1986), 11–16.
- [4] H. DARMON and L. MEREL, Winding quotients and some Variants of Fermat's Last Theorem, *J. reine angew. Math.* **490** (1997), 81–100.
- [5] XIAOLEI DONG and ZHENFU CAO, The Terai–Jeśmanowicz conjecture on the equation $a^x + b^y = c^z$, *Chinese Ann. Math. Ser. A* **21** no. 6 (2000), 709–714.
- [6] L. JEŚMANOWICZ, Some remarks on Pythagorean numbers, *Wiakom. Mat. ser. 2*, **1**(2) (1956), 196–202.

- [7] C. KO, On the Diophantine equation $x^2 = y^n + 1$, $xy \neq 0$, *Sci. Sinica* **14** (1965), 457–460.
- [8] M. 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** no. 7 (1997), 148–149.
- [9] M. LE, On Terai's conjecture concerning Pythagorean numbers, *Bull. Austral. Math. Soc.* **61** (2000), 329–334.
- [10] D. H. LEHMER, An extended theory of Lucas' functions, *Ann. Math.* **31** (1931), 419–438.
- [11] W. LJUNGGREN, Zur Theorie der Gleichung $x^2 + 1 = Dy^4$, *Avh. Norske Vid. Akad. Oslo* **5** (1942), 1–27.
- [12] M. MIGNOTTE, A corollary to a theorem of Laurent–Mignotte–Nesterenko, *Acta Arith.* **86** (1998), 101–111.
- [13] L. J. MORDELL, Diophantine equations, *Academic Press*, 1969.
- [14] P. RIBENBOIM, 13 Lectures on Fermat's Last Theorem, *Springer*, 1979.
- [15] C. STÖRMER, L'équation $m \arctan \frac{1}{x} + n \arctan \frac{1}{y} = k \frac{\pi}{4}$, *Bull. Soc. Math. France* **27** (1899), 160–170.
- [16] N. TERAI, The Diophantine equation $a^x + b^y = c^z$, *Proc. Japan Acad. Ser. A Math. Sci.* **70** (1994), 22–26.
- [17] N. TERAI, The Diophantine equation $a^x + b^y = c^z$ II., *Proc. Japan Acad. Ser. A Math. Sci.* **71** (1995), 109–110.
- [18] N. TERAI, Applications of a lower bound for linear forms in two logarithms to exponential Diophantine equations, *Acta Arith.* **90** no. 1 (1999), 17–35.

ZHENFU CAO
 DEPARTMENT OF COMPUTER SCIENCE
 SHANGHAI JIAO TONG UNIVERSITY
 SHANGHAI 200030
 P.R. CHINA

E-mail: zfciao@cs.sjtu.edu.cn

XIAOLEI DONG
 DEPARTMENT OF COMPUTER SCIENCE
 SHANGHAI JIAO TONG UNIVERSITY
 SHANGHAI 200030
 P.R. CHINA

E-mail: xldong@mail.sjtu.edu.cn

(Received November 30, 2000; revised May 2, 2002)