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

By Maohua Le

Department of Mathematics, Zhanjing Normal College
29 Cunjin Road, Chikan Zhanjing, Guangdong, P. R. China

(Communicated by Shokichi Iyanaga, M. J. A., April 12, 2004)

Abstract: Let a, b, c be fixed coprime positive integers. In this paper we prove that if $b \equiv 3 \pmod 4$, $a \equiv -1 \pmod{b^{2l}}$, $a^2 + b^{2l-1} = c$ and c is odd, where l is a positive integer, then the equation $a^x + b^y = c^z$ has only the positive integer solution $(x, y, z) = (2, 2l-1, 1)$.

Key words: Exponential diophantine equations; primitive divisors of Lucas numbers.

1. Introduction. Let $\mathbf{Z}$, $\mathbf{N}$ be the sets of all integers and positive integers respectively. Let a, b, c be fixed coprime positive integers. Recently, using the theory of linear forms in logarithms, Terai [7] proved that if b is a prime with $b \equiv 3 \pmod 4$, $a \equiv -1 \pmod{b^{2l}}$, $a^2 + b^{2l-1} = c$ and c is odd, where $l \in \{1, 2\}$, then the equation

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

has only the solution $(x, y, z) = (2, 2l-1, 1)$. In this paper, by means of different approach, we shall show that the conditions b is a prime and $l \in \{1, 2\}$ can be eliminated from the above-mentioned result. We prove a general result as follows:

Theorem. *Let l be a positive integer. If $b \equiv 3 \pmod 4$, $a \equiv 1 \pmod{b^{2l}}$, $a^2 + b^{2l-1} = c$ and c is odd, then* (1) *has only the solution* $(x, y, z) = (2, 2l-1, 1)$.

2. Preliminaries.

Lemma 1 ([2, 3]). *The equation $X^2 + 3^{2m+1} = Y^n$, $X, Y, m, n \in \mathbf{Z}$, $X > 0$, $Y > 0$, $\gcd(X, Y) = 1$, $m \geq 0$, $n > 1$ has only the solution $(X, Y, m, n) = (10, 7, 2, 3)$ with n an odd prime.*

Let D be a positive integer, and let $\mathrm{h}(-4D)$ denote the class number of positive binary quadratic forms of discriminant $-4D$.

Lemma 2. *Let k be an odd integer with $\gcd(D, k) = 1$. If $D > 3$, then every solution (X, Y, Z) of the equation*

$$X^2 + DY^2 = k^Z, \quad X, Y, Z \in \mathbf{Z},$$
$$\gcd(X, Y) = 1, \quad Z > 0$$

can be expressed as

$$Z = Z_1 t, \quad t \in \mathbf{N},$$
$$X + Y\sqrt{-D} = \lambda_1 (X_1 + \lambda_2 Y_1 \sqrt{-D})^t,$$
$$\lambda_1 \lambda_2 \in \{1, -1\},$$

where X_1, Y_1, Z_1 are positive integers satisfying

$$X_1^2 + DY_1^2 = k^{Z_1}, \quad \gcd(X_1, Y_1) = 1,$$
$$\mathrm{h}(-4D) \equiv 0 \pmod{Z_1}.$$

Proof. This lemma is the special case of [6, Theorems 1 and 2] for $D_1 = 1$ and $D_2 < 3$. □

Lemma 3 ([5, Theorems 12.10.1 and 12.14.3]). *For any positive integer D, we have*

$$\mathrm{h}(-4D) < \frac{4\sqrt{D}}{\pi} \log(2e\sqrt{D}).$$

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

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

where $B = A^2 - 4C$. We call (A, B) 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

$$L_s(\alpha, \beta) = \frac{\alpha^s - \beta^s}{\alpha - \beta}, \quad s = 0, 1, 2, \cdots.$$

For equivalent Lucas pairs (α_1, β_1) and (α_2, β_2), we have $L_s(\alpha_1, \beta_1) = \pm L_s(\alpha_2, \beta_2)$ for any $s \geq 0$. A prime p is called a primitive divisor of $L_s(\alpha, \beta)$ ($s > 1$) if

$$p \mid L_s(\alpha, \beta) \quad \text{and} \quad p \nmid BL_1(\alpha, \beta) \cdots L_{s-1}(\alpha, \beta).$$

2000 Mathematics Subject Classification. 11D61.

A Lucas pair (α, β) such that $L_s(\alpha, \beta)$ has no primitive divisors will be called a s-defective Lucas pair. Further, a positive integer s is called totally non-defective if no Lucas pair is s-defective.

Lemma 4 ([8]). *Let s satisfy $4 < s \le 30$ and $s \neq 6$. Then, up to equivalence, all parameters of s-defective Lucas pairs are given as follows*:

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

Lemma 5 ([1]). *If $s > 30$, then s is totally non-defective.*

3. Proof of theorem. Let (x, y, z) be a solution of (1) with $(x, y, z) \neq (2, 2l-1, 1)$. Since $a \equiv -1 \pmod{b}$ and $c \equiv a^2 \equiv 1 \pmod{b}$, we see from (1) that x must be even. Since $b \equiv 3 \pmod{4}$ and c is odd, we see from $a^2 + b^{2l-1} = c$ that a is even and $c \equiv 3 \pmod{4}$. Hence, by (1), we get $y \equiv z \pmod{2}$. Further, since $c \equiv 3 \pmod{4}$, we conclude that $y \equiv z \equiv 1 \pmod{2}$ by (1). It implies that y and z are both odd. Hence, by Lemma 1, we may assume that b is not a power of 3.

Since $a \equiv -1 \pmod{b^{2l}}$ and $a^2 + b^{2l-1} = c$, we have $c \equiv 1 + b^{2l-1} \pmod{b^{2l}}$. Hence, by (1), we get $1 + b^y \equiv 1 \pmod{b^{2l-1}}$ and $y \ge 2l - 1$. If $y = 2l - 1$, then from (1) we get

$$1 + b^{2l-1} \equiv (1 + b^{2l-1})^z \pmod{b^{2l}}, \tag{2}$$

whence we obtain

$$z - 1 \equiv 0 \pmod{b}. \tag{3}$$

Further, since $y = 2l - 1$ and $(x, y, z) \neq (2, 2l-1, 1)$, we have $z > 1$. Therefore, by (3), we get

$$z - 1 \ge b. \tag{4}$$

If $y > 2l - 1$, then from (1) we get

$$1 \equiv (1 + b^{2l-1})^z \pmod{b^{2l}}. \tag{5}$$

It implies that $z \equiv 0 \pmod{b}$ and

$$z \ge b. \tag{6}$$

Therefore, by (4), (6) holds for any case.

Since $b > 3$ and y is odd, we find from (1) that $(X, Y, Z) = (a^{x/2}, b^{(y-1)/2}z)$ is a solution of the equation

$$X^2 + bY^2 = c^Z, \quad X, Y, Z \in \mathbf{Z}, \quad \gcd(X, Y) = 1, \quad Z > 0. \tag{7}$$

Since c is odd, by Lemma 2, we obtain

$$z = Z_1 t, \quad t \in \mathbf{N}, \tag{8}$$

$$a^{x/2} + b^{(y-1)/2}\sqrt{-b} = \lambda_1 (X_1 + \lambda_2 Y_1 \sqrt{-b})^t, \quad \lambda_1 \lambda_2 \in \{1, -1\}, \tag{9}$$

where X_1, Y_1, Z_1 are positive integers satisfying

$$X_1^2 + bY_1^2 = c^{Z_1}, \quad \gcd(X_1, Y_1) = 1, \quad \mathrm{h}(-4b) \equiv 0 \pmod{Z_1}. \tag{10}$$

Moreover, since z is odd, we see from (8) that t must be odd.

Let

$$\alpha = X_1 + Y_1\sqrt{-b}, \quad \beta = X_1 - Y_1\sqrt{-b}. \tag{11}$$

By (10) and (11), we have

$$\alpha + \beta = 2X_1, \quad \alpha\beta = c^{Z_1}, \quad \frac{\alpha}{\beta} = \frac{1}{c^{Z_1}}\left((X_1^2 - bY_1^2) + 2X_1Y_1\sqrt{-b}\right). \tag{12}$$

Since $\gcd(X_1, Y_1) = \gcd(b, c) = 1$, we observe from (12) that $\alpha + \beta$ and $\alpha\beta$ are nonzero coprime integers and α/β is not a root of unity. Hence, (α, β) is a Lucas pair with parameters $(2X_1, -4bY_1^2)$. Further, let $L_s(\alpha, \beta)$ $(s = 0, 1, 2, \cdots)$ denote the corresponding Lucas numbers. By (9) and (11), we get

$$b^{(y-1)/2} = Y_1 |L_t(\alpha, \beta)|. \tag{13}$$

We find from (13) that the Lucas number $L_t(\alpha, \beta)$ has no primitive divisors. Therefore, by Lemma 5, we get $t \le 30$. Further, it is easy to remove all cases in Lemma 4 and conclude that $t \le 4$. So we have $t \in \{1, 3\}$.

When $t = 1$, we get from (8) and (10) that $z = Z_1$ and $\mathrm{h}(-4b) \equiv 0 \pmod{z}$. It implies that $\mathrm{h}(-4b) \ge z$. Further, by (6),

$$\mathrm{h}(-4b) \ge b. \tag{14}$$

By Lemma 3, we see from (14) that

$$b < \frac{4\sqrt{b}}{\pi}\log(2e\sqrt{b}), \tag{15}$$

whence we conclude that $b < 19$. Recall that $b \equiv 3 \pmod{4}$ and b is not a power of 3. We have $b \in \{7, 11, 15\}$. But, (14) is impossible, since $\mathrm{h}(-4 \cdot 7) = 1$, $\mathrm{h}(-4 \cdot 11) = 3$ and $\mathrm{h}(-4 \cdot 15) = 2$.

When $t = 3$, we get from (9) that

$$b^{(y-1)/2} = \lambda_1 \lambda_2 Y_1 (3X_1^2 - bY_1^2). \tag{16}$$

Let $d = \gcd(Y_1, 3X_1^2 - bY_1^2)$. Since $\gcd(X_1, Y_1) = 1$, we have $d = 1$ or 3. Notice that $\gcd(b, c) = 1$ and $\gcd(b, X_1) = 1$ by (10). If $d = 1$ and b is a power of prime, then $b \neq$ a power of 3 and $\gcd(b, 3X_1^2 - bY_1^2) = 1$. Hence, from (16) we get $Y_1 = b^{(y-1)/2}$ and

$$3X_1^2 - b^y = 1, \tag{17}$$

since $b^y \equiv 3 \pmod 4$. Recall that $c \equiv 1 \pmod b$. We get from (10) and (17) that $X_1^2 \equiv 1 \pmod b$ and $3X_1^2 \equiv 1 \pmod b$, respectively. It implies that $3 \equiv 1 \pmod b$, a contradiction. If $d = 3$, then $3 \mid b$, by (16). Since b is not a power of 3, b has at least two distinct prime divisors. Therefore when $d = 1$ and $b \neq a$ power of prime or $d = 3$, by the genus theory of binary quadratic forms (see [4, Section 48]), we have $\mathrm{h}(-4b) \equiv 0 \pmod 2$. Further, by (8) and (10), we get $z = 3Z_1$ and $\mathrm{h}(-4b) \equiv 0 \pmod{2z/3}$. It follows that

$$\mathrm{h}(-4b) \geq \frac{2}{3} b, \tag{18}$$

by (6). Further, by Lemma 3, we obtain from (18) that

$$\frac{2}{3} b < \frac{4\sqrt{b}}{\pi} \log(2e\sqrt{b}), \tag{19}$$

whence we conclude that $b \leq 51$, since $3 \mid b$ for $d = 3$, we have $b \in \{15, 35, 39, 51\}$. But, (18) is impossible, since $\mathrm{h}(-4 \cdot 15) = 2$, $\mathrm{h}(-4 \cdot 35) = 2$, $\mathrm{h}(-4 \cdot 39) = 4$ and $\mathrm{h}(-4 \cdot 51) = 6$. To sum up, the theorem is proved.

Acknowledgements. This paper was supported by the National Natural Science Foundation of China (No. 10271104), the Guangdong Provincial Natural Science Foundation (No. 011781) and the Natural Science Foundation of the Education Department of Guangdong Province (No. 0161). The author would like to thank the referees for their valuable suggestions.

References

[1] Bilu, Y., Hanrot, G., and Voutier, P. M.: Existence of primitive divisors of Lucas and Lehmer numbers. With an appendix by M. Mignotte. J. Reine Angew. Math., **539**, 75–122 (2001).

[2] Brown, E.: Diophantine equations of the form $x^2 + D = y^n$. J. Reine Angew. Math., **274/275**, 385–389 (1975).

[3] Brown, E.: Diophantine equations of the form $ax^2 + Db^2 = y^p$. J. Reine Angew. Math., **291**, 118–127 (1977).

[4] Hecke, E.: Vorlesungen uber die Theorie der algebraischen Zahlen. Akademische Verlagsgesellschaft, Leipzig (1923).

[5] Hua, L.-K.: Introduction to Number Theory. Springer Verlag, Berlin (1982).

[6] Le, M.-H.: Some exponential diophantine equations I. The equation $D_1 x^2 - D_2 y^2 = \lambda k^2$. J. Number Theory, **55**, 209–221 (1995).

[7] Terai, N: On the exponential diophantine equation $a^x + l^y = c^z$. Proc. Japan Acad., **77A**, 151–154 (2001).

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