第27卷第2期 数 学 研 究 与 评 论 Vol.27, No.2
2007年5月 JOURNAL OF MATHEMATICAL RESEARCH AND EXPOSITION May, 2007

Article ID: 1000-341X(2007)02-0236-05 **Document code**: A

On the Exponential Diophantine Equation $x^2 + (3a^2 - 1)^m = (4a^2 - 1)^n$

HU Yong-zhong

(Department of Mathematics, Foshan University, Guangdong 528000, China)

(E-mail: fsyzhujx@pub.foshan.gd.cn)

Abstract: We apply a new, deep theorem of Bilu, Hanrot & Voutier and some fine results on the representation of the solutions of quadratic Diophantine equations to solve completely the exponential Diophantine equation $x^2 + (3a^2 - 1)^m = (4a^2 - 1)^n$ when $3a^2 - 1$ is a prime or a prime power.

Key words: exponential Diophantine equations ; Lucas sequences; primitive divisors; Kronecker symbol.

MSC(2000): 11D25; 11D61

CLC number: O156

1. Introduction

Diophantine equations of the type

$$D_1 x^2 + D_2^m = ck^n, \quad \gcd(D_1, D_2) = 1, \quad c \in \{1, 2, 4\}, \tag{1}$$

where D_1, D_2, x, m, c, k, n are positive integers with $\gcd(D_1 D_2, k) = 1$, have been considered by several authors[2,3,5−7]. Thanks to a new deep result of Bilu, Hanrot & Voutier[1], Yann Bugeaud[2] proved the following:

Theorem BGD *Let $D > 2$ be an integer and let p be an odd prime which does not divide D. If there exists a positive integer a with $D = 3a^2 + 1$ and $p = 4a^2 + 1$, then the Diophantine equation*

$$x^2 + D^m = p^n, \quad \text{in positive integers } x, m \text{ and } n, \tag{2}$$

has at most three solutions (x, m, n), namely, $(a, 1, 1), (8a^3+3a, 1, 3), (x_3, m_3, n_3)$, with m_3 (if the third solution exists) even. Otherwise, the Diophantine equation (2) has at most two solutions.

We[9,10] have already applied the main result of [1] and improved Yann Bugeaud's result by proving that if $a > 1$ and either $4a^2 + 1$ or $3a^2 + 1$ is a prime, then the only positive integer solutions of the Diophantine equation

$$x^2 + (3a^2 + 1)^m = (4a^2 + 1)^n \tag{3}$$

Received date: 2005-04-29; **Accepted date**: 2006-12-10

Foundation item: the Natural Science Foundation of Guangdong Province (04009801); the Important Science Research Foundation of Foshan University.

are $(x,m,n)\in\{(a,1,1),\,(8a^3+3a,1,3)\}$.

In this paper, we use the same idea and some fine results on the representation of the solutions of quadratic Diophantine equations to solve completely the exponential Diophantine equations

$$x^2+(3a^2-1)^m=(4a^2-1)^n \ \text{ in integers } \ x>0, m>0, n>0 \tag{4}$$

when $3a^2-1$ is an odd prime or a prime power.

Theorem *Let $a>1$ and $3a^2-1$ be a prime (therefore a is even). Then the only solutions of Diophantine equation (4) are $(x,m,n)\in\{(a,1,1),(8a^3-3a,1,3)\}$.*

Remark We have excluded the case $3a^2-1=2$ or $3a^2-1$ is a power of 2, since the Diophantine equation $x^2+2^m=y^n$, in positive integers x,m,y and $n>2$, has been solved[3].

2. Some lemmas

Definition 1 *A Lucas pair is a pair $(\alpha,\,\beta)$ of algebraic integers such that $(\alpha+\beta)$ and $\alpha\beta$ are non-zero coprime rational integers and α/β is not a root of unity. For a given Lucas pair (α,β), one defines the corresponding sequence of Lucas numbers by*

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

Definition 2 *Let (α,β) be a Lucas pair. The prime number p is a primitive divisor of the Lucas number $u_n(\alpha,\beta)$ if p divides $u_n(\alpha,\beta)$ but does not divide $(\alpha-\beta)^2u_1\cdots u_{n-1}$.*

One of the key arguments for our proof is the result obtained by Bilu, Hanrot & Voutier[1].

Theorem BHV *For any integer $n>30$, every n-th term of any Lucas sequence has a primitive divisor. Further, for any positive integer $n\le 30$, all Lucas sequence whose n-th term has no primitive divisor are explicitly determined.*

Lemma 1[12] *For any odd positive integer n $(5\le n\le 30)$, all Lucas sequence whose n-th term $u_n(\alpha,\beta)$ has no primitive divisor are given as follows:*

$$\begin{aligned}
n=5,(\alpha,\beta)=\;&(\pm\frac{1\pm\sqrt{5}}{2},\pm\frac{1\mp\sqrt{5}}{2}),(\pm\frac{1\pm\sqrt{-7}}{2},\pm\frac{1\mp\sqrt{-7}}{2}),(\pm\frac{1\pm\sqrt{-15}}{2},\pm\frac{1\mp\sqrt{-15}}{2}),\\
&(\pm(6\pm\sqrt{-19}),\pm(6\mp\sqrt{-19})),(\pm(1\pm\sqrt{-10}),\pm(1\mp\sqrt{-10})),\\
&(\pm\frac{1\pm\sqrt{-11}}{2},\pm\frac{1\mp\sqrt{-11}}{2}),(\pm(6\pm\sqrt{-341}),\pm(6\mp\sqrt{-341}));\\
n=7,(\alpha,\beta)=\;&(\pm\frac{1\pm\sqrt{-7}}{2},\pm\frac{1\mp\sqrt{-7}}{2}),(\pm\frac{1\pm\sqrt{-19}}{2},\pm\frac{1\mp\sqrt{-19}}{2});\\
n=13,(\alpha,\beta)=\;&(\pm\frac{1\pm\sqrt{-7}}{2},\pm\frac{1\mp\sqrt{-7}}{2}).
\end{aligned}$$

We do not state here the complete list of the n-th term of Lucas sequences without primitive divisor and we refer the readers to [12].

Lemma 2[8] *The only positive integer solution of the equation $2z^2=x^4+y^4$, $\gcd(x,y)=1$ is $x=y=1$.*

The following two lemmas are certainly known, but we have never seen a complete proof in available literature before. Recently, Yuan has given a complete proof in [11].

Lemma 3[11] *Let $D \notin \{1,3\}$ be a square-free positive integer. The solutions of equation*

$$X^2 + DY^2 = P^n \quad X, Y, n \in Z, \gcd(X, DY) = 1, 2 \not| P, n > 0 \tag{5}$$

can be put into at most $2^{\omega(P)-1}$ classes. Further, in each such class S, there is a unique solution (X_1, Y_1, n_1) such that $X_1 > 0, Y_1 > 0$ and n_1 is minimal among the solutions of S. Moreover, every solution (X_2, Y_2, n_2) of (4) belonging to S can be expressed as

$$n_2 = n_1 t, (X_2 + Y_2\sqrt{-D}) = \pm(X_1 \pm Y_1\sqrt{-D})^t,$$

where $t > 0$ is an integer, and $\omega(P)$ denotes the number of distinct prime factors of P.

Lemma 4[11] *(a) For all (X, Y, n) belonging to the same class, there is a unique rational integer l satisfying*

$$l^2 \equiv -D \pmod P, X \equiv \pm lY \pmod P, 0 < l \leq \frac{P}{2}. \tag{6}$$

(b) For distinct classes, the rational integer l as claimed in (a) is distinct.

Lemma 5[13] *The only solution of the equation $x^2 + 1 = 2y^n$, $x, y, n \in N$, $2 \nmid n$, $n > 1$ is $x = y = 1$.*

3. Proof of the theorem

Proof Let (x, m, n) be a solution of (4). We divide the proof into three cases.

First, we consider the case that $2|n$. By (4), we have

$$[(4a^2-1)^{\frac{n}{2}} - x][(4a^2-1)^{\frac{n}{2}} + x] = (3a^2-1)^m.$$

Noting $3a^2 - 1$ is prime, therefore, $(4a^2-1)^{\frac{n}{2}} - x = 1, (4a^2-1)^{\frac{n}{2}} + x = (3a^2-1)^m$, and it follows that

$$2(4a^2-1)^{\frac{n}{2}} = (3a^2-1)^m + 1. \tag{7}$$

We recall that a is even. Considering the above equality and taking modulo $4a^2$ we get

$$(-1)^{\frac{n}{2}}2 \equiv 3ma^2 + (-1)^m + 1 \pmod{4a^2}. \tag{8}$$

Since $a > 1$, we see from (8) that $2|m$. If $n = 2$, one can easily derive that (7) does not hold for $a > 1$. If $\frac{n}{2}$ is odd and $\frac{n}{2} > 1$, by lemma5 we can also derive that (7) does not hold for $a > 1$. If $\frac{n}{2}$ is even, we infer from (8) that $4|m$, and we see from (7)and Lemma 2 that $a = 0$.

Now, we turn to the case $2|m, 2 \not| n$. By taking modulo 4 we get from (4) that $x^2 + 1 \equiv -1 \pmod 4$, which is not possible.

Now , we deal with the case$2 \not| mn$. We can rewrite our equation (4) under the form:

$$x^2 - (4a^2-1)^n = -(3a^2-1)^m. \tag{9}$$

By (9), we can get the following decomposition in the algebraic integers ring $Z[\sqrt{4a^2-1}]$:

$$\begin{aligned}&[x+(4a^2-1)^{\frac{n-1}{2}}\sqrt{4a^2-1}][x-(4a^2-1)^{\frac{n-1}{2}}\sqrt{4a^2-1}]\\&=(a\pm\sqrt{4a^2-1})^m(a\mp\sqrt{4a^2-1})^m.\end{aligned}\tag{10}$$

One easily verifies that $\gcd(x+(4a^2-1)^{\frac{n-1}{2}}\sqrt{4a^2-1},x-(4a^2-1)^{\frac{n-1}{2}}\sqrt{4a^2-1})=\varepsilon$, where $\varepsilon=\pm(2a\pm\sqrt{4a^2-1})^k$ is a unit in $Z[\sqrt{4a^2-1}]$. Since $3a^2-1$ is prime, both $(a+\sqrt{4a^2-1})$ and $(a-\sqrt{4a^2-1})$ are prime ideals in $Z[\sqrt{4a^2-1}]$. Observing that $2a+\sqrt{4a^2-1}$ is a fundamental unit, by (10), we have

$$x+(4a^2-1)^{\frac{n-1}{2}}\sqrt{4a^2-1}=\pm(2a\pm\sqrt{4a^2-1})^k(a\pm\sqrt{4a^2-1})^m\tag{11}$$

and

$$x-(4a^2-1)^{\frac{n-1}{2}}\sqrt{4a^2-1}=\pm(2a\mp\sqrt{4a^2-1})^k(a\mp\sqrt{4a^2-1})^m.\tag{12}$$

We see from (9) that $a|x$. If $2\nmid k$, by taking modulo a we get from (11) that

$$x\pm\sqrt{4a^2-1}\equiv\pm\sqrt{4a^2-1}^k\sqrt{4a^2-1}^m\equiv\pm(4a^2-1)^{\frac{k+m}{2}}\equiv\pm1\pmod a.$$

It follows that $x\equiv\pm1\pmod a$, which is not possible since $a>1$. Let $k=2k_1$. We can rewrite (11) in the form

$$x+(4a^2-1)^{\frac{n-1}{2}}\sqrt{4a^2-1}=\pm(2a\pm\sqrt{4a^2-1})^{2k_1}(a\pm\sqrt{4a^2-1})^m.$$

By taking modulo $4a^2-1$, we get

$$x\equiv\pm((2a)^{2k_1}\pm4ak_1\sqrt{4a^2-1})(a^m\pm ma\sqrt{4a^2-1})\pmod{4a^2-1}.$$

It follows that

$$x\equiv\pm((4a^2)^{k_1}a^m)\pm A\sqrt{4a^2-1}\equiv\pm a^m\pm A\sqrt{4a^2-1}\pmod{4a^2-1},$$

where $A=\pm(2a)^{2k_1}ma\pm4a^{m+1}k_1$. Hence, $x\equiv\pm a^m\pmod{4a^2-1}$. Observe that

$$(3a^2-1)^{\frac{m-1}{2}}\equiv(-a^2)^{\frac{m-1}{2}}\equiv\pm a^{m-1}\pmod{4a^2-1}$$

and

$$x\equiv\pm a^m\equiv\pm a\cdot(3a^2-1)^{\frac{m-1}{2}}\pmod{4a^2-1}.$$

By Lemma 4 we know that two solutions $(x,(3a^2-1)^{\frac{m-1}{2}},n)$ and $(a,1,1)$ of the equation

$$x^2+(3a^2-1)y^2=(4a^2-1)^n\tag{13}$$

belong to the same class. By Lemma 3 we get

$$x+(3a^2-1)^{\frac{m-1}{2}}\sqrt{-(3a^2-1)}=\pm(a\pm\sqrt{-(3a^2-1)})^n$$

and

$$x-(3a^2-1)^{\frac{m-1}{2}}\sqrt{-(3a^2-1)}=\pm(a\mp\sqrt{-(3a^2-1)})^n.$$

It follows that

$$(3a^2-1)^{\frac{m-1}{2}} = \pm\frac{(a+\sqrt{-(3a^2-1)})^n-(a-\sqrt{-(3a^2-1)})^n}{2\sqrt{-(3a^2-1)}}. \tag{14}$$

We see that $(a+\sqrt{-(3a^2-1)}+a-\sqrt{-(3a^2-1)})$ and $(a+\sqrt{-(3a^2-1)})(a-\sqrt{-(3a^2-1)})$ are non-zero coprime integers. Notice that $\frac{a+\sqrt{-(3a^2-1)}}{a-\sqrt{-(3a^2-1)}}$ is a root of $(4a^2-1)x^2+(4a^2-2)x+4a^2-1=0$ and $\gcd(4a^2-1,4a^2-2)=1$. This implies that $\frac{a+\sqrt{-(3a^2-1)}}{a-\sqrt{-(3a^2-1)}}$ is not a root of unit. By Definition 1, $(a+\sqrt{-(3a^2-1)}, a-\sqrt{-(3a^2-1)})$ is a Lucas pair. Since $[(a+\sqrt{-(3a^2-1)})-(a-\sqrt{-(3a^2-1)})]^2=-4(3a^2-1)$ and $3a^2-1$ is prime, by Definition 2 and (14), we know that the only prime factor $3a^2-1$ of $u_n(a+\sqrt{-(3a^2-1)}, a-\sqrt{-(3a^2-1)})$ is not its primitive divisor, which implies that u_n has not any primitive divisor. By Theorem BHV, we have $n\le 30$; by Lemma 1, we have $n=1$ or 3. If $n=1$, by (14) we get a solution of (3), namely $(x,m,n)=(a,1,1)$. If $n=3$, by (14) we get another solution $(x,m,n)=(8a^3-3a,1,3)$. □

Remark By the proof of Theorem, if $3a^2-1$ is a power of an odd prime number, one can get the same result.

参考文献:

[1] BILU Y, HANROT G, VOUTIER P M. *Existence of primitive divisors of Lucas and Lehmer numbers* [J]. J. Reine Angew. Math., 2001, **539**: 75–122.
[2] BUGEAUD Y. *On some exponential Diophantine equations* [J]. Monatsh. Math., 2001, **132**(2): 93–97.
[3] BUGEAUD Y, SHOREY T N. *On the number of solutions of the generalized Ramanujan-Nagell equation* [J]. J. Reine Angew. Math., 2001, **539**: 55–74.
[4] LEHMER D H. *An extended theory of Lucas' functions* [J]. Ann. Math., 1930, **31**: 419–448.
[5] LE Mao-hua. *The diophantine equation* $x^2+D^m=p^n$ [J]. Acta Arith., 1989, **52**: 255–265.
[6] LJUNGGREN W. *On the diophantine equation* $Cx^2+D=2y^n$ [J]. Math. Scand, 1966, **18**: 69–86.
[7] MIGNOTTE M. *On the Diophantine equation* $D_1x^2+D_m^2=4y^n$ [J]. Portugal. Math., 1997, **54**(4): 457–460.
[8] MORDELL L J. *Diophantine Equations* [M]. Academic Press, London-New York, 1969.
[9] YUAN Ping-zhi, HU Yong-zhong. *On the Diophantine equation* $x^2+D^m=p^n$ [J]. J. Number Theory, 2005, **111**(1): 144–153.
[10] HU Yong-zhong, LIU Rong-xuan. *On the solutions of the exponential Diophantine equation* $x^2+(3a^2+1)^m=(4a^2+1)^n$ [J]. Sichuan Daxue Xuebao, 2006, **43**(1): 41–46.
[11] YUAN Ping-zhi. *On the diophantine equation* $ax^2+by^2=ck^n$ [J]. Indag Math., N.S., 2005, **16**(2): 301–320.
[12] VOUTIER P M. *Primitive divisors of Lucas and Lehmer sequences* [J]. Math. Comp., 1995, **64**(210): 869–888.
[13] STÖMER C. *L'equation* $m\arctan\frac{1}{x}+n\arctan\frac{1}{y}=k\frac{\pi}{4}$ [J]. Bull. Soc. Math. France, 1899, **27**: 160–170.

关于指数丢番图方程 $x^2+(3a^2-1)^m=(4a^2-1)^n$

胡 永 忠

(佛山科学技术学院数学系，广东 佛山 528000)

摘要: 应用 Bilu, Hanrot 和 Voutier 关于本原素因子的深刻结果以及二次丢番图方程解的表示的一些精细结果，完全解决了指数型丢番图方程 $x^2+(3a^2-1)^m=(4a^2-1)^n$ 当 $3a^2-1$ 是奇素数或奇素数幂时的求解问题.

关键词: 指数丢番图方程； Lucas 序列；本原素因子； Kronecker 符号.