Maohua Le

A note on the diophantine equation $x^2 + b^Y = c^z$

Czechoslovak Mathematical Journal, Vol. 56 (2006), No. 4, 1109–1116

Persistent URL: http://dml.cz/dmlcz/128133

Czechoslovak Mathematical Journal, 56 (131) (2006), 1109–1116

A NOTE ON THE DIOPHANTINE EQUATION $x^2 + b^Y = c^z$

Maohua Le, Guangdong

(Received May 19, 2003)

Abstract. Let a, b, c, r be positive integers such that $a^2 + b^2 = c^r$, $\min(a, b, c, r) > 1$, $\gcd(a, b) = 1, a$ is even and r is odd. In this paper we prove that if $b \equiv 3 \pmod 4$ and either b or c is an odd prime power, then the equation $x^2 + b^y = c^z$ has only the positive integer solution $(x, y, z) = (a, 2, r)$ with $\min(y, z) > 1$.

Keywords: exponential diophantine equation, Lucas number, positive divisor

MSC 2000: 11D61

1. Introduction

Let $\mathbb{Z}$, $\mathbb{N}$, $\mathbb{Q}$ be the sets of all integers, positive integers and rational numbers respectively. In 1933, Terai [10] proposed the following conjecture.

Conjecture 1. *If* (a, b, c) *is a primitive Pythagorean triple such that*

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

then the equation

$$x^2 + b^y = c^z, \quad x, y, z \in \mathbb{N}$$

has only the solutions $(x, y, z) = (a, 2, 2)$.

This problem is related to an early conjecture of Jeśmanowicz [5]. As an analogue of Conjecture 1, Cao and Dong [3] considered the following conjecture:

Supported by the National Natural Science Foundation of China (No. 10271104) and the Guangdong Provincial Natural Science Foundation (No. 04011425).

Conjecture 2. *If a, b, c, r, s, t are fixed positive integers such that*

$$a^x + b^t = c^r, \quad \min(a,b,c,r,s,t) > 1, \ \gcd(a,b) = 1, \ a \equiv 0 \pmod 2,$$

then the equation

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

has only the solutions $(x,y,z) = (a,t,r)$.

However, the condition $\min(y,z) > 1$ is necessary in Conjuecture 2 (see [4]). In general, this conjecture is far from solved. In this paper we consider the case that a, b, c, r are fixed positive integers satisfying

(1) $a^2 + b^2 = c^r, \quad \min(a,b,c,r) > 1, \ \gcd(a,b) = 1, \ a \equiv 0 \pmod 2, \ r \not\equiv 0 \pmod 2.$

In this respect, Cao, Dong and Li [4] proved that if

$$a = |V_r|, \quad b = |U_r|, \quad c = m^2 + 1 \tag{2}$$

and b is an odd prime power with $b \equiv 3 \pmod 4$, where m is an even integer with $m > 1$ and the integers $U(r), V(r)$ satisfy

$$V_r + U_r\sqrt{-1} = \left(m + \sqrt{-1}\right)^r, \tag{3}$$

then the equation

$$x^2 + b^y = c^z, \quad x,y,z \in \mathbb{N} \ \min(y,z) > 1 \tag{4}$$

has only the solution $(x,y,z) = (a,2,r)$. In this paper, we show that the condition (2) can be eliminated from the above mentioned result. We shall prove two general results:

Theorem 1. *If* (1) *holds and b is an odd prime power with $b \equiv 3 \pmod 4$, then* (4) *has only the solution $(x,y,z) = (a,2,r)$.*

Theorem 2. *If* (1) *holds, $b \equiv 3 \pmod 4$ and c is an odd prime power, then* (4) *has only the solution $(x,y,z) = (a,2,r)$.*

2. Proof of Theorem 1

Lemma 1 ([8, pp. 122–123])**.** *Let r be an odd integer with $r > 1$. Then every solution (X, Y, Z) of the equation*

$$X^2 + Y^2 = Z^r, \quad X, Y, Z \in \mathbb{N}, \ \gcd(X, Y) = 1, \ Y \equiv 0 \pmod 2$$

can be expressed as

$$X + Y\sqrt{-1} = \lambda_1\bigl(m + \lambda_2 l\sqrt{-1}\bigr)^r, \quad \lambda_1, \lambda_2 \in \{-1, 1\},$$
$$Z = m^2 + l^2, \quad m, l \in \mathbb{N}, \ \gcd(m, l) = 1, \ m \equiv 0 \pmod 2).$$

Lemma 2. *Let k be an odd integer with $k > 1$, and let $\omega(k)$ denote the number of distinct prime divisors of k. If the equation*

$$m^2 + l^2 = k, \quad m, l \in \mathbb{N}, \ \gcd(m, l) = 1, \ m \equiv 0 \pmod 2 \tag{5}$$

has solutions (m, l), then (5) has exactly $2^{\omega(k)-1}$ solutions (m, l).

P r o o f. This lemma follows directly from Lemma 1 of [7]. □

Lemma 3 ([6])**.** *The equation*

$$x^2 - 1 = Y^n, \quad X, Y, n \in \mathbb{N}, \ \min(X, Y, n) > 1$$

has only the solution $(X, Y, n) = (3, 2, 3)$.

Lemma 4 ([9])**.** *Let d is a positive square free integer with square free, and let $h(-d)$ denote the class number of the imaginary quadratic field $Q\bigl(\sqrt{-d}\bigr)$. If $d > 2$, then the equation*

$$1 + dX^2 = Y^n, \quad X, Y, n \in \mathbb{N}, \ Y \not\equiv 0 \pmod 2,$$
$$n > 1, \ n \not\equiv 0 \pmod 2, \ h(-d) \not\equiv 0 \pmod n$$

has no solutions (X, Y, n).

Lemma 5. *Let p be an odd integer with $p \equiv 3 \pmod 4$. The equation*

$$1 + 3X^2 = p^{2n}, \quad X, n \in \mathbb{N}, \ n \not\equiv 0 \pmod 2 \tag{6}$$

has only the solution $(p, X, n) = (7, 4, 1)$.

Proof. Since $h(-3) = 1$, by Lemma 4 we can suppose that $n = 1$ in (6). Then $(u, v) = (p, X)$ is a solution of the equation

$$u^2 - 3v^2 = 1, \quad u, v \in \mathbb{N}. \tag{7}$$

Since X is even and $2 + \sqrt{3}$ is the fundamental solution of (7), we get

$$p + X\sqrt{3} = \left(2 + \sqrt{3}\right)^{2t} = \left(7 + 4\sqrt{3}\right)^t, \quad t \in \mathbb{N}, \tag{8}$$

whence we obtain

$$p = \sum_{j=0}^{[n/2]} \binom{t}{2j} 7^{t-2j} 48^i. \tag{9}$$

Since $p \equiv 3 \pmod 4$, we see from (9) that t is odd. Hence, by (9), we get $t = 1$ and $p = 7$. Thus, (6) has only the solution $(p, X, n) = (7, 4, 1)$. The lemma is proved. □

Lemma 6 ([3, Lemma 1]). *Let b be an odd prime power, and let c be a positive integer with $\gcd(b, c) = 1$. If (4) has a solution (x, y, z) such that both y and z are even, then we have*

(i) $b = 239$, $c = 13$, $(x, y, z) = (28560, 2, 8)$.

(ii) $b^2 + 1 = 2c^2$, $(x, y, z) = (\frac{1}{2}(b^2 - 1), 2, 4)$.

(iii) $b^{2t} + 1 = 2c$, $(x, y, z) = (\frac{1}{2}(b^{2t} - 1), 2t, 4)$, *where t is a positive integer.*

Let α, β be algebraic integers. If $\alpha + \beta$ and $\alpha\beta$ are nonzero coprime integers and α/β is not a root of unity, then (α, β) is called a Lucas pair. Further, let $A = \alpha + \beta$ and $C = \alpha\beta$. Then we have

$$\alpha = \frac{1}{2}\left(A + \lambda\sqrt{B}\right), \quad \beta = \frac{1}{2}\left(A - \lambda\sqrt{B}\right), \quad \lambda \in \{-1, 1\},$$

where $B = A^2 - 4C$. The numbers of the pair (A, B) are called the parameters of the Lucas pair (α, β). Two Lucas pairs (α_1, β_1) and (α_2, β_2) are equivalent if $\alpha_1/\alpha_2 = \beta_1/\beta_2 = \pm 1$. Given a Lucas pair (α, β), one defines the corresponding sequence of Lucas numbers by

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

For equivalent Lucas pairs (α_1, β_1) and (α_2, β_2), we have $L_n(\alpha_1, \beta_1) = \pm L_n(\alpha_2, \beta_2)$ for any $n \geqslant 0$. A Prime p is called a primitive divisor of $L_t(\alpha, \beta)$ if $p \mid L_n$ and $BL_1 \ldots L_{n-1} \not\equiv 0 \pmod p$. A Lucas pair (α, β) such that $L_n(\alpha, \beta)$ has no primitive divisors will be called an n-defective Lucas pair. Further, a positive integer n is called totally non-defective if no Lucas pair is n-defective.

Lemma 7 ([11]). *Let n satisfy $4 < n \leqslant 30$ and $n \neq 6$. Then, up to equivalence, all parameters of n-defective Lucas pairs are given as follows:*

(i) $n = 5$, $(A, B) = (1, 5), (1, -7), (2, -40), (1, -11), (1, -15), (12, -76), (12, -1364)$.
(ii) $n = 7$, $(A, B) = (1, -7), (1, -19)$.
(iii) $n = 8$, $(A, B) = (2, -24), (1, -7)$.
(iv) $n = 10$, $(A, B) = (2, -8), (5, -3), (5, -47)$.
(v) $n = 12$, $(A, B) = (1, 5), (1, -7), (1, -11), (2, -56), (1, -15), (1, -19)$.
(vi) $n \in \{13, 18, 30\}$, $(A, B) = (1, -7)$.

Lemma 8 ([1, Theorem 1.4]). *If $n > 30$, then n is totally non-defective.*

Lemma 9. *If a, b, c, r satisfy* (1) *and b is an odd prime with $b \equiv 3 \pmod 4$, then either $(a, b, c, r) = (524, 7, 65, 3)$ or a, b, c and r satisfy* (2).

Proof. By Lemma 1, we get from (1) that

$$a + b\sqrt{-1} = \lambda_1 \bigl(m + \lambda_2 l \sqrt{-1}\bigr)^r, \quad \lambda_1, \lambda_2 \in \{-1, 1\}, \tag{10}$$

$$c = m^2 + l^2, \ m, l \in \mathbb{N}, \ \gcd(m, l) = 1, \ m \equiv 0 \pmod 2. \tag{11}$$

From (10), we obtain

$$b = \lambda_1 \lambda_2 l \sum_{i=0}^{(r-1)/2} \binom{r}{2i+1} m^{m-2i-1} (-l^2)^i. \tag{12}$$

Since b is an odd prime power with $b \equiv 3 \pmod 4$, we have

$$b = p^k, \tag{13}$$

where p is an odd prime and k is an odd integer. By (12) and (13), we get

$$l = p^s, \quad \Bigl| \sum_{i=0}^{(r-1)/2} \binom{r}{2i+1} m^{r-2i-1} (-l^2)^i \Bigr| = p^{k-s}, \quad s \in \mathbb{Z}, \ 0 \leqslant s \leqslant k. \tag{14}$$

By (3), (10), (11) and (14), if $s = 0$, then a, b, c, r satisfy (2). If $s > 0$, let

$$\alpha = m + l\sqrt{-1}, \quad \beta = m - l\sqrt{-1}. \tag{15}$$

Then (α,β) is a Lucas pair with parameters $(2m,-4l^2)$. Further, let $L_n(\alpha,\beta)$ $(n\geqslant 0)$ denote the corresponding Lucas numbers. Then, by (14), we get

$$l=p^s,\quad |L_r(\alpha,\beta)|=p^{k-s},\quad 0<s\leqslant k. \tag{16}$$

It implies that the Lucas number $L_r(\alpha,\beta)$ has no primtitive divisors. Since r is an odd integer with $r>1$, by Lemmas 7 and 8 we obtain $r=3$.

When $r=3$ and $s=k$, we get from (14) that

$$p^{2s}-3m^2=1. \tag{17}$$

Since $b\equiv 3 \pmod 4$, we see from (13) that $p\equiv 3 \pmod 4$. Hence, by Lemma 5, we get from (17) that $p=7$, $s=1$ and $m=4$. Therefore, by (10) and (11), we abtain $(a,b,c,r)=(524,7,65,3)$.

When $r=3$ and $s<k$, since $s>0$ and $\gcd(m,l)=1$, we get from (14) that $p=3$, $k-s=1$ and

$$m^2-3^{2s-1}=1. \tag{18}$$

By Lemma 3, we find from (18) that $m=2$ and $s=1$. Hence, by (13), we get $b=3^2=9$. But, since $b\equiv 3 \pmod 4$, this is impossible. Thus the lemma is proved. □

P r o o f of Theorem 1. Since $b\equiv 3 \pmod 4$, by Theorem of [4] and our Lemma 9 it suffices to prove the theorem for $(a,b,c,r)=(524,7,65,3)$. Then (4) can be written as

$$x^2+7^y=65^z,\quad x,y,z\in\mathbb{N},\ \min(y,z)>1. \tag{19}$$

Let (x,y,z) be a solution of (19) with $(x,y,z)\neq(524,2,3)$. By Lemma 6, we have $y\equiv 0 \pmod 2$ and $z\not\equiv 0 \pmod 2$. Hence, by Lemma 1, we get

$$x+7^{y/2}\sqrt{-1}=\lambda_1\big(m+\lambda_2 l\sqrt{-1}\big)^z,\quad \lambda_1,\lambda_2\in\{-1,1\}, \tag{20}$$

$$65=m^2+l^2,\quad m,l\in\mathbb{N},\ \gcd(m,l)=1,\ m\equiv 0 \pmod 2. \tag{21}$$

Since $\omega(65)=2$, by Lemma (2), (21) has exactly two solutions $(m,l)=(4,7)$ and (8,1).

When $(m,l)=(4,7)$, let

$$\alpha=4+7\sqrt{-1},\quad \beta=4-7\sqrt{-1}. \tag{22}$$

Then (α, β) is a Lucas pair with parameters $(8, 196)$. Further, let $L_n(\alpha, \beta)$ $(n \geqslant 0)$ denote the corresponding Lucas numbers. Then, from (20) and (22) we get

$$7^{y/2-1} = |L_z(\alpha, \beta)|. \tag{23}$$

This implies that the Lucas number $L_z(\alpha, \beta)$ has no primtitive divisors. On the other hand, since $z > 1$ and $(x, y, z) \neq (524, 2, 3)$, we see from (20) that $z > 3$. But, by Lemmas 7 and 8, (23) is impossible.

When $(m, l) = (8, 1)$, we get from (20) that

$$7^{y/2} = \lambda_1 \lambda_2 \sum_{i=0}^{(z-1)/2} (-1)^i \binom{z}{2i+1} 8^{z-2i-1}. \tag{24}$$

Since $8 \equiv 1 \pmod 7$ and

$$\begin{aligned} \sum_{i=0}^{(z-1)/2} (-1)^i \binom{z}{2i+1} &= \sum_{j=0}^{z} \binom{z}{j} \sin \frac{j\pi}{2} \\ &= 2^z \sin \frac{z\pi}{4} \left(\cos \frac{\pi}{4}\right)^z = (-1)^{(z-1)(z+5)/8} 2^{(z-1)/2}, \end{aligned} \tag{25}$$

by (24), we obtain $0 \equiv \pm 2^{(z-1)/2} \pmod 7$, a contradiction. Thus, (4) has only the solution $(x, y, z) = (524, 2, 3)$ for $(a, b, c, r) = (524, 7, 65, 3)$. The theorem is proved. □

3. Proof of Theorem 2

Lemma 10 ([2, Theorem 4]). *Let D be a positive integer with $D > 2$, and let p be an odd prime with $D \not\equiv 0 \pmod p$. If $(D, p) = (3s^2 + 1, 4s^2 + 1)$, where s is a positive integer, then the equation*

$$X^2 + D^Y = p^z, \quad X, Y, Z \in \mathbb{N} \tag{26}$$

has at most three solutions $(X, Y, Z) = (s, 1, 1)$, $(8s^2 + 3s, 1, 3)$ and (X_3, Y_3, Z_3), where Y_3 is even. Otherwise, (26) has at most two solutions (X, Y, Z). Further, if these are (X_1, Y_1, Z_1) and (X_2, Y_2, Z_2), then $Y_1 \equiv Y_2 \pmod 2$.

P r o o f of Theorem 2. Since c is an odd prime power, we have $c = p^t$, where p is an odd prime and t is a positive integer. Hence, if (x, y, z) is a solution of (4), then $(X, Y, Z) = (x, y, tz)$, is a solution of the equation

$$X^2 + b^Y = p^Z, \quad X, Y, Z \in \mathbb{N}. \tag{27}$$

Since $b \equiv 3 \pmod 4$, hence if (4) has a solution $(x, y, z) \neq (a, 2, r)$, then (27) has at least two solutions (X, Y, Z) with $Y \equiv 0 \pmod 2$. But, by Lemma 10, this is impossible. Thus, the theorem is proved. □

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. *539* (2001), 75–122.

[2] *Y. Bugeaud*: On some exponential diophantine equations. Monatsh. Math. *132* (2001), 93–97.

[3] *Z.-F. Cao and X.-L. Dong*: The diophantine equation $a^2 + b^y = c^z$. Proc. Japan Acad. *77A* (2001), 1–4.

[4] *Z.-F. Cao, X.-L. Dong and Z. Li*: A new conjecture concerning the diophantine equation $x^2 + b^y = c^z$. Proc. Japan Acad. *78A* (2002), 199–202.

[5] *L. Jeśmanowicz*: Several remarks on Pythagorean number. Wiadom. Mat. *1* (1955/1956), 196–202. (In Polish.)

[6] *C. Ko*: On the diophantine equation $x^2 = y^n + 1, xy \neq 0$. Sci.Sin. *14* (1964), 457–460.

[7] *M.-H. Le*: A note on Jeśmanowicz' conjecture. Colloq. Math. *64* (1995), 47–51.

[8] *L. J. Mordell*: Diophantine Equations. Academic Press, London, 1969.

[9] *T. Nagell*: Sur I'impossibilité de quelques equation á deux indéterminées. Norsk Matem. Forenings Skrifter *13* (1921), 65–82.

[10] *N. Terai*: The diophantine equation $x^2 + q^m = p^n$. Acta Arith. *63* (1993), 351–358.

[11] *P. Voutier*: Primitive divisors of Lucas and Lehmer sequences. Math. Comp. *64* (1995), 869–888.

Author's address: Department of Mathematics, Zhanjiang Normal College, Zhanjiang, Guangdong, P. R. China.