A note on the Diophantine equation $a^x + b^y = c^z$

by

ZHENFU CAO (Harbin)

1. Introduction. Let \mathbb{Z} , \mathbb{N} , \mathbb{P} be the sets of integers, positive integers and primes respectively, and

$$\mathbb{P}^{\mathbb{N}} = \{ p^n \, | \, p \in \mathbb{P} \text{ and } n \in \mathbb{N} \}.$$

Clearly, $\mathbb{P} \subseteq \mathbb{P}^{\mathbb{N}}$. In [13] Nagell first proved that if $\max(a, b, c) \leq 7$, then all the solutions $(x, y, z) \in \mathbb{N}^3$ of the equation

$$a^x + b^y = c^z, \quad a, b, c \in \mathbb{P}, \ a > b$$

are given by

(1)

$$\begin{split} &(a,b,c)=(3,2,5):(x,y,z)=(1,1,1),(2,4,2);\\ &(a,b,c)=(5,2,3):(x,y,z)=(2,1,3),(1,2,2);\\ &(a,b,c)=(5,3,2):(x,y,z)=(1,1,3),(1,3,5),(3,1,7);\\ &(a,b,c)=(3,2,7):(x,y,z)=(1,2,1);\\ &(a,b,c)=(7,2,3):(x,y,z)=(1,1,2),(2,5,4);\\ &(a,b,c)=(7,3,2):(x,y,z)=(1,2,4);\\ &(a,b,c)=(5,2,7):(x,y,z)=(1,2,5). \end{split}$$

Later, Mąkowski [11], Hadano [7], Uchiyama [23], Qi Sun and Xiaoming Zhou [16], and Xiaozhuo Yang [24] determined all solutions $(x, y, z) \in \mathbb{N}^3$ of equation (1), when $11 \leq \max(a, b, c) \leq 23$. In [1] we have given all solutions $(x, y, z) \in \mathbb{N}^3$ of equation (1), when $29 \leq \max(a, b, c) \leq 97$ (60 solutions in total), and we have proved the following:

THEOREM A. If $\max(a, b, c) > 13$, then equation (1) has at most one solution $(x, y, z) \in \mathbb{N}^3$ with z > 1.

¹⁹⁹¹ Mathematics Subject Classification: Primary 11D61.

Key words and phrases: exponential Diophantine equation.

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

^[85]

A more general result was given in [2]. Let $A, B \in \mathbb{N}, A > B > 1$ and gcd(A, B) = 1. If the equation

(2)
$$X^2 + ABY^2 = p^2$$
, $X, Y, Z \in \mathbb{N}, p \in \mathbb{P}$, and $gcd(X, Y) = 1$,
has a solution (X, Y, Z) , then there exists a unique solution (X_n, Y_n)

which satisfies $Z_p \leq Z$, where Z runs over all solutions of (2). That (X_p, Y_p, Z_p) is called the *least solution* of (2). From [2] we have

THEOREM B. If $x, y \in \mathbb{N}$ satisfy the equation

(3)
$$Ax^2 + By^2 = 2^z, \quad z > 2, \ x \mid^* A, \ y \mid^* B$$

where the symbol $x \mid^* A$ means that every prime divisor of x divides A, then

$$|Ax^2 - By^2| = 2X_2, \quad xy = Y_2, \ 2z - 2 = Z_2,$$

 $except \ for \ (A,B,x,y,z) = (5,3,1,3,5), (5,3,5,1,7) \ and \ (13,3,1,9,8).$

THEOREM C. If $x, y \in \mathbb{N}$ satisfy the equation

(4)
$$Ax^2 + By^2 = p^z, \quad p \in \mathbb{P}, \ x \mid^* A, \ y \mid^* B,$$

then

$$|Ax^2 - By^2| = X_p, \quad 2xy = Y_p, \ 2z = Z_p$$

or

 $|Ax^{2} - By^{2}| = X_{p}|X_{p}^{2} - 3ABY_{p}^{2}|, \quad 2xy = Y_{p}|3X_{p}^{2} - ABY_{p}^{2}|, \ 2z = 3Z_{p},$ the latter occurring only for

$$Ax^{2} + By^{2} = 3^{4s+3} \left(\frac{3^{2s} - 1}{8}\right) + \left(\frac{3^{2s+2} - 1}{8}\right) = \left(\frac{3^{2s+1} - 1}{2}\right)^{3} = p^{z},$$

where $s \in \mathbb{N}$.

From Theorems B and C, we have (cf. Lemma 6 of [15])

THEOREM D. The equation

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

has at most one solution when the parities of x and y are fixed, except for (a, b, c) = (5, 3, 2), (13, 3, 2), (10, 3, 13). The solutions in case (5, 3, 2) are given by (x, y, z) = (1, 1, 3), (1, 3, 5), (3, 1, 7), in case (13, 3, 2) by (1, 1, 4) and (1, 5, 8), and in case (10, 3, 13) by (1, 1, 1) and (1, 7, 3) (cf. [14], [3]).

In [3], we obtained further results when the right sides of equation (3) and equation (4) are replaced by $4k^z$ and k^z respectively, where $k \in \mathbb{N}$.

Recently, N. Terai [20, 21] conjectured that if $a, b, c, p, q, r \in \mathbb{N}$ are fixed, and $a^p + b^q = c^r$, where $p, q, r \ge 2$, and gcd(a, b) = 1, then the Diophantine equation

(5)
$$a^x + b^y = c^z, \quad x, y, z \in \mathbb{N},$$

has only the solution (x, y, z) = (p, q, r). The conjecture is clearly false. For example, from Nagell's result [13], we see that the equation $3^x + 2^y = 5^z$ has two solutions (x, y, z) = (1, 1, 1), (2, 4, 2), and the equation $7^x + 2^y = 3^z$ also has two solutions (x, y, z) = (1, 1, 2), (2, 5, 4). Furthermore, if a = 1 or b = 1, then the conjecture is also false. So, the condition $\max(a, b, c) > 7$ should be added to the hypotheses of the conjecture.

For p = q = r = 2 the above statement was conjectured previously by Jeśmanowicz. We shall use the term Terai–Jeśmanowicz conjecture for the above conjecture with the added condition that $\max(a, b, c) > 7$. Some recent results on the Terai–Jeśmanowicz conjecture are as follows:

(a) If p = q = r = 2, we may assume without loss of generality that $2 \mid a$. Then we have

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

where $s, t \in \mathbb{N}, s > t$, gcd(s, t) = 1 and 2 | st. In 1982, we [4] proved that

(Cao.1) if $2 || s, t \equiv 1 \pmod{4}$, or $2 || s, t \equiv 3 \pmod{4}$ and s + t has a prime factor of the form 4k - 1, then the Terai–Jeśmanowicz conjecture holds;

(Cao.2) if $(s,t) \equiv (1,6)$, $(5,2) \pmod{8}$, or $(s,t) \equiv (3,4) \pmod{4}$ and s+t has a prime factor of the form 4k-1, then the Terai–Jeśmanowicz conjecture holds (also see [5], pp. 366–367).

Maohua Le [8, 9, 6] proved that

(Le.1) if $2 \parallel s, t \equiv 3 \pmod{4}$ and $s \ge 81t$, then the Terai–Jeśmanowicz conjecture holds;

(Le.2) if $2^2 \parallel a$ and $c \in \mathbb{P}^{\mathbb{N}}$, then the Terai–Jeśmanowicz conjecture holds; (Le.3) if t = 3, s is even, and $s \leq 6000$, then the Terai–Jeśmanowicz conjecture holds.

K. Takakuwa and Y. Asaeda [17–19] considered the case s = 2s', t = 3, 7, 11, 15. For example, they proved that if $2 \nmid s'$, then the Terai–Jeśmanowicz conjecture holds.

(b) N. Terai [20–22] considered the cases (p,q,r) = (2,2,3); (2,2,5); (2,2,r), where $r \in \mathbb{P}$. He proved that

(Terai.1) if $a = m(m^2 - 3)$, $b = 3m^2 - 1$, $c = m^2 + 1$ with m even and b is a 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 equation (5) has only the solution (x, y, z) = (2, 2, 3);

(Terai.2) if $a = m|m^4 - 10m^2 + 5|$, $b = 5m^4 - 10m^2 + 1$, $c = m^2 + 1$ with m even and b is a 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 $c \mod{l}$, then equation (5) has only the solution (x, y, z) = (2, 2, 5).

In addition, Scott [15] proved a result which implies the following.

THEOREM E. If c = 2, then the Terai–Jeśmanowicz conjecture is true. If c is an odd prime, then there is at most one other solution to the Terai–Jeśmanowicz conjecture.

In this note, we deal with the Terai–Jeśmanowicz conjecture for the special case p = q = 2, r odd. We have

THEOREM. If $p = q = 2, 2 \nmid r, c \equiv 5 \pmod{8}$, $b \equiv 3 \pmod{4}$ and $c \in \mathbb{P}^{\mathbb{N}}$, then the Terai-Jeśmanowicz conjecture holds.

COROLLARY 1 TO THEOREM. Let

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

where $m, n \in \mathbb{N}$, gcd(m, n) = 1. If $m \equiv 2 \pmod{4}$, $n \equiv 1 \pmod{4}$ and $m^2 + n^2 \in \mathbb{P}^{\mathbb{N}}$, then equation (5) has only the solution (x, y, z) = (2, 2, 3).

COROLLARY 2 TO THEOREM. Let

(6)
$$a = m|m^4 - 10m^2n^2 + 5n^4|, \quad b = n|5m^4 - 10m^2n^2 + n^4|, \quad c = m^2 + n^2,$$

where $m, n \in \mathbb{N}$ with gcd(m, n) = 1, $m^2 + n^2 \in \mathbb{P}^{\mathbb{N}}$ and $m \equiv 2 \pmod{4}$. If one of the following cases holds, then equation (5) has only the solution (x, y, z) = (2, 2, 5):

CASE 1: $m > \sqrt{2n}$ and $n \equiv 3 \pmod{4}$; CASE 2: $m > \sqrt{10n}$; CASE 3: n = 1.

From Corollary 1, we see that if $m \equiv 2 \pmod{4}$ and $m^2 + 1 \in \mathbb{P}$, then the equation

$$(m(m^2-3))^x + (3m^2-1)^y = (m^2+1)^z, \quad x, y, z \in \mathbb{N},$$

has only the solution (x, y, z) = (2, 2, 3).

2. Preliminaries. We will use the following lemmas.

LEMMA 1. If $2 \nmid r$ and r > 1, then all solutions (X, Y, Z) of the equation $X^2 + Y^2 = Z^r$, $X, Y, Z \in \mathbb{Z}$, 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 $\lambda_1, \lambda_2 \in \{-1, 1\}, X_1, Y_1 \in \mathbb{N} \text{ and } gcd(X_1, Y_1) = 1.$

Lemma 1 follows directly from a theorem in the book of Mordell [12], pp. 122–123.

LEMMA 2. For any $k \in \mathbb{N}$ and any complex numbers α, β , we have

$$\alpha^{k} + \beta^{k} = \sum_{j=0}^{[k/2]} \begin{bmatrix} k \\ j \end{bmatrix} (\alpha + \beta)^{k-2j} (-\alpha\beta)^{j},$$

where

$$\begin{bmatrix} k \\ j \end{bmatrix} = \frac{(k-j-1)!k}{(k-2j)!\,j!} \in \mathbb{N} \quad (j=0,1,\ldots,[k/2]).$$

It is Formula 1.76 in [10].

LEMMA 3. Let $a, b, c, p, q, r \in \mathbb{N}$ satisfy the hypotheses of the Terai-Jeśmanowicz conjecture. If $p = q = 2, 2 \nmid r$, and if $c \equiv 5 \pmod{8}, 2 \mid a$, then

$$\left(\frac{a}{c}\right) = -1, \quad \left(\frac{b}{c}\right) = 1,$$

and so $2 \mid x$ in equation (5). Here $\left(\frac{*}{c}\right)$ denotes the Legendre–Jacobi symbol.

Proof. Since $p = q = 2, 2 \nmid r$, we have

(7)
$$a^2 + b^2 = c^r, \quad a, b, c \in \mathbb{N}, \ \gcd(a, b) = 1.$$

By Lemma 1, we deduce from (7) that

(8)
$$a + b\sqrt{-1} = \lambda_1 (m + \lambda_2 n \sqrt{-1})^r, \quad c = m^2 + n^2$$

where $\lambda_1, \lambda_2 \in \{-1, 1\}, m, n \in \mathbb{N}$ and gcd(m, n) = 1. From (8), we have

$$2\lambda_1 a = (m + \lambda_2 n \sqrt{-1})^r + (m - \lambda_2 n \sqrt{-1})^r,$$

$$2\lambda_1 b \sqrt{-1} = (m + \lambda_2 n \sqrt{-1})^r - (m - \lambda_2 n \sqrt{-1})^r.$$

Hence, by Lemma 2 we have

(9)
$$\lambda_1 a = \frac{1}{2} \sum_{j=0}^{(r-1)/2} {r \brack j} (2m)^{r-2j} (-m^2 - n^2)^j$$
$$= m \sum_{j=0}^{(r-1)/2} {r \brack j} (4m^2)^{(r-1)/2 - j} (-m^2 - n^2)^j,$$

(10)
$$\lambda_1 b = \frac{1}{2\sqrt{-1}} \sum_{j=0}^{(r-1)/2} {r \brack j} (2\lambda_2 n \sqrt{-1})^{r-2j} (m^2 + n^2)^j$$
$$= \lambda_2 n \sum_{j=0}^{(r-1)/2} {r \brack j} (-4n^2)^{(r-1)/2-j} (m^2 + n^2)^j.$$

Since $c \equiv 5 \pmod{8}$, and $2 \mid a$, we see from (8) and (9) that $2 \mid m, 2 \nmid n$.

So by (9) and (10), we have

$$\begin{pmatrix} \frac{a}{c} \end{pmatrix} = \left(\frac{\lambda_1 a}{c}\right) = \left(\frac{m(4m^2)^{(r-1)/2}}{m^2 + n^2}\right) = \left(\frac{m}{m^2 + n^2}\right) = -\left(\frac{m/2}{m^2 + n^2}\right) = -1,$$
$$\begin{pmatrix} \frac{b}{c} \end{pmatrix} = \left(\frac{\lambda_1 b}{c}\right) = \left(\frac{\lambda_2 n(-4n^2)^{(r-1)/2}}{m^2 + n^2}\right) = \left(\frac{n}{m^2 + n^2}\right) = 1.$$

This completes the proof of Lemma 3.

3. Proof of the Theorem and its corollaries

Proof of Theorem. Since $c \equiv 5 \pmod{8}$ and $b \equiv 3 \pmod{4}$, we have $2 \mid a$. By Lemma 3, we find that $2 \mid x$. From (5), we have $3^y \equiv 1 \pmod{4}$. Hence $2 \mid y$. Then by Theorem D, we deduce that equation (5) has at most one solution (x, y, z), except for

$$(a, b, c) = (5, 3, 2), (13, 3, 2), (10, 3, 13).$$

Clearly, $(a, b, c) \neq (5, 3, 2)$ since $\max(a, b, c) > 7$, and the equations $13^p + 3^q = 2^r$ and $10^p + 3^q = 13^r$ are all impossible since $p, q, r \ge 2$ (see [23] and [14]). Thus, (5) has only the solution (x, y, z) = (2, 2, r). The Theorem is proved.

Proof of Corollary 1. If $m > n/\sqrt{3}$, then we find that $b = n(3m^2 - n^2) \equiv 3 \pmod{4}$. By the Theorem, Corollary 1 holds.

If $m < n/\sqrt{3}$, then

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

By Lemma 3 and Theorem D, if 2 | y, then Corollary 1 holds. Now assume that $2 \nmid y$. From (5),

(11)
$$\left(\frac{n(n^2 - 3m^2)}{3n^2 - m^2}\right) = \left(\frac{b}{3n^2 - m^2}\right)^y = \left(\frac{m^2 + n^2}{3n^2 - m^2}\right)^z$$

Since $m \equiv 2 \pmod{4}$ and $n \equiv 1 \pmod{4}$, we have

(12)
$$\left(\frac{n(n^2-3m^2)}{3n^2-m^2}\right) = \left(\frac{n^2-3m^2}{3n^2-m^2}\right) = \left(\frac{3n^2-m^2}{n^2-3m^2}\right) = \left(\frac{8m^2}{n^2-3m^2}\right) = -1,$$

(13)
$$\left(\frac{m^2+n^2}{3n^2-m^2}\right) = \left(\frac{3n^2-m^2}{n^2+m^2}\right) = \left(\frac{-4m^2}{n^2+m^2}\right) = 1$$

From (11)–(13), we get -1 = 1, a contradiction. This proves the corollary.

Proof of Corollary 2. From the Theorem, it suffices to prove Cases 2 and 3 of Corollary 2. Now we assume that

$$a = m|m^4 - 10m^2n^2 + 5n^4|, \quad b = 5m^4 - 10m^2n^2 + n^4, \quad c = m^2 + n^2,$$

 $m>\sqrt{10}n$ and $n\equiv 1 \pmod{4}.$ Clearly, $m^4-10m^2n^2+5n^4\in\mathbb{N}.$ If $5\nmid n,$ then we have

$$\begin{pmatrix} \frac{b}{m^4 - 10m^2n^2 + 5n^4} \end{pmatrix}$$

$$= \left(\frac{m^4 - 10m^2n^2 + 5n^4}{5m^4 - 10m^2n^2 + n^4} \right)$$

$$= \left(\frac{5}{5m^4 - 10m^2n^2 + n^4} \right) \left(\frac{5m^4 - 50m^2n^2 + 25n^4}{5m^4 - 10m^2n^2 + n^4} \right)$$

$$= \left(\frac{-40m^2n^2 + 24n^4}{5m^4 - 10m^2n^2 + n^4} \right) = \left(\frac{5m^2 - 3n^2}{5m^4 - 10m^2n^2 + n^4} \right)$$

$$= \left(\frac{5m^4 - 10m^2n^2 + n^4}{5m^2 - 3n^2} \right) = \left(\frac{-7m^2 + n^2}{5m^2 - 3n^2} \right)$$

$$= \left(\frac{5}{5m^2 - 3n^2} \right) \left(\frac{-7(5m^2 - 3n^2) - 16n^2}{5m^2 - 3n^2} \right) = \left(\frac{5m^2 - 3n^2}{5} \right) = -1.$$

If $5 \mid n$ then we also have

$$\left(\frac{b}{m^4 - 10m^2n^2 + 5n^4}\right) = -1$$

by a similar method. Moreover

$$\left(\frac{c}{m^4 - 10m^2n^2 + 5n^4}\right) = \left(\frac{m^4 - 10m^2n^2 + 5n^4}{m^2 + n^2}\right) = \left(\frac{16}{m^2 + n^2}\right) = 1.$$

Hence, from (5) we have 2 | y. From Lemma 3 we deduce similarly that 2 | x. Then Theorem D implies Case 2. For Case 3 the only remaining case is m = 2. Then a = 38, b = 41, c = 5. As above we find 2 | x, 2 | y, and Case 3 follows from Theorem D.

4. An open problem. Let r > 1 be a given odd number, and let

$$a = m \bigg| \sum_{j=0}^{(r-1)/2} {r \brack j} (4m^2)^{(r-1)/2-j} (-m^2 - 1)^j \bigg|,$$

$$b = \bigg| \sum_{j=0}^{(r-1)/2} {r \brack j} (-4)^{(r-1)/2-j} (m^2 + 1)^j \bigg|,$$

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

where $m \in \mathbb{N}$ with $m^2 + 1 \in \mathbb{P}$ and $m \equiv 2 \pmod{4}$. Clearly, (a, b, c) is a solution of equation (7). Is it possible to prove the Terai–Jeśmanowicz

conjecture by the method of this paper under the above condition? When r = 3, 5, the answer to the question is "yes".

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

References

- [1] Z. F. Cao, On the Diophantine equation $a^x + b^y = c^z$, I, Chinese Sci. Bull. 32 (1987), 1519–1521; II, ibid. 33 (1988), 237 (in Chinese).
- [2] —, On the Diophantine equation $ax^2 + by^2 = p^z$, J. Harbin Inst. Tech. 23 (1991), 108–111.
- [3] —, Divisibility of the class numbers of imaginary quadratic fields, Acta Math. Sinica 37 (1994), 50–56 (in Chinese).
- [4] —, On Jeśmanowicz' conjecture, Res. Rep. Harbin Inst. Tech. 253 (1982), 1–14.
- [5] —, Introduction to Diophantine equations, Harbin Inst. Tech. Press, 1989 (in Chinese).
- [6] Y. D. Guo and M. H. Le, A note on Jeśmanowicz' conjecture concerning Pythagorean numbers, Comment. Math. Univ. St. Paul. 44 (1995), 225–228.
- [7] T. Hadano, On the Diophantine equation $a^x = b^y + c^z$, Math. J. Okayama Univ. 19 (1976/77), 25–29.
- [8] M. H. Le, On Jeśmanowicz' conjecture concerning Pythagorean numbers, Proc. Japan Acad. Ser. A Math. Sci. 72 (1996), 97–98.
- [9] —, A note on Jeśmanowicz' conjecture, Colloq. Math. 69 (1995), 47–51.
- [10] R. Lidl and H. Niederreiter, *Finite Fields*, Addison-Wesley, Reading, MA, 1983.
- [11] A. Mąkowski, On the diophantine equation $2^x + 11^y = 5^z$, Nord. Mat. Tidskr. 7 (1959), 81–96.
- [12] L. J. Mordell, *Diophantine Equations*, Academic Press, 1969.
- [13] T. Nagell, Sur une classe d'équations exponentielles, Ark. Mat. 3 (1958), 569–582.
- [14] M. Perisastri, A note on the equation $a^x b^y = 10^z$, Math. Student 37 (1969), 211–212.
- [15] R. Scott, On the equations $p^x b^y = c$ and $a^x + b^y = c^z$, J. Number Theory 44 (1993), 153–165.
- [16] Q. Sun and X. M. Zhou, On the Diophantine equation $a^x + b^y = c^z$, Chinese Sci. Bull. 29 (1984), 61 (in Chinese).
- [17] K. Takakuwa, On a conjecture on Pythagorean numbers, III, Proc. Japan Acad. Ser. A Math. Sci. 69 (1993), no. 9, 345–349.
- [18] K. Takakuwa and Y. Asaeda, On a conjecture on Pythagorean numbers, ibid. 69 (1993), no. 7, 252–255.
- [19] —, —, On a conjecture on Pythagorean numbers, II, ibid. 69 (1993), no. 8, 287–290.
- [20] N. Terai, The Diophantine equation $a^x + b^y = c^z$, ibid. 70 (1994), 22–26.
- [21] —, The Diophantine equation $a^x + b^y = c^z$, II, ibid. 71 (1995), 109–110.
- [22] —, The Diophantine equation $a^x + b^y = c^z$, III, ibid. 72 (1996), 20–22.
- [23] S. Uchiyama, On the Diophantine equation $2^x = 3^y + 13^z$, Math. J. Okayama Univ. 19 (1976/77), 31–38.

[24] X. Z. Yang, On the Diophantine equation $a^x + b^y = c^z$, Sichuan Daxue Xuebao 4 (1985), 151–158 (in Chinese).

Department of Mathematics Harbin Institute of Technology Harbin 150001, P.R. China E-mail: zfcao@hope.hit.edu.cn

> Received on 21.9.1998 and in revised form on 7.5.1999

(3472)