ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 37, Number 4, 2007

ON THE DIOPHANTINE EQUATION $y^x - x^y = z^{2*}$

MAOHUA LE

ABSTRACT. In this paper we prove that the equation $y^x - x^y = z^2$, $\min(x, y) > 1$, $\gcd(x, y) = 1$, has no positive integer solutions (x, y, z) with xy odd.

1. Introduction. Let $\mathbf{Z}, \mathbf{N}$ be the sets of all integers and positive integers, respectively. Recently, using a combination of lower bounds of linear forms in p-adic and archimedian logarithms, Luca and Mignotte [**4**] proved that the equation

$$(1) \qquad y^x - x^y = z^2, \quad x, y, z \in \mathbf{N}, \quad \min(x, y) > 1, \quad \gcd(x, y) = 1$$

has only the solution $(x, y, z) = (2, 3, 1)$ with xy even. This equation is related to a special case of the famous Catalan's equation. In addition, the authors of [**4**] showed that they have no idea how to solve (1) when xy is odd. In this paper we completely solve this problem as follows.

Theorem. *The equation* (1) *has no solutions* (x, y, z) *with* xy *odd.*

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

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

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

can be expressed as

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

2000 AMS *Mathematics subject classification.* Primary 11D61.
Keywords and phrases. Exponential diophantine equations.
Supported by the National Natural Science Foundation of China (No. 10271104) and the Guangdong Provincial Natural Science Foundation (No. 06029035).
Received by the editors on April 17, 2003, and in revised form on July 21, 2003.

where X_1, Y_1, Z_1 are positive integers satisfying

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

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

Lemma 2 [**2**, Theorems 12.10.1 and 12.14.3]. *For any positive integer D, we have*

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

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

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

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 $n \geq 0$. A prime p is called a primitive divisor of $L_n(\alpha, \beta)$, $n > 1$, if

$$p \mid L_n(\alpha, \beta) \quad \text{and} \quad p \nmid bL_1(\alpha, \beta) \cdots L_{n-1}(\alpha, \beta).$$

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 nondefective if no Lucas pair is n-defective.

Lemma 3 [**5**]. *Let n satisfy $4 < n \leq 30$ 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 4 [**1**]. *If $n > 30$, then n is totally nondefective.*

3. Proof of the theorem. Let (x,y,z) be a solution of (1) with xy odd. Since $\min(x,y) > 1$ and $\gcd(x,y) = 1$, we have $x > y > 1$, $x \geq 5$ and $y \geq 3$.

Since x and y are both odd, we see from (1) that $(X,Y,Z) = (z, x^{(y-1)/2}, x)$ is a solution of (2) for $D = x$ and $k = y$. Therefore, by Lemma 1, we get

$$x = Z_1 t, \quad t \in \mathbf{N}, \tag{3}$$

$$z + x^{(y-1)/2}\sqrt{-x} = \lambda_1(X_1 + \lambda_2 Y_1\sqrt{-x}\,)^t, \quad \lambda_1, \lambda_2 \in \{1,-1\}, \tag{4}$$

where X_1, Y_1, Z_1 are positive integers satisfying

$$X_1^2 + xY_1^2 = y^{Z_1}, \quad \gcd(X_1,Y_1) = 1, \quad h(-4x) \equiv 0 \pmod{Z_1}. \tag{5}$$

Let

$$\alpha = X_1 + Y_1\sqrt{-x}, \quad \beta = X_1 - Y_1\sqrt{-x}. \tag{6}$$

By (5) and (6), we get

$$\begin{aligned} &\alpha + \beta = 2X_1, \quad \alpha\beta = y^{Z_1}, \\ &\frac{\alpha}{\beta} = \frac{1}{y^{Z_1}}\,((X_1^2 - xY_1^2) + 2X_1Y_1\sqrt{-x}\,). \end{aligned} \tag{7}$$

Since $\gcd(X_1,Y_1) = \gcd(x,y) = 1$, we observe from (7) 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 $(2X_1, -4xY_1^2)$. Further, let $L_n(\alpha, \beta)$, $n = 0, 1, 2, \ldots$, denote the corresponding Lucas numbers. By (4) and (6), we get

$$x^{(y-1)/2} = Y_1 |L_t(\alpha, \beta)|. \tag{8}$$

We find from (8) that the Lucas number $L_t(\alpha, \beta)$ has no primitive divisors. Therefore, by Lemma 4, we obtain $t \leq 30$. Since x is odd, t is also odd and by Lemma 3 we see that $t \in \{1, 3\}$. Thus, by (3) and (5), we obtain either

$$h(-4x) \equiv 0 \pmod{x} \tag{9}$$

or

$$h(-4x) \equiv 0 \left(\operatorname{mod} \frac{x}{3}\right). \tag{10}$$

By Lemma 2, if (9) holds, then $h(-4x) \geq x$ and

$$x < \frac{4\sqrt{x}}{\pi} \log(2e\sqrt{x}), \tag{11}$$

whence we conclude that $x \leq 17$. But (9) is impossible if x is an odd integer with $5 \leq x \leq 17$.

By (3) and (5), if (10) holds, then $3 \mid x$. When x is a power of 3, we have $x = 3^r$, where r is a positive integer with $r > 1$. Since $h(-12) = 1$ and $h(-36) = 2$, by [**2**, Theorems 12.10.1 and 12.10.2], we get

$$h(-4 \cdot 3^r) = \begin{cases} 2 \cdot 3^{r/2-1} & \text{if } r \text{ is even}, \\ 3^{(r-1)/2} & \text{if } r \text{ is odd}. \end{cases} \tag{12}$$

We see from (12) that (10) is false if $x = 3^r$ and $r > 1$. When x is not a power of 3, x has at least two distinct odd prime divisors, since $3 \mid x$. By the genus theory of binary quadratic forms, we have $2 \mid h(-4x)$. Therefore, by Lemma 2, we get from (10) that

$$\frac{2}{3} x < \frac{4\sqrt{\pi}}{\pi} \log(2e\sqrt{x}), \tag{13}$$

whence we conclude that $x \leq 51$. Notice that $h(-4 \cdot 15) = 2$, $h(-4 \cdot 21) = 4$, $h(-4 \cdot 33) = 4$, $h(-4 \cdot 39) = 4$, $h(-4 \cdot 45) = 4$ and $h(-4 \cdot 51) = 6$. It implies that (10) is false if $x \leq 51$, $3 \mid x$ and x is not a power of 3. To sum up, the theorem is proved. $\square$

REFERENCES

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

2. L.-K. Hua, *Introduction to number theory*, Springer-Verlag, Berlin, 1982.

3. M.-H. Le, *Some exponential diophantine equations* I: *The equation* $D_1x^2 - D_2y^2 = \lambda k^2$, J. Number Theory **55** (1995), 209–221.

4. F. Luca and M. Mignotte, *On the equation* $y^x \pm x^y = z^2$, Rocky Mountain J. Math. **30** (2000), 651–661.

5. P.M. Voutier, *Primitive divisors of Lucas and Lehmer sequences*, Math. Comput. **64** (1995), 869–888.

Department of Mathematics, Zhanjiang Normal College, 29 Cunjin Road, Chikan Zhanjing, Guangdong, P.R. China
E-mail address: `lmhhhh2006@163.com`