ACTA ARITHMETICA
110.2 (2003)

An application of a lower bound for linear forms in two logarithms to the Terai–Jeśmanowicz conjecture

by

Zhenfu Cao and Xiaolei Dong (Shanghai)

1. Introduction. Let $\mathbb{Z}$ and $\mathbb{N}$ be the sets of integers and positive integers respectively. The Terai–Jeśmanowicz conjecture is stated as follows (see [CD]):

Conjecture. *For given coprime integers $a, b, c > 1$, the Diophantine equation*

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

has at most one solution in integers $x, y, z > 1$.

It is known (see Lemma 14) that if a, b, c satisfy $a^2 + b^2 = c^3$, then there exist integers m, n such that $a = m^3 - 3mn^2$, $b = 3m^2n - n^3$, $c = m^2 + n^2$. A similar result holds if $a^2 + b^2 = c^5$. In this paper we consider the case $n = 1$.

(A) Suppose

$$a = m^3 - 3m, \quad b = 3m^2 - 1, \quad c = m^2 + 1, \tag{2}$$

where $2 \mid m \in \mathbb{N}$. It has been proved that the Terai–Jeśmanowicz conjecture holds in the following cases:

(A.1) 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 (see [T1]);

(A.2) if b is an odd prime and $4 \nmid m$ (see [L1]);

(A.3) if b is an odd prime (see [DC]) and if c is a prime (see [C1] and [DC]).

2000 *Mathematics Subject Classification*: Primary 11D61.

Key words and phrases: exponential Diophantine equation, Terai–Jeśmanowicz conjecture, linear forms in two logarithms, lower bound.

This project was supported by China Postdoctoral Science Foundation and the National Natural Science Foundation of China under Grant No. 60072018 and No. 60225007.

(B) Suppose

$$a = m|m^4 - 10m^2 + 5|, \quad b = 5m^4 - 10m^2 + 1, \quad c = m^2 + 1, \tag{3}$$

where $2 \mid m \in \mathbb{N}$. It has been proved that the Terai–Jeśmanowicz conjecture holds in the following cases:

(B.1) 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 (see [T2]);

(B.2) if b is an odd prime (see [DC]) and if c is a prime (see [C1] and [DC]).

(C) Suppose that the positive integers a, b, c satisfy $a^2 + b^2 = c^r$, where $2 \nmid r \geq 3$. It has been proved that the Terai–Jeśmanowicz conjecture holds in the following cases:

(C.1) if $c \equiv 5 \pmod 8, b \equiv 3 \pmod 4$ and c is a prime power (see [C1]; in a recent paper [L2], Le only got a special case of the result of [C1]);

(C.2) if $b \equiv 3 \pmod 8, 2 \parallel a, \left(\frac{a}{l}\right) = -1$ and $b \geq 30a$, where $l > 1$ is a divisor of b and $\left(\frac{*}{*}\right)$ denotes the Jacobi symbol (see [T3]; recently, in [CD] we improved the result of Terai [T3], by proving that if $b \equiv 3 \pmod 4, 2 \parallel a$ and $b \geq 25.1a$, then the Terai–Jeśmanowicz conjecture holds).

In this paper, using a lower bound for linear forms in two logarithms and some recent results on Diophantine equations, we prove the following further results.

THEOREM 1. *For a, b, c as in* (2) *and* (3), *the Terai–Jeśmanowicz conjecture holds. That is, if $m \in \mathbb{N}$ with $2 \mid m$, then the equation*

$$(m^3 - 3m)^x + (3m^2 - 1)^y = (m^2 + 1)^z \tag{4}$$

has only the solution $(x, y, z) = (2, 2, 3)$, and if $m \in \mathbb{N}$ with $2 \mid m$, then the equation

$$(m|m^4 - 10m^2 + 5|)^x + (5m^4 - 10m^2 + 1)^y = (m^2 + 1)^z \tag{5}$$

has only the solution $(x, y, z) = (2, 2, 5)$.

THEOREM 2. *Let $m, r \in \mathbb{N}$ with $2 \mid m$, $2 \nmid r$, $r > 5$. Define the integers U_r, V_r by $(m + \sqrt{-1})^r = V_r + U_r\sqrt{-1}$. If $a = |V_r|$, $b = |U_r|$, $c = m^2 + 1$ with $m \equiv 2 \pmod 4$, $b \equiv 3 \pmod 4$, and if $r < m/\sqrt{825 \log(m^2 + 1) - 1}$ and $m \geq 200$, then equation* (1) *has only the solution $(x, y, z) = (2, 2, r)$.*

REMARK. In [CD], we also proved that Theorem 2 holds when "$r < \frac{m}{\sqrt{825 \log(m^2+1)-1}}$ and $m \geq 200$" is replaced by "b is a prime". In addition, it is easy to check that for every odd $r > 5$, if $m > 80r\sqrt{\log r}$, then

$$\frac{m}{\sqrt{825\log(m^2+1)-1}} > \frac{80r\sqrt{\log r}}{\sqrt{825\log(80^2r^2\log r+1)-1}}$$
$$> r\sqrt{\frac{6400\log r}{825\log(2\cdot 80^2r^2\log r)}} > r.$$

Hence, Theorem 2 also holds when "$r < \frac{m}{\sqrt{825\log(m^2+1)-1}}$ and $m \geq 200$" is replaced by "$m > 80r\sqrt{\log r}$".

In the course of the proofs we derive some results on Diophantine equations which may be of independent interest. Lemma 7 implies that the equation $x^5+y^5 = 12z^2$ has no integer solutions with x and y coprime and $z \neq 0$. Lemma 10 says that for every integer $k > 1$ the equation $x^{2k} + y^4 = z^2$ has no solutions in positive coprime integers x, y, z.

2. A lower bound for linear forms in two logarithms and its applications

LEMMA 1. *Let* $\Lambda = X\log A - Y\log B$, *where* $X, Y, A, B \in \mathbb{N}$ *satisfy* $\min\{A, B\} > 4$. *If* $\Lambda \neq 0$, *then*

$$\begin{aligned}\log|\Lambda| \geq\ & -15.41761(h+1.677)^2\log A\log B\\ & -9.9(h+1.677)(\log A+\log B)\\ & -22.2118(h+1.59)^{3/2}(\log A\log B)^{1/2}\\ & -\log((h+1.59)^2\log A\log B)-2h-5.424,\end{aligned} \tag{6}$$

where

$$h = \max\left\{\log\left(\frac{Y}{\log A}+\frac{X}{\log B}\right)+0.17, 7.2\right\}.$$

Proof. In a result of Mignotte [M] (see Lemma 1 of Terai [T3]), just as in [T3, pp. 19–20], put $\varrho = 4.9$, $\lambda = \log\varrho$,

$$a_1 = (\varrho-1)\log A + 2\log A = (\varrho+1)\log A > \lambda,$$
$$a_2 = (\varrho-1)\log B + 2\log B = (\varrho+1)\log B > \lambda,$$

$C = 4.5$, $K_0 = 177$ and $f(K_0) = 1.2879$. Since

$$\log\left(\frac{b_1}{a_2}+\frac{b_2}{a_1}\right) = \log\left(\frac{X}{\log B}+\frac{Y}{\log A}\right)-\log(\varrho+1),$$

we can also take

$$h = \max\left\{\log\left(\frac{Y}{\log A}+\frac{X}{\log B}\right)+0.17, 7.2\right\}.$$

Hence, Lemma 1 of [T3] proves (6). ∎

LEMMA 2. *Suppose that* $\min(b,c) \geq 200^2$ *and* $b > a^{2/n}$, *where* $n \in \mathbb{N}$ *and* $n \leq 422$. *If equation* (1) *has a solution with* $x = 2$, *then*

$$y < 1650 \log c.$$

Proof. Let $\Lambda = z \log c - y \log b$. By Lemma 1, we obtain

$$\begin{aligned}(7)\qquad \log|\Lambda| \geq\ & -15.41761(h+1.677)^2 \log c \log b \\ & -9.9(h+1.677)(\log c + \log b) \\ & -22.2118(h+1.59)^{3/2}(\log c \log b)^{1/2} \\ & -\log((h+1.59)^2 \log c \log b) - 2h - 5.424,\end{aligned}$$

where

$$h = \max\left\{\log\left(\frac{y}{\log c} + \frac{z}{\log b}\right) + 0.17, 7.2\right\}.$$

On the other hand, if equation (1) has solution with $x = 2$, then

$$(8)\qquad z \log c = \log(b^y + a^2) = y \log b + \log\left(1 + \frac{a^2}{b^y}\right) < y \log b + \frac{a^2}{b^y}.$$

From (8), we see that

$$(9)\qquad \log|\Lambda| < 2 \log a - y \log b.$$

Hence, from (7) and (9), we get

$$\begin{aligned}(10)\qquad \frac{y}{\log c} <\ & \frac{2 \log a}{\log b \log c} + 15.41761(h+1.677)^2 \\ & + 9.9(h+1.677)\left(\frac{1}{\log b} + \frac{1}{\log c}\right) \\ & + \frac{22.2118(h+1.59)^{3/2}}{(\log b \log c)^{1/2}} + \frac{\log((h+1.59)^2 \log b \log c)}{\log b \log c} \\ & + \frac{2h + 5.424}{\log b \log c}.\end{aligned}$$

If $h = 7.2$, then $\log\left(\frac{y}{\log c} + \frac{z}{\log b}\right) \leq 7.03$. Since $c^z > b^y$, we get

$$\frac{2y}{\log c} < \frac{y}{\log c} + \frac{z}{\log b} \leq e^{7.03} = 1130.03061018\ldots$$

So, the assertion holds. If $h = \log\left(\frac{y}{\log c} + \frac{z}{\log b}\right) + 0.17$, since $n \leq 422$ we can suppose that $y \geq n$, then by (8), $b^n > a^2$ and $\min(b,c) \geq 200^2$, we obtain

$$\begin{aligned}(11)\qquad h =\ & \log\left(\frac{y}{\log c} + \frac{z}{\log b}\right) + 0.17 < \log\left(\frac{2y}{\log c} + \frac{a^2}{b^y \log b \log c}\right) + 0.17 \\ <\ & \log\left(\frac{2y}{\log c} + \frac{1}{\log b \log c}\right) + 0.17 < \log\left(\frac{2y}{\log c} + 0.009\right) + 0.17,\end{aligned}$$

and we have $\frac{2\log a}{\log b\log c} < \frac{n}{\log c} < 39.824$. So, from (10) and (11) we get $y < 1650\log c$. ∎

LEMMA 3. *Let $m, r \in \mathbb{N}$ with $2 \mid m$, $2 \nmid r$, $r > 1$. Define the integers U_r, V_r by $(m+\sqrt{-1})^r = V_r + U_r\sqrt{-1}$. If $a = |V_r|$, $b = |U_r|$, $c = m^2+1$ with $m \geq 200$, and if equation* (1) *has the solution (x, y, z) with $x = 2$, $2 \mid y$ and $y \geq 4$, then*

$$r > \frac{m}{\sqrt{825\log(m^2+1)-1}}.$$

Proof. It is clear that if $m \geq 200$ then $\min(b, c) \geq 200^2$ and $b > a^{2/n}$, where $n \leq 422$ is some positive integer (for example, $n = 4$). Hence, by Lemma 2 we get

$$y < 1650\log(m^2+1). \tag{12}$$

On the other hand, taking (1) mod m^4, we have

$$r^2m^2 + \left(1 - y\cdot\frac{1}{2}\,r(r-1)m^2\right) \equiv (1+zm^2) \pmod{m^4},$$

i.e. $\frac{1}{2}r(r-1)y + z \equiv r^2 \pmod{m^2}$, and so

$$\frac{1}{2}\,r(r-1)y + z \geq r^2 + m^2, \tag{13}$$

since $y \geq 4$ and $\frac{1}{2}r(r-1)y + z > r^2$. Now, we prove that $z < \frac{1}{2}ry$. Suppose $z \geq \frac{1}{2}ry$. Since $z > r$, we have

$$c^{rz} = (a^2+b^2)^z = \sum_{j=0}^{z}\binom{z}{j}(a^2)^j(b^2)^{z-j} > \sum_{j=0}^{r}\binom{r}{j}(a^2)^j(b^2)^{ry/2-j}$$

$$> \sum_{j=0}^{r}\binom{r}{j}(a^2)^j b^{ry-yj} = (a^2+b^y)^r = c^{zr},$$

which is impossible. Thus, $z < \frac{1}{2}ry$ and from (13) we get

$$y > 2 + \frac{2}{r^2}\,m^2. \tag{14}$$

By (12) and (14), we get the assertion. ∎

3. Some results on Diophantine equations

LEMMA 4. *Suppose that p is an odd prime and $D > 0$ is not divisible by primes of the form $2kp+1$. If the Diophantine equation*

$$x^p + y^p = Dz^2, \qquad x, y, z \in \mathbb{Z},\ \gcd(x, y) = 1,$$

has a solution with $2 \mid z$, then $2p \mid z$.

Proof. For the case $D = 2$ see Cao [C2] and for the case $D > 2$ see [C3]. ∎

LEMMA 5. *If p is an odd prime with $p \geq 7$, then the Diophantine equation*

$$x^p + y^p = 3z^2, \quad x, y, z \in \mathbb{Z},\ \gcd(x, y) = 1,$$

has no solution with $z \neq 0$.

Proof. This is a recent result of Bennett and Skinner [BS]. ∎

LEMMA 6. *The Diophantine equation*

$$125x^4 - 25x^2y^2 + y^4 = z^2, \quad x, y, z \in \mathbb{N},\ \gcd(x, y) = 1, \tag{15}$$

has no solution.

Proof. It is clear that $2 \nmid x + y$ and we may suppose that xy has the least possible value. From (15), we have

$$(2y^2 - 25x^2)^2 - 125x^4 = 4z^2,$$

and so

$$(|2y^2 - 25x^2| - 2z)(|2y^2 - 25x^2| + 2z) = 125x^4. \tag{16}$$

Suppose that $2 \mid y$. We have $2 \nmid x$. As is easily seen, $\gcd(|2y^2 - 25x^2| - 2z, |2y^2 - 25x^2| + 2z) = 1$. Hence, from (16) we get

$$|2y^2 - 25x^2| \pm 2z = 125x_1^4, \quad |2y^2 - 25x^2| \mp 2z = x_2^4,$$

and so either

$$4y^2 = 125x_1^4 + x_2^4 + 50x_1^2x_2^2, \tag{17}$$

or

$$-4y^2 = 125x_1^4 + x_2^4 - 50x_1^2x_2^2, \tag{18}$$

where $x = x_1x_2$, $x_1, x_2 \in \mathbb{N}$ with $\gcd(x_1, x_2) = 1$ and $2 \nmid x_1x_2$. Reducing mod 16, we see that (18) is impossible since $2 \mid y$. For (17), write

$$\left(\frac{x_2^2 + 25x_1^2}{2}\right)^2 - 5^3x_1^4 = y^2,$$

and so

$$\left(\frac{x_2^2 + 25x_1^2}{2} + y\right)\left(\frac{x_2^2 + 25x_1^2}{2} - y\right) = 5^3x_1^4. \tag{19}$$

Since $\gcd\left(\frac{x_2^2+25x_1^2}{2} + y, \frac{x_2^2+25x_1^2}{2} - y\right) = 1$, from (19) we get

$$\frac{x_2^2 + 25x_1^2}{2} \pm y = 5^3x_3^4, \quad \frac{x_2^2 + 25x_1^2}{2} \mp y = x_4^4, \tag{20}$$

where $x_1 = x_3x_4$, $x_3, x_4 \in \mathbb{N}$ with $\gcd(x_3, x_4) = 1$ and $2 \nmid x_3x_4$. From $x_1 = x_3x_4$ and (20), we have

$$125x_3^4 - 25x_3^2x_4^2 + x_4^4 = x_2^2$$

which is impossible by reduction mod 8 and $2 \nmid x_3x_4$.

Suppose that $2 \nmid y$. We have $2 \mid x$. As is easily seen, $\gcd(|2y^2 - 25x^2| - 2z, |2y^2 - 25x^2| + 2z) = 4$. Hence, from (16) we get

$$|2y^2 - 25x^2| \pm 2z = 4 \cdot 125x_1^4, \quad |2y^2 - 25x^2| \mp 2z = 4x_2^4,$$

and so

$$y^2 = 125x_1^4 + x_2^4 + 50x_1^2x_2^2, \tag{21}$$

or

$$-y^2 = 125x_1^4 + x_2^4 - 50x_1^2x_2^2, \tag{22}$$

where $x = 2x_1x_2$, $x_1, x_2 \in \mathbb{N}$ with $\gcd(x_1, x_2) = 1$ and $2 \mid x_1x_2$. Reducing mod 4, we see that (22) is impossible since $2 \mid x_1x_2$. For (21), reducing mod 8, we see that $2 \mid x_1$, $2 \nmid x_2$. Write

$$(x_2^2 + 25x_1^2)^2 - 4 \cdot 5^3x_1^4 = y^2,$$

and so

$$\left(\frac{x_2^2 + 25x_1^2 + y}{2}\right)\left(\frac{x_2^2 + 25x_1^2 - y}{2}\right) = 5^3x_1^4. \tag{23}$$

Since $\gcd\left(\frac{x_2^2+25x_1^2+y}{2}, \frac{x_2^2+25x_1^2-y}{2}\right) = 1$, from (23) we get

$$x_2^2 + 25x_1^2 \pm y = 2 \cdot 5^3x_3^4, \quad x_2^2 + 25x_1^2 \mp y = 2x_4^4, \tag{24}$$

where $x_1 = x_3x_4$, $x_3, x_4 \in \mathbb{N}$ with $\gcd(x_3, x_4) = 1$ and $2 \mid x_3x_4$. From $x_1 = x_3x_4$ and (24), we have

$$125x_3^4 - 25x_3^2x_4^2 + x_4^4 = x_2^2$$

which is impossible by the method of descent since $x_3x_4 = x_1 < x \le xy$. ∎

Lemma 7. *The Diophantine equation*

$$x^5 + y^5 = 3z^2, \quad x, y, z \in \mathbb{Z},\ \gcd(x, y) = 1, \tag{25}$$

has no solution with $2 \mid z$ *and* $z \neq 0$.

Proof. Suppose that equation (25) has a solution with $2 \mid z$ and $z \neq 0$. We may assume that $z \in \mathbb{N}$. Then by Lemma 4, we have $10 \mid z$. Hence, (25) gives

$$x + y = 60z_1^2, \quad x^4 - x^3y + x^2y^2 - xy^3 + y^4 = 5z_2^2, \tag{26}$$

where $z = 10z_1z_2$, $z_1, z_2 \in \mathbb{N}$ with $\gcd(z_1, z_2) = 1$ and $2 \nmid z_2$. Without loss of generality, we may assume that $x > y$. Let $x + y = 10a, x - y = 2b$, where $a = 6z_1^2$ and $b \in \mathbb{N}$ with $\gcd(a, b) = 1$. Then from (26), we have

$$125a^4 + 50a^2b^2 + b^4 = z_2^2, \quad a, b \in \mathbb{N}. \tag{27}$$

By the same argument as in the proof of (21), we deduce from (27) that equation (15) has a solution. This is impossible by Lemma 6. ∎

LEMMA 8 ([DM]). *If $n \in \mathbb{N}$ with $n \geq 4$, then the equation*

$$x^n + y^n = z^2, \quad x, y, z \in \mathbb{Z},\ xyz \neq 0,\ \gcd(x, y) = 1,$$

has no solution.

LEMMA 9 ([CD, Theorem 3]). *Suppose that $k \in \mathbb{N}$ with $k > 1$. If $2 \mid A$, then the Diophantine equation*

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

has no solution with $AB \neq 0$.

LEMMA 10. *If $k \in \mathbb{N}$ with $k > 1$, then the Diophantine equation*

$$A^{2k} + B^4 = C^2, \quad A, B, C \in \mathbb{Z},\ \gcd(A, B) = 1, \tag{28}$$

has no solution with $AB \neq 0$.

Proof. If $2 \mid k$, then it is clear that the conclusion holds (see [R] or [C4]). If $k = 3$, then it also holds (see [B, Theorem 1.3.1]).

Now, we suppose that $2 \nmid k > 3$ and equation (28) has a solution with $AB \neq 0$.

If $2 \nmid B$, then from (28), we have

$$|A|^k = 2uv, \quad B^2 = u^2 - v^2, \tag{29}$$

where $u, v \in \mathbb{N}$ with $\gcd(u, v) = 1, 2 \nmid u + v$. Then from the second equality of (29), we see that $2 \mid v$. So, from the first equality of (29), we get

$$2v = A_1^k, \quad u = A_2^k, \tag{30}$$

where $A_1, A_2 \in \mathbb{N}$ with $\gcd(A_1, A_2) = 1, 2 \nmid A_2$. From the second equality of (29), we get

$$u + v = B_1^2, \quad u - v = B_2^2, \quad B = B_1 B_2, \tag{31}$$

where $B_1, B_2 \in \mathbb{N}$ with $B_1 > B_2$, $\gcd(B_1, B_2) = 1, 2 \nmid B_1 B_2$. From (30) and (31), we have

$$A_1^k = B_1^2 - B_2^2, \quad 2A_2^k = B_1^2 + B_2^2. \tag{32}$$

Notice that $\gcd(B_1, B_2) = 1, 2 \nmid B_1 B_2$. From the first equality of (32), we get

$$B_1 \pm B_2 = 2A_3^k, \quad B_1 \mp B_2 = 2^{k-1} A_4^k, \tag{33}$$

where $A_3, A_4 \in \mathbb{N}$ with $\gcd(A_3, A_4) = 1$. Clearly, from (33) we have

$$B_1 = A_3^k + 2^{k-2} A_4^k, \quad \pm B_2 = A_3^k - 2^{k-2} A_4^k.$$

Substituting these into the second equality of (32), we have

$$A_2^k = A_3^{2k} + (2^{k-2} A_4^k)^2,$$

which is impossible by Lemma 8.

If $2 \mid B$, then from (28), we have

$$|A|^k = u^2 - v^2, \quad B^2 = 2uv, \tag{34}$$

where $u, v \in \mathbb{N}$ with $\gcd(u, v) = 1, 2 \nmid u + v$. Then from the first equality of (34), we get

$$u + v = A_1^k, \quad u - v = A_2^k,$$

and so

$$2u = A_1^k + A_2^k, \quad 2v = A_1^k - A_2^k, \tag{35}$$

where $A_1, A_2 \in \mathbb{N}$ with $\gcd(A_1, A_2) = 1$. From the second equality of (34), we get $2u = B_1^2$ or $2v = B_1^2$, where $B_1 \in \mathbb{N}$. Hence,

$$A_1^k + A_2^k = B_1^2 \quad \text{or} \quad A_1^k - A_2^k = B_1^2. \tag{36}$$

By Lemma 8, (36) is impossible since $k > 3$. ∎

4. Proof of theorems. We also need the following lemmas to prove our theorems.

LEMMA 11 ([CD, Lemma 2]). *Let $a, b, c \in \mathbb{N}$ satisfy $a^2 + b^2 = c^r$ 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 $x = 2$, $2 \mid y$, $2 \nmid z$.*

LEMMA 12 ([DC, Lemmas 2.1 and 2.2]). *If either equation (4) or (5) has a solution, then $2 \mid x$, $2 \mid y$.*

LEMMA 13 ([DC, Lemma 2.7]). *Let $m, r \in \mathbb{N}$ with $2 \mid m$, $2 \nmid r$, $r > 1$. 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 equation (1) has a solution (x, y, z) with $2 \mid y$, $2 \nmid z$, then $x = 2$.*

LEMMA 14 ([T1]). *The positive integer solutions of the equation $a^2 + b^2 = c^3$ with $\gcd(a, b) = 1$ are given by*

$$a = m|m^2 - 3n^2|, \quad b = n|3m^2 - n^2|, \quad c = m^2 + n^2,$$

where $m, n \in \mathbb{N}$ are such that $\gcd(m, n) = 1$ and $m \not\equiv n \pmod 2$.

Proof of Theorem 1. By Lemma 12, we have $2 \mid x$, $2 \mid y$. There are two cases.

CASE (i): $2 \nmid z$. By Lemma 13, we know that $x = 2$. First consider equation (4). If $y = 2$ then there is the only solution $(x, y, z) = (2, 2, 3)$. For $y \geq 4$, Lemma 3 shows that if $m \geq 200$ then $3 > m/\sqrt{825 \log(m^2 + 1) - 1}$. This is impossible if $m \geq 300$. If $m < 300$, then by Claim 1 of [T3] and by computer calculations, we have $3 \mid z$. Using the method of [T3], we verify that equation (4) has no solution.

REMARK. Using the results of [C1] and [DC], if m^2+1 or $3m^2-1$ is prime, then the conclusion of the theorem holds. By computing, if both $m^2 + 1$ and $3m^2 - 1$ are not primes, then the first values of m are $32, 38, 42, 46, 62, \ldots$

By a similar method, we can find that equation (5) has only the solution $(x, y, z) = (2, 2, 5)$.

Case (ii): $2 \mid z$. Put $x = 2x_1$, $y = 2y_1$, $z = 2z_1$, where $x_1, y_1, z_1 \in \mathbb{N}$. Then by taking equation (1) mod m^4, we see that if $x_1 = 1$, then

$$\tfrac{1}{2}r(r-1) \cdot 2y_1 + 2z_1 \equiv r^2 \pmod{m^2}, \quad r \in \{3, 5\}, \tag{37}$$

and if $x_1 > 1$, then

$$\tfrac{1}{2}r(r-1) \cdot 2y_1 + 2z_1 \equiv 0 \pmod{m^2}, \quad r \in \{3, 5\}. \tag{38}$$

Clearly, (37) is impossible since $2 \mid m$. So $x_1 > 1$ and (38) holds. By Lemma 9, z_1 is odd. We see that (38) is impossible if $r = 5$.

Now, we consider the case $r = 3$. By Lemma 11, it suffices to prove the theorem if $4 \mid m$. From (38), we know that $2 \nmid y_1$ since $2 \nmid z_1$. Notice that equation (4) implies

$$(m^3 - 3m)^{2x_1} = ((m^2+1)^{z_1} - (3m^2-1)^{y_1})((m^2+1)^{z_1} + (3m^2-1)^{y_1}). \tag{39}$$

Clearly,

$$\begin{aligned} ((m^2+1)^{z_1} - (3m^2-1)^{y_1}) &\equiv 2 \pmod{m^2}, \\ ((m^2+1)^{z_1} + (3m^2-1)^{y_1}) &\equiv 0 \pmod{m^2} \end{aligned}$$

since $2 \nmid y_1 z_1$. So, from (39) we get

$$\begin{aligned} (m^2+1)^{z_1} - (3m^2-1)^{y_1} &= 2u^{2x_1}, \\ (m^2+1)^{z_1} + (3m^2-1)^{y_1} &= \tfrac{1}{2}m^{2x_1}v^{2x_1}, \end{aligned} \tag{40}$$

where $u, v \in \mathbb{N}$ with

$$\gcd(u, v) = 1, \quad uv = m^2 - 3. \tag{41}$$

By (40), we have $(m^2+1)^{z_1} - (3m^2-1)^{y_1} \equiv 0 \pmod{u}$ and $(m^2+1)^{z_1} + (3m^2-1)^{y_1} \equiv 0 \pmod{v}$. Since (41) gives $m^2 \equiv 3 \pmod{u}$ and $m^2 \equiv 3 \pmod{v}$, we infer, using Jacobi's symbol, that $\left(\frac{2}{u}\right) = 1$ and $\left(\frac{-2}{v}\right) = 1$. Thus, from $4 \mid m$ and (41), we get $u \equiv 7 \pmod 8$ and $v \equiv 3 \pmod 8$. If $2 \mid x_1$, then from Lemma 10 and equation (4), we have $y_1 = 1$. By (40), we have

$$\begin{aligned} 3m^2 - 1 = (3m^2-1)^{y_1} &= \tfrac{1}{4}m^{2x_1}v^{2x_1} - u^{2x_1} \\ &= \left(\tfrac{1}{2}m^{x_1}v^{x_1} + u^{x_1}\right)\left(\tfrac{1}{2}m^{x_1}v^{x_1} - u^{x_1}\right) \geq \tfrac{1}{2}m^{x_1}v^{x_1} + u^{x_1}. \end{aligned}$$

It follows that $3m^2 - 1 > \frac{1}{2}m^2 \cdot 3^2 + 1 > 3m^2 - 1$, a contradiction. Hence, we get $2 \nmid x_1 y_1 z_1$ and $x_1 > 1$, $y_1 > 1$.

Also, by the second equality of (40), we have $3 \mid m$. From this and (38), we see that $3 \mid z_1$. Let $z_1 = 3z_2$, $z_2 \in \mathbb{N}$. Hence, (40) implies that

$$u^{2x_1} + \tfrac{1}{4}m^{2x_1}v^{2x_1} = (m^2+1)^{3z_2}. \tag{42}$$

By Lemma 14, from (42) we get

$$\tfrac{1}{2}m^{x_1}v^{x_1} = s|s^2 - 3t^2|, \quad u^{x_1} = t|t^2 - 3s^2|, \tag{43}$$

where $s, t \in \mathbb{N}$ with $\gcd(s,t) = 1$ and $2 \nmid s+t$. Since $3 \mid m$, we know from (43) that $3 \mid s$. Hence, $\gcd(t, t^2 - 3s^2) = 1$ since $\gcd(s,t) = 1$. Thus, by the second equality of (43), we have $t = u_1^{x_1}$, $|t^2 - 3s^2| = u_2^{x_1}$, and so

$$u_1^{2x_1} + (\pm u_2)^{x_1} = 3s^2, \tag{44}$$

where $u_1, u_2 \in \mathbb{N}$ with $\gcd(u_1, u_2) = 1$ and $2 \nmid u_1 u_2$. Since $2 \nmid x_1 > 1$, we have $p \mid x_1$, where p is an odd prime. If $p = 3$, then equation (4) is impossible by Lemma 8 and $6 \mid x$, $6 \mid z$. If $p = 5$, then (44) is impossible by Lemma 7. If $p \geq 7$, then (44) is also impossible by Lemma 5. ∎

Proof of Theorem 2. It is clear that $2 \parallel a$ when $m \equiv 2 \pmod 4$. Then from Lemma 11, we get $x = 2$, $y = 2y_1$ and $2 \nmid z$, where $y_1 \in \mathbb{N}$. Assume that $y_1 > 1$. By Lemma 3, we have $r > m/\sqrt{825 \log(m^2+1) - 1}$. This contradicts the assumption. Thus $y_1 = 1$ and from (1) we obtain $z = r$. ∎

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

References

[BS] M. Bennett and C. Skinner, *Ternary Diophantine equations via Galois representations and modular forms*, Canad. J. Math., to appear. Or see http://www.math.ubc.ca/~bennett/publ.html.

[B] N. Bruin, *Chabauty methods and covering techniques applied to generalized Fermat equations*, thesis, 1999.

[C1] Z. F. Cao, *A note on the Diophantine equation* $a^x + b^y = c^z$, Acta Arith. 91 (1999), 85–93.

[C2] —, *On the Diophantine equation* $x^{2n} - \mathcal{D}y^2 = 1$, Proc. Amer. Math. Soc. 98 (1986), 11–16.

[C3] —, *On the Diophantine equation* $x^p - y^p = \mathcal{D}z^2$, Dongbei Shuxue (Northeast. Math. J.) 2 (1986), 219–227; MR88b:11013.

[C4] —, *Introduction to Diophantine Equations*, Harbin Institute Technology Press, 1989; MR92e: 11018.

[CD] Z. F. Cao and X. L. Dong, *On the Terai–Jeśmanowicz conjecture*, Publ. Math. Debrecen 61 (2002), 253–265.

[DM] H. Darmon and L. Merel, *Winding quotients and some variants of Fermat's Last Theorem*, J. Reine Angew. Math. 490 (1997), 81–100.

[DC] X. L. Dong and Z. F. Cao, *The Terai–Jeśmanowicz conjecture on the equation* $a^x + b^y = c^z$, Chinese Ann. Math. Ser. A 21 (2000), 709–714.

[L1] 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 (1997), no. 7, 148–149.

[L2] —, *On Terai's conjecture concerning Pythagorean numbers*, Bull. Austral. Math. Soc. 61 (2000), 329–334.

[M] M. Mignotte, *A corollary to a theorem of Laurent–Mignotte–Nesterenko*, Acta Arith. 86 (1998), 101–111.

[R] P. Ribenboim, *13 Lectures on Fermat's Last Theorem*, Springer, 1979.

[T1] N. Terai, *The Diophantine equation* $a^x + b^y = c^z$, Proc. Japan Acad. Ser. A Math. Sci. 70 (1994), no. 1, 22–26.
[T2] —, *The Diophantine equation* $a^x + b^y = c^z$, *II*, ibid. 71 (1995), no. 6, 109–110.
[T3] —, *Applications of a lower bound for linear forms in two logarithms to exponential Diophantine equations*, Acta Arith. 90 (1999), 17–35.

Department of Computer Science
Shanghai Jiao Tong University
Shanghai 200030
P.R. China
E-mail: zfcao@cs.sjtu.edu.cn

Department of Mathematics
Shanghai Jiao Tong University
Shanghai 200030
P.R. China
E-mail: xldong@mail.sjtu.edu.cn

Received on 19.4.2002
and in revised form on 25.11.2002 (4265)