BULL. AUSTRAL. MATH. SOC. 11D61, 11B39
VOL. 64 (2001) [99–105]

AN EXPONENTIAL DIOPHANTINE EQUATION

MAOHUA LE

Let p be an odd prime with $p > 3$. In this paper we give all positive integer solutions (x, y, m, n) of the equation $x^2 + p^{2m} = y^n$, $\gcd(x, y) = 1$, $n > 2$ satisfying $2 \mid n$ or $2 \nmid n$ and $p \not\equiv (-1)^{(p-1)/2} \pmod{4n}$.

1. INTRODUCTION

Let $\mathbb{Z}, \mathbb{N}, \mathbb{Q}$ be the sets of all integers, positive integers and rational numbers respectively. Let p be a prime. There have been many papers concerned with solutions (x, y, m, n) of the equation

$$x^2 + p^m = y^n,\ x, y, m, n \in \mathbb{N},\ \gcd(x, y) = 1,\ n > 2. \tag{1}$$

All solutions of (1) for $p \in \{2, 3\}$ have been determined. The known results include the following:

1. (Nagell [**12**].) If $p = 2$, then the only solution of (1) with $m = 2$ is $(x, y, m, n) = (11, 5, 2, 3)$.
2. (Cohn [**3**].) If $p = 2$, then the only solution of (1) with $2 \nmid m$ are $(x, y, m, n) = (5, 3, 1, 3)$ and $(7, 3, 5, 4)$.
3. (Le [**5, 6**].) If $p = 2$, then (1) has no solutions (x, y, m, n) satisfying $2 \mid m$ and $m > 2$.
4. (Arif and Muriefah [**1**].) If $p = 3$, then the only solution of (1) with $2 \nmid m$ is $(x, y, m, n) = (10, 7, 5, 3)$.
5. (Luca [**9**].) If $p = 3$, then the only solution of (1) with $2 \mid m$ is $(x, y, m, n) = (46, 13, 4, 3)$.

In this paper we investigate the solutions (x, y, m, n) of (1) for m even. Then (1) may be written as

$$x^2 + p^{2m} = y^n,\ x, y, m, n \in \mathbb{N},\ \gcd(x, y) = 1,\ n > 2. \tag{2}$$

We prove the following two results.

Received 3rd October, 2000
Supported by the National Natural Science Foundation of China (No. 19871073), the Guangdong Provincial Natural Science Foundation (No. 980869) and the Natural Science Foundation of the Higher Education Department of Guangdong Province (No. 9901).

Theorem 1. *If $p > 3$, then all the solutions (x, y, m, n) of (2) with $2 \mid m$ are given as follows:*

(i) $p = 239$, $(x, y, m, n) = (28560, 13, 1, 8)$.

(ii) $p = E(q)$, $(x, y, m, n) = \left(\left((E(q))^2 - 1\right)/2,\ F(q), 1, 4\right)$, *where q is an odd prime, and*

$$E(q) = \frac{1}{2}\left(\left(1+\sqrt{2}\right)^q + \left(1-\sqrt{2}\right)^q\right), \quad F(q) = \frac{1}{2\sqrt{2}}\left(\left(1+\sqrt{2}\right)^q - \left(1-\sqrt{2}\right)^q\right). \tag{3}$$

Theorem 2. *If $p > 3$ and $p \not\equiv (-1)^{(p-1)/2} \pmod{4n}$, then (2) has no solutions (x, y, m, n) with $2 \nmid n$.*

By the above theorems, we can completely determine all solutions of (2) for the case that p is either a Fermat prime or a Mersenne prime.

Corollary 1. *If p is a Fermat prime with $p > 3$, then (2) has no solutions (x, y, m, n).*

Corollary 2. *If $p = 7$, then the only solution of (2) is $(x, y, m, m) = (24, 5, 1, 4)$. If p is a Mersenne prime with $p > 7$, then (2) has no solutions (x, y, m, n).*

2. Preliminaries

Lemma 1. [**11**, pp.12–13] *Every solution (X, Y, Z) of the equation*

$$X^2 + Y^2 = Z^2,\ X, Y, Z \in \mathbb{N},\ \gcd(X, Y) = 1,\ 2 \mid X \tag{4}$$

can be expressed as

$$X = 2AB,\ Y = A^2 - B^2,\ Z = A^2 + B^2, \tag{5}$$

where A, B are positive integers satisfying

$$A > B,\ \gcd(A, B) = 1,\ 2 \mid AB. \tag{6}$$

Lemma 2. [**11**, pp.122–123] *Let n be an odd integer with $n > 1$. Then every solution (X, Y, Z) of the equation*

$$X^2 + Y^2 = Z^n,\ X, Y, Z \in \mathbb{N},\ \gcd(X, Y) = 1 \tag{7}$$

can be expressed as

$$Z = A^2 + B^2,\ X + Y\sqrt{-1} = \lambda_1\left(A + \lambda_2 B\sqrt{-1}\right)^n,\ \lambda_1, \lambda_2 \in \{-1, 1\}, \tag{8}$$

https://doi.org/10.1017/S0004972700019717 Published online by Cambridge University Press

where A, B are coprime positive integers.

Lemma 3. [7] *The only solutions of the operation*

$$X^2 + 1 = 2Y^4,\ X,\ Y \in \mathbb{N} \tag{9}$$

are $(X,Y) = (1,1)$ and (239,13).

Lemma 4. [8] *Let D be a positive integer which is not a square. Then the equation*

$$X^4 - DY^2 = -1,\ X, Y \in \mathbb{N} \tag{10}$$

has at most one solution (X,Y). Moreover, if (X,Y) is a solution of (10), then the fundamental solution $U_1 + V_1\sqrt{D}$ of the Pell equation

$$U^2 - DV^2 = -1,\ U, V \in \mathbb{N} \tag{11}$$

satisfies

$$U_1 = dt^2,\ X^2 + Y\sqrt{D} = \left(U_1 + V_1\sqrt{D}\right)^d,\ d, t \in \mathbb{N},\ 2 \nmid d,\ d \text{ is square free.} \tag{12}$$

Lemma 5. [13] *The equation*

$$X^2 + 1 = 2Y^r,\ X, Y, r \in \mathbb{N},\ X > Y > 1,\ r > 1,\ 2 \nmid r \tag{13}$$

has no solutions (X,Y,r).

Lemma 6. [4, Lemma 15] *The equation*

$$X^{2r} + 1 = 2Y^2,\ X, Y, r \in \mathbb{N},\ X > 1,\ Y > 1,\ r > 1,\ 2 \nmid r \tag{14}$$

has no solutions (X,Y,r).

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

$$\alpha = \frac{1}{2}\left(a + \lambda\sqrt{b}\right),\ \beta = \frac{1}{2}\left(a - \lambda\sqrt{b}\right),\ \lambda \in \{-1, 1\}, \tag{15}$$

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 $u_t = u_t(\alpha, \beta) = (\alpha^t - \beta^t)/(\alpha - \beta)$ for $t = 0, 1, 2, \ldots$. For equivalent Lucas pairs (α_1, β_1) and (α_2, β_2), we have $u_t(\alpha_1, \beta_1) = \pm u_t(\alpha_2, \beta_2)$ for any $t \geqslant 0$. A prime p is a primitive divisor of $u_t(\alpha, \beta)$ if $p \mid u_t$ and $p \nmid bu_1 \cdots u_{t-1}$.

Lemma 7. [10] *Let (α,β) be a Lucas pair with parameters (a,b). If p is a primitive divisor of $u_t(\alpha,\beta)$ $(t>2)$, then $p-\left(\frac{b}{p}\right)\equiv 0 \pmod t$ where $\left(\frac{b}{p}\right)$ is the Legendre symbol.*

A Lucas pair (α,β) such that $u_t(\alpha,\beta)$ has no primitive divisors will be called a t-defective Lucas pair.

Lemma 8. [14] *Let t satisfy $4<t<30$ and $t\neq 6$. Then, up to equivalence, all parameters of t-defective Lucas pairs are given as follows:*

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

A positive integer t is called totally non-defective if no Lucas pair is t-defective.

Lemma 9. [2] *If $t>30$, then t is totally non-defective.*

3. Proofs

Proof of Theorem 1: Let (x,y,m,n) be a solution of (2). Since $p>3$ and $n>2$, we have $2\mid x$ and $2\nmid y$. If $2\mid n$, since $\gcd\left(y^{n/2}+x,\ y^{n/2}-x\right)=1$, then from (2) we get $y^{n/2}+x=p^{2m}$ and $y^{n/2}-x=1$. This implies that

$$p^{2m}+1=2y^{n/2}, \tag{16}$$

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

Since $n/2>1$, by Lemma 5, we see from (16) that $n/2$ has no odd prime divisors. So we have $n=2^{s+1}$, where s is a positive integer.

When $s=1$, (16) can be written as

$$p^{2m}+1=2y^2. \tag{18}$$

Then $(u,v)=(p^m,y)$ is a solution of the Pell equation

$$u^2-2v^2=-1,\ u,v\in\mathbb{N}. \tag{19}$$

Since $1+\sqrt{2}$ is the fundamental solution of (19), we get

$$\begin{aligned} p^m&=\frac{1}{2}\left(\left(1+\sqrt{2}\right)^l+\left(1-\sqrt{2}\right)^l\right),\\ y&=\frac{1}{2\sqrt{2}}\left(\left(1+\sqrt{2}\right)^l-\left(1-\sqrt{2}\right)^l\right),\ l\in\mathbb{N},\ 2\nmid l. \end{aligned} \tag{20}$$

https://doi.org/10.1017/S0004972700019717 Published online by Cambridge University Press

On the other hand, if m has an odd prime divisor r, then $(X,Y) = (p^{m/r}, y)$ is a solution of (14). However, by Lemma 6, this is impossible. Therefore, if $m > 1$, then m is a power of 2 and $(X,Y) = (p^{m/2}, y)$ is a solution of (10) for $D = 2$. But, by Lemma 4, this is impossible too. So we have $m = 1$. Then the positive integer l in (20) must be an odd prime. Thus, by (17) and (20), we obtain the solution (ii).

When $s > 1$, we see from (16) that $(X,Y) = (p^m, y^{n/8})$ is a solution of (9). Therefore, by Lemma 3, we get the solution (i). Thus, the theorem is proved. $\square$

Proof of Theorem 2: Let (x,y,m,n) be a solution of (2) with $2 \nmid n$. Then $(X,Y,Z) = (x, p^m, y)$ is a solution of (7). By Lemma 2, we get

$$x + p^m\sqrt{-1} = \lambda_1\left(A + \lambda_2 B\sqrt{-1}\right)^n, \ \lambda_1, \lambda_2 \in \{-1, 1\}, \tag{21}$$

where A, B are positive integers satisfying

$$A^2 + B^2 = y, \ \gcd(A,B) = 1. \tag{22}$$

From (21), we get

$$p^m = \lambda_1\lambda_2 B \sum_{i=0}^{(n-1)/2} \binom{n}{2i+1} A^{n-2i-1}\left(-B^2\right)^i. \tag{23}$$

Let

$$\alpha = A + B\sqrt{-1}, \quad \beta = A - B\sqrt{-1}. \tag{24}$$

We see from (22) and (24) that (α, β) is a Lucas pair with parameters $\left(2A, -4B^2\right)$. Further, let $u_t(\alpha,\beta)$ $(t = 0, 1, 2, \dots)$ denote the corresponding Lucas numbers. By (23), we get

$$p^m = \pm B u_n(\alpha, \beta). \tag{25}$$

Notice that $\left(\dfrac{-4B^2}{p}\right) = \left(\dfrac{-1}{p}\right) = (-1)^{(p-1)/2}$, where $\left(\dfrac{*}{p}\right)$ is the Legendre symbol. By Lemma 7, if p is a primitive divisor of $u_n(\alpha,\beta)$, then $p - (-1)^{(p-1)/2} \equiv 0 \pmod{n}$. Since $2 \nmid n$ and $p - (-1)^{(p-1)/2} \equiv 0 \pmod 4$, we get $p \equiv (-1)^{(p-1)/2} \pmod{4n}$. Therefore, by (25), if the solution (x,y,m,n) satisfies $p \not\equiv (-1)^{(p-1)/2} \pmod{4n}$, then $u_n(\alpha,\beta)$ has no primitive divisors. By Lemmas 8 and 9, we deduce that $n = 3$ and $p \mid B$. Then, by (23), we get

$$B = p^s, \ 3A^2 - B^2 = \pm p^{m-s}, \ s \in \mathbb{N}, \ s \leqslant m. \tag{26}$$

https://doi.org/10.1017/S0004972700019717 Published online by Cambridge University Press

Since $\gcd(A,B) = 1$, we see from (26) that $p = 3$. thus, if $p > 3$, then (2) has no solutions (x,y,m,n) satisfying $2 \nmid n$ and $p - (-1)^{(p-1)/2} \not\equiv 0 \pmod{4n}$. The theorem is proved. □

Proof of Corollary 1: Let p be a Fermat prime. Then we have

$$p = 2^{2^s} + 1, \ s \in \mathbb{N}. \tag{27}$$

Since $p - (-1)^{(p-1)/2} = 2^{2^s}$, by Theorem 2, then (2) has no solutions (x,y,m,n) with $2 \nmid n$.

On the other hand, since $p \neq 239$, by the proof of Theorem 1, if (x,y,m,n) is a solution of (2) with $2 \mid n$, then we have $m = 1$, $n = 4$ and

$$p^2 + 1 = 2y^2. \tag{28}$$

Substitute (27) into (28), and we get

$$2^{2^{s+1}-2} + \left(2^{2^s-1} + 1\right)^2 = y^2. \tag{29}$$

Therefore, by Lemma 1, we obtain from (29) that

$$2^{2^s-1} = 2AB, \ 2^{2^s-1} + 1 = A^2 - B^2, \ y = A^2 + B^2, \tag{30}$$

where A, B are positive integers satisfying (6). From (30), since $\gcd(A,B) = 1$, we get from the first equation $s > 1$, $A = 2^{2^s-2}$ and $B = 1$. However, by the second equation in (30), we get

$$1 \equiv 2^{2^s-1} + 1 = 2^{2^{s+1}-4} - 1 \equiv 3 \pmod 4, \tag{31}$$

which is a contradiction. Thus, the corollary is proved. □

Proof of Corollary 2: Let p be a Mersenne prime. Then we have

$$p = 2^r - 1, \ r \text{ is an odd prime}, \tag{32}$$

if $p \geqslant 7$. Since $p-(-1)^{(p-1)/2} = 2^r$, by Theorem 2, then (2) has no solutions (x,y,m,n) with $2 \nmid n$.

By Theorem 1, if $r = 3$, then $p = 7$ and the only solution of (2) with $2 \mid n$ is $(x,y,m,n) = (24,5,1,4)$. Since $p \neq 239$, by the proof of Theorem 1, if $r > 3$ and (x,y,m,n) is a solution of (2) with $2 \mid n$, then $m = 1$, $n = 4$ and (28) holds. Substitute (32) into (28), and we get

$$2^{2r-2} + \left(2^{r-1} - 1\right)^2 = y^2. \tag{33}$$

By Lemma 1, we obtain from (33) that

$$2^{r-1} = 2AB, \ 2^{r-1} - 1 = A^2 - B^2, \ y = A^2 + B^2, \tag{34}$$

whence we obtain $A = 2^{r-2}$ and $B = 1$, since $\gcd(A,B) = 1$, but these do not satisfy the second equation in (34), when $r > 3$. Thus, if $p > 7$, then (2) has no solutions (x,y,m,n). The corollary is proved. □

REFERENCES

[1] S.A. Arif and F.S.A. Muriefah, 'The diophantine equation $x^2 + 3^m = y^n$', *Internat. J. Math. Math. Sci.* **21** (1998), 619–620.

[2] Y. Bilu, G. Hanrot and P.M. Voutier, 'Existence of primitive divisors of Lucas and Lehmer numbers', *J. Reine Angew. Math.* (to appear).

[3] J.H.E. Cohn, 'The diophantine equation $x^2 + 2^k = y^n$', *Arch. Math. (Basel)* **59** (1992), 341–344.

[4] M.-H. Le, 'On the diophantine equation $(x^m + 1)(x^n + 1) = y^2$', *Acta Arith.* **82** (1997), 17–26.

[5] M.-H. Le, 'Diophantine equation $x^2 + 2^m = y^n$', *Chinese Sci. Bull.* **2** (1997), 1515–1517.

[6] M.-H. Le, 'On Cohn's conjecture concerning the diophantine equation $x^2 + 2^m = y^n$', *Arch. Math. (Basel)* (to appear).

[7] W. Ljunggren, 'Zur Theorie der Gleichung $x^2 + 1 = Dy^4$', *Avh. Norske Vid. Akad. Oslo* **5** (1942), 1–27.

[8] W. Ljunggren, 'Ein satz über die Diophantische gleichung $Ax^2 - By^4 = C$ $(C = 1, 2, 4)$', *Tolfte Skandinaviska Matematikerkongressen, Lund* (1954), 188–194.

[9] F. Luca, 'On a diophantine equation', *Bull. Austral. Math. Soc.* **61** (2000), 241–246.

[10] E. Lucas, 'Théorie des functions numériques simplement périodiques', *Amer. J. Math.* **1** (1878), 184–240, 289–321.

[11] L.J. Mordell, *Diophantine equations* (Academic Press, London, 1969).

[12] T. Nagell, 'Contributions to the theory of a category of diophantine equations of the second degree with two unknowns', *Nova Acta Soc. Sci. Upsal. (4)* **16** (1954), 1–38.

[13] C. Störmer, 'L'équation m arc tan $(1/x) + n$ arc tan $(1/y) = k\pi/4$', *Bull. Soc. Math. France* **27** (1899), 160–170.

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

Department of Mathmatics
Zhanjiang Normal College
Postal Code 524048
Zhanjiang, Guangdong
People's Republic of China