TAIWANESE JOURNAL OF MATHEMATICS
Vol. 12, No. 5, pp. 1015-1034, August 2008
This paper is available online at http://www.tjm.nsysu.edu.tw/

THE EXPONENTIAL DIOPHANTINE EQUATION $AX^2 + BY^2 = \lambda k^Z$ AND ITS APPLICATIONS

Zhenfu Cao, Chuan I Chu and Wai Chee Shiu

Abstract. Let $A, B \in \mathbb{N}$ with $A > 1, B > 1$ and $\gcd(A, B) = 1$, $k \geq 2$ be an integer coprime with AB, and let $\lambda \in \{1, 2, 4\}$ be such that if $\lambda = 4$, then $A \neq 4$ and $B \neq 4$; and if k is even, then $\lambda = 4$. In this paper, we shall describe all solutions of the equation

$$AX^2 + BY^2 = \lambda k^Z,\ X, Y, Z \in \mathbb{Z}, \gcd(X, Y) = 1,\ Z > 0$$

with $X|^*A$ or $Y|^*B$, where the symbol $X|^*A$ means that every prime divisor of X divides A. Then, using this result, we give some more general results on the number of solutions of the equation $la^x + mb^y = \lambda c^z$, $x > 1$, $y > 1$, $z > 1$. In addition, using Cao's result on Pell equation, we obtain some improvement of Terai's results on the equations $a^x + 2 = c^z, a^x + 4 = c^z$ and $a^x + 2^y = c^z$.

1. Introduction

In this paper, we let $\mathbb{Z}$, $\mathbb{N}$, $\mathbb{P}$ be the sets of integers, positive integers and prime numbers respectively. For $x, A \in \mathbb{N}$, the notation $x|^*A$ means that every prime factor of x is also a factor of A.

Let $A, B \in \mathbb{N}$ with $A > 1, B > 1$ and $\gcd(A, B) = 1$. If the equation

$$X^2 + ABY^2 = p^Z,\ X, Y, Z \in \mathbb{N}, p \in \mathbb{P}, \gcd(X, Y) = 1 \tag{1.1}$$

has a solution (X, Y, Z), then there exists a unique solution (X_p, Y_p, Z_p) which satisfies $Z_p \leq Z$, where Z runs over all solution of (1.1). The solution (X_p, Y_p, Z_p) is called the *least solution* of (1.1).

Received May 3, 2006, accepted September 13, 2006.
Communicated by Bang-Yen Chen.
2000 *Mathematics Subject Classification*: 11D45, 11D61, 11D72.
Key words and phrases: Exponential Diophantine equation, Quadratic field.
This work is supported by the National Natural Science Foundation of China for Distinguished Young Scholars under Grant No. 60225007; the Faculty Research Grant of Hong Kong Baptist University.

In [10], Cao considered the solutions $(x, y, z) \in \mathbb{N}^3$ of the Diophantine equation

$$AX^2 + BY^2 = p^Z,\ \ X, Y, Z \in \mathbb{N},\ p \in \mathbb{P},\ \gcd(X, Y) = 1. \tag{1.2}$$

He obtained the following two theorems.

Theorem A. *Suppose that $x, y, z \in \mathbb{N}$ satisfy the equation*

$$Ax^2 + By^2 = 2^z,\ \ z > 2,\ x|^*A \text{ and } y|^*B. \tag{1.3}$$

Then

$$|Ax^2 - By^2| = 2X_2,\ xy = Y_2,\ 2z - 2 = Z_2,$$

except for $(A, B, x, y, z) = (5, 3, 1, 3, 5)$, $(5, 3, 5, 1, 7)$ and $(13, 3, 1, 9, 8)$, where (X_2, Y_2, Z_2) is the least solution of the equation (1.1) with $p = 2$.

Theorem B. *Suppose that $x, y, z \in \mathbb{N}$ satisfy the equation*

$$Ax^2 + By^2 = p^z,\ \ p \in \mathbb{P},\ p > 2,\ x|^*A \text{ and } y|^*B. \tag{1.4}$$

Then

$$|Ax^2 - By^2| = X_p,\ 2xy = Y_p,\ 2z = Z_p,$$

or

$$|Ax^2 - By^2| = X_p|X_p^2 - 3ABY_p^2|,\ 2xy = Y_p|3X_p^2 - ABY_p^2|,\ 2z = 3Z_p,$$

the latter occurring only for

$$Ax^2 + By^2 = 3^{4s+3}\left(\frac{3^{2s}-1}{8}\right) + \left(\frac{3^{2s+2}-1}{8}\right) = \left(\frac{3^{2s+1}-1}{2}\right)^3 = p^z,$$

where (X_p, Y_p, Z_p) is the least solution of the equation (1.1) and $s \in \mathbb{N}$.

From Theorems A and B, we have (please see Lemma 6 of [23]).

Theorem C. *The equation*

$$a^x + b^y = c^z, \gcd(a, b) = 1,\ c \in \mathbb{P},\ a > 1, b > 1$$

has at most one solution when the parities of x and y are fixed, except for $(a, b, c) = (5, 3, 2)$, $(13, 3, 2)$, or $(10, 3, 13)$. The solutions in the case of $(5, 3, 2)$ are given by $(x, y, z) = (1, 1, 3)$, $(1, 3, 5)$, $(3, 1, 7)$; in the case of $(13, 3, 2)$ by $(1, 1, 4)$ and $(1, 5, 8)$; and in the case of $(10, 3, 13)$ by $(1, 1, 1)$ and $(1, 7, 3)$. (c.f. [6, 22]).

In [11], Cao obtained further results when the right sides of Equation (1.3) and Equation (1.4) are replaced by $4k^z$ and k^z respectively, where $k \in \mathbb{N}$.

Let $A, B \in \mathbb{N}$ with $A > 1$, $B > 1$ and $\gcd(A, B) = 1$. Let $k \geq 2$ be an integer coprime with AB, and let $\lambda \in \{1, 2, 4\}$ be such that $\lambda = 4$ if k is even. In this paper, we shall first consider a more general equation of the form:

$$AX^2 + BY^2 = \lambda k^Z,\ X, Y, Z \in \mathbb{Z},\ \gcd(X, Y) = 1,\ Z > 0. \tag{1.5}$$

Suppose that $\lambda = 4$, $A = 4$ and (X, Y, Z) is a solution of (1.5). Since $\gcd(A, B) = 1$, Y must be even. Thus Equation (1.5) can be rewritten as

$$X^2 + B\Big(\frac{Y}{2}\Big)^2 = k^Z,\ X, Y, Z \in \mathbb{Z},\ \gcd(X, Y) = 1,\ Z > 0.$$

This equation was discussed in [11]. From now on, we will assume that if $\lambda = 4$, then $A \neq 4$. For the same reason we shall assume that $B \neq 4$ as well if $\lambda = 4$.

2. Preliminaries

Before considering Equation (1.5) we recall some known results.

For $a, b, c \in \mathbb{Z}$, the discriminant of the form $aX^2 + 2bXY + cY^2$ is $4b^2 - 4ac$, thus $-4D$ is the discriminant of $D_1X^2 + D_2Y^2$, where $D = D_1D_2$. The set of positive binary quadratic forms of discriminant $-4D$ is partitioned into a finite number of equivalence classes which we denote by $h(-4D)$.

By Theorems 11.4.3, 12.10.1 and 12.14.3 of Hua [18], we get (see Proposition 1 of [3]).

Lemma 2.1. *Let $D \in \mathbb{N}$. We have*

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

Let D_1 and D_2 be coprime positive integers, $D = D_1D_2$ and let $k \geq 2$ be an integer coprime with D. Let $\lambda \in \{1, 2, 4\}$ be such that $\lambda = 4$ if k is even. Keeping these notations, Bugeaud and Shorey [3] proved the following lemma.

Lemma 2.2. *Let $D_1D_2 \notin \{1, 3\}$. The solutions of the equation*

$$D_1X^2 + D_2Y^2 = \lambda k^Z,\ X, Y, Z \in \mathbb{Z},\ \gcd(X, Y) = 1,\ Z > 0 \tag{2.1}$$

can be put into at most $2^{\omega(k)-1}$ classes, where $\omega(k)$ denotes the number of distinct prime divisors of k. Furthermore, in each such class $\mathcal{S}$, there is a unique solution

(X_1, Y_1, Z_1) such that $X_1 > 0, Y_1 > 0$ and Z_1 is minimal among the solutions in $\mathcal{S}$. This minimal solution satisfies the condition that Z_1 divides $h(-4D)$ if $D_1 = 1$ or $D_2 = 1$, and $2Z_1$ divides $h(-4D)$ otherwise. Moreover, every solution (X, Y, Z) of (2.1) belonging to $\mathcal{S}$ can be defined as

$$Z = Z_1 t, \quad \frac{X\sqrt{D_1} + Y\sqrt{-D_2}}{\sqrt{\lambda}} = \lambda_1 \left(\frac{X_1\sqrt{D_1} + \lambda_2 Y_1 \sqrt{-D_2}}{\sqrt{\lambda}} \right)^t \tag{2.2}$$

where $t \geq 1$ is an integer, $\lambda_1 \in \{-1, 1, -i, i\}$ and $\lambda_2 \in \{-1, 1\}$. If $\lambda = 2$, then t is odd. Furthermore, $\lambda_1 \in \{-1, 1\}$ if $D_2 \neq 1$ or t is odd and $\lambda_1 \in \{-i, i\}$ if $D_2 = 1$ and t is even.

A *Lucas pair* (respectively a *Lehmer pair*) is a pair (α, β) of algebraic integers such that $\alpha+\beta$ and $\alpha\beta$ (respectively $(\alpha+\beta)^2$ 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

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

For a given Lehmer pair (α, β), we define the corresponding sequence of Lehmer numbers by

$$\widetilde{u}_n = \widetilde{u}_n(\alpha, \beta) = \begin{cases} \dfrac{\alpha^n - \beta^n}{\alpha - \beta}, & \text{if } n \text{ is odd,} \\[2ex] \dfrac{\alpha^n - \beta^n}{\alpha^2 - \beta^2}, & \text{if } n \text{ is even.} \end{cases}$$

It is clear that every Lucas pair (α, β) is also a Lehmer pair, and

$$u_n = \begin{cases} \widetilde{u}_n, & \text{if } n \text{ is odd,} \\ (\alpha + \beta)\widetilde{u}_n, & \text{if } n \text{ is even.} \end{cases}$$

Let (α, β) be a Lucas (resp. Lehmer) pair. A prime number p is a *primitive divisor* of the Lucas (resp. Lehmer) number $u_n(\alpha, \beta)$ (resp. $\widetilde{u}_n(\alpha, \beta)$) if p divides u_n but does not divide $(\alpha - \beta)^2 u_1 \cdots u_{n-1}$ (resp. if p divides $\widetilde{u}_n$ but does not divide $(\alpha^2 - \beta^2)^2 \widetilde{u}_1 \cdots \widetilde{u}_{n-1}$). Y. Bilu, G. Hanrot and P. Voutier [2] proved the following

Lemma 2.3. *For any integer $n > 30$, every n-th term of any Lucas or Lehmer sequence has a primitive divisor.*

A Lucas (respectively Lehmer) pair (α, β) such that $u_n(\alpha, \beta)$ (respectively $\widetilde{u}_n(\alpha, \beta)$) has no primitive divisors will be called *n-defective* Lucas (respectively

Lehmer) pair. Two Lucas pairs (α_1, β_1) and (α_2, β_2) are equivalent if $\frac{\alpha_1}{\alpha_2} = \frac{\beta_1}{\beta_2} = \pm 1$. Two Lehmer pairs (α_1, β_1) and (α_2, β_2) are equivalent if $\frac{\alpha_1}{\alpha_2} = \frac{\beta_1}{\beta_2} \in \{\pm 1, \pm\sqrt{-1}\}$.

For $n \leq 30$, all n-defective Lucas pairs and Lehmer paris are determined by Voutier [26] and Bilu et al. [2] as follows.

Lemma 2.4. ([26]) *Let n satisfy $4 < n \leq 30$ and $n \neq 6$. Then, up to equivalence, all n-defective Lucas pairs are of the form $((a - \sqrt{b})/2, (a + \sqrt{b})/2)$, where (a, b) is given in Table 1 of* [2].

Let n satisfy $6 < n \leq 30$ and $n \notin \{8, 10, 12\}$. Then, up to equivalence, all n-defective Lehmer pairs are of the form $((\sqrt{a} - \sqrt{b})/2, (\sqrt{a} + \sqrt{b})/2)$, where (a, b) is given in Table 2 of [2].

Lemma 2.5. ([2]) *Any Lucas pair is 1-defective, and any Lehmer pair is 1- and 2-defective.*

For $n \in \{2, 3, 4, 6\}$, all (up to equivalence) n-defective Lucas pairs are of the form $((a - \sqrt{b})/2, (a + \sqrt{b})/2)$, where (a, b) is given in Table 3 of [2].

For $n \in \{3, 4, 5, 6, 8, 10, 12\}$, all (up to equivalence) n-defective Lehmer pairs are of the form $((\sqrt{a} - \sqrt{b})/2, (\sqrt{a} + \sqrt{b})/2)$, where (a, b) is given in Table 4 of [2].

From Remark 1.1, Proposition 2.1(i) and Corollary 2.2 of [2], we get a classical result as follows.

Lemma 2.6. *If p is a primitive divisor of the Lucas (respectively Lehmer) number $u_n(\alpha, \beta)$ (respectively $\widetilde{u}_n(\alpha, \beta)$), then $n \equiv \pm 1 \pmod{p}$.*

In this paper, we let F_l and L_l be the l-th terms of Fibonacci number and Lucas number respectively, $l \in \mathbb{Z}$. That is $F_0 = 0$, $F_1 = 1$, $F_l = F_{l-1} + F_{l-2}$ and $L_0 = 2$, $L_1 = 1$, $L_l = L_{l-1} + L_{l-2}$. By Binet formulas we have

$$L_l^2 - 5F_l^2 = (-1)^l 4. \tag{2.3}$$

Lemma 2.7. *For $n \geq 3$, the equation $L_l = 2^n$ has no solution for $l \geq 0$. Indeed $L_0 = 2$ and $L_3 = 2^2$ are the only solutions.*

Proof. If $L_l = 2^n$ for some $n \geq 3$, then from (2.3) we have $2^{2n} - 5F_l^2 = (-1)^l 4$. So F_l is even. Hence we have, $2^{2n-2} - 5\left(\frac{F_l}{2}\right)^2 = (-1)^l$. Thus $\frac{F_l}{2}$ must be odd and then $\left(\frac{F_l}{2}\right)^2 \equiv 1 \pmod{8}$. Hence we have $3 \equiv (-1)^l \pmod{8}$, which is impossible. ∎

Lemma 2.8. *For $n \geq 4$, the equation $F_l = 2^n$ has no solution for $l \geq 0$. Indeed $F_3 = 2$ and $F_6 = 2^3$ are the only solutions.*

Proof. If $F_l = 2^n$ for some $n \geq 4$, then from (2.3) we have L_l is even and $\left(\frac{L_l}{2}\right)^2 - 5(2^{n-1})^2 = (-1)^l$. Thus $\frac{L_l}{2}$ must be odd and l is even. Hence $\left(\frac{L_l}{2}\right)^2 - 1 = 5(2^{n-1})^2$. Put $a = \frac{L_l}{2} + 1$ and $b = \frac{L_l}{2} - 1$. As both a and b are even and $a - b = 2$ we have two cases.

Case 1. Suppose that $a = 5 \cdot 2^i$ with $i \geq 1$ and $b = 2^{2n-2-i}$ with $2n-2-i \geq 1$. Since $a - b = 2$, we have $5 \cdot 2^{i-1} - 2^{2n-i-3} = 1$. Clearly the equation cannot have solution if $2 \leq i \leq 2n - 4$.

If $i=1$, then we have $5-2^{2n-4}=1$. Hence $2^{2n-4}=4$ which implies that $n=3$.

If $i = 2n - 3$, then we get $5 \cdot 2^{2n-4} - 1 = 1$, which is also impossible.

Case 2. Suppose that $a = 2^j$ and $b = 5 \cdot 2^{2n-2-j}$ for some $j \geq 4$ (since $a > b$) and $2n - 2 - j \geq 1$. Since $a - b = 2$, we have $2^{j-1} - 5 \cdot 2^{2n-j-3} = 1$.

Thus if $2n - j - 3 \geq 1$, then the above equation cannot have solution. We only have to consider $2n - j - 3 = 0$. That is, $j - 1 = 2n - 4$. Again we get $2^{2n-4} - 5 = 1$ which obviously has no solution. ■

It is easy to check the following lemma holds. Also one may refer to Lemma 2.3 of [3].

Lemma 2.9. *For any integer $l \geq 2$ and any $\varepsilon \in \{-1, 1\}$, we have*

$$4F_l - F_{l+2\varepsilon} = L_{l-\varepsilon},$$

and

$$4L_l - L_{l+2\varepsilon} = 5F_{l-\varepsilon}.$$

Furthermore, for any integer $l \geq 4$, we have

$$F_{l+2}\left(\frac{9F_{2l-1} - F_{2l-7} + (-1)^{l-1} \cdot 6}{10}\right)^2 + L_{l-1} = 4F_l^5$$

and

$$F_{l-2}\left(\frac{9F_{2l+1} - F_{2l-5} + (-1)^{l} \cdot 6}{10}\right)^2 + L_{l+1} = 4F_l^5.$$

3. Main Theorems

It is known (for example, see [13]) that if Equation (1.5) has a solution (X, Y, Z), then the solutions of the equation can be put into at most $2^{\omega(k)-1}$ classes, where $\omega(k)$ denotes the number of distinct prime divisors of k . In each such class, say $\mathcal{S}$, there is a unique solution $(X_{\lambda\mathcal{S}}, Y_{\lambda\mathcal{S}}, Z_{\lambda\mathcal{S}})$ such that $X_{\lambda\mathcal{S}} > 0, Y_{\lambda\mathcal{S}} > 0$ and $Z_{\lambda\mathcal{S}}$ is minimal among the solutions in $\mathcal{S}$.

Theorem 3.1. *Suppose* $(X, Y, Z) \in \mathbb{N}^3$ *is a solution in the class* $\mathcal{S}$ *of Equation* (1.5)*, and* $X|^*A$ *or* $Y|^*B$*. Then*

$$(X, Y, Z) = (X_{\lambda\mathcal{S}}, Y_{\lambda\mathcal{S}}, Z_{\lambda\mathcal{S}}),$$

except the following exceptional cases:

(1) $3{\cdot}13^2{+}5{\cdot}1^2 = 4{\cdot}2^7$, $5{\cdot}41^2{+}7{\cdot}7^2 = 4{\cdot}3^7$, $13{\cdot}71^2{+}3{\cdot}1^2 = 4{\cdot}4^7$ (*or* $= 4{\cdot}2^{14}$), $7 \cdot 1169^2 + 11 \cdot 1^2 = 2 \cdot 9^7$ (*or* $= 2 \cdot 3^{14}$);

(2) $5 \cdot 19^2 + 3 \cdot 9^2 = 4 \cdot 2^9$;

(3) $\frac{\lambda}{4}(q + 3^l)(2q - 3^l)^2 + \frac{\lambda}{4}(3q - 3^l)(3^l)^2 = \lambda q^3$, $q \in \mathbb{N}$ *with* $q > 3^{l-1}$, $l \geq 0$ *and* $3 \nmid q$ *if* $l > 0$,

$$q \equiv \begin{cases} (-1)^{l+1} \pmod 4, & \textit{for } \lambda = 1, \\ (-1)^l \pmod 4, q > 1, & \textit{for } \lambda = 2, \\ 0 \pmod 2, & \textit{for } \lambda = 4; \end{cases}$$

(4) (a) $\frac{\lambda}{4}F_{l-2\varepsilon}\big[4F_l^2 - 2F_{l-2\varepsilon}F_l + (-1)^l\big]^2 + \frac{\lambda}{4}L_{l+\varepsilon} \cdot 1^2 = \lambda F_l^5, l \in \mathbb{N}$, *where* $\varepsilon = \pm 1$, $l \geq 3$ *and*

$$l \equiv \begin{cases} 2\varepsilon \pmod 6, & \textit{for } \lambda = 1, \\ 5\varepsilon \pmod 6, & \textit{for } \lambda = 2, \\ 0, \varepsilon \pmod 3, & \textit{for } \lambda = 4. \end{cases}$$

(b) $\frac{\lambda}{4}L_{l-2\varepsilon}\big[4L_l^2 - 2L_{l-2\varepsilon}L_l + 5(-1)^{l+1}\big]^2 + \frac{\lambda}{4} \cdot 5F_{l+\varepsilon} \cdot 5^2 = \lambda L_l^5$, *where* $\varepsilon = \pm 1$, $l \geq 0$ *and*

$$l \equiv \begin{cases} 5\varepsilon \pmod 6, & \textit{for } \lambda = 1, \\ 2\varepsilon \pmod 6, & \textit{for } \lambda = 2, \\ 0, \varepsilon \pmod 3, l \neq 1, & \textit{for } \lambda = 4. \end{cases}$$

Proof. For $A > 1, B > 1$, we have $AB \notin \{1, 3\}$. Let $(X, Y, Z) \in \mathbb{N}^3$ be a solution in the class $\mathcal{S}$ of Equation (1.5). Put $(X_1, Y_1, Z_1) = (X_{\lambda\mathcal{S}}, Y_{\lambda\mathcal{S}}, Z_{\lambda\mathcal{S}})$. By Lemma 2.2, we get

$$Z = Z_1 t, \quad \frac{X\sqrt{A} + Y\sqrt{-B}}{\sqrt{\lambda}} = \lambda_1 \left(\frac{X_1\sqrt{A} + \lambda_2 Y_1\sqrt{-B}}{\sqrt{\lambda}}\right)^t, \tag{3.1}$$

where $t \geq 1$, $\lambda_1, \lambda_2 \in \{-1, 1\}$.

Suppose t is even. By Lemma 2.2, λ is equal to 1 or 4. From (3.1) we have

$$\frac{X\sqrt{A}+Y\sqrt{-B}}{\sqrt{\lambda}} = \lambda_1 \left(\frac{u+v\sqrt{-AB}}{\sqrt{\lambda}}\right)^{t/2}, \text{ where}$$

$$u = \frac{AX_1^2 - BY_1^2}{\sqrt{\lambda}} = \frac{-2BY_1^2 + \lambda k^{Z_1}}{\sqrt{\lambda}} = \frac{2AX_1^2 - \lambda k^{Z_1}}{\sqrt{\lambda}}, \tag{3.2}$$

$$v = \frac{2}{\sqrt{\lambda}}\lambda_2 X_1 Y_1.$$

One can easily check that $u, v \in \mathbb{Z}$ and

$$u^2 + v^2 AB = \lambda k^{2Z_1}. \tag{3.3}$$

We would like to write $\lambda_1 \left(\frac{u+v\sqrt{-AB}}{\sqrt{\lambda}}\right)^{t/2} = \frac{U+V\sqrt{-AB}}{\sqrt{\lambda}}$ for some $U, V \in \mathbb{Q}$. It can be shown that $U, V \in \mathbb{Z}$ (for $\lambda = 1$, it is clear; for $\lambda = 4$ it can be shown by induction).

From (3.1) we have $X\sqrt{A} = U$ and $Y = V\sqrt{A}$. Hence A is a square. From (1.5), we have $A(X^2 + BV^2) = \lambda k^Z$. Since $\gcd(AB, k) = 1$, $A|\lambda$. Since $A > 1$ and A is a square, $A = 4 = \lambda$. But this contradicts to our assumption.

Hence we get that t must be odd.

Let

$$\alpha = \frac{X_1\sqrt{A}+Y_1\sqrt{-B}}{\sqrt{\lambda}}, \ \beta = \frac{X_1\sqrt{A}-Y_1\sqrt{-B}}{\sqrt{\lambda}}.$$

Then from (3.1) we have

$$X = X_1\left|\frac{\alpha^t+\beta^t}{\alpha+\beta}\right|, Y = Y_1\left|\frac{\alpha^t-\beta^t}{\alpha-\beta}\right|,$$

and so $X = X_1 a, Y = Y_1 b$, where

$$a = |(\alpha^t+\beta^t)/(\alpha+\beta)|, \ b = |(\alpha^t-\beta^t)/(\alpha-\beta)|. \tag{3.4}$$

Clearly, the number $(\alpha^t+\beta^t)/(\alpha+\beta)$ is t-th term of Lehmer sequence with pair $(\alpha, -\beta)$ and the number $(\alpha^t-\beta^t)/(\alpha-\beta)$ also is t-th term of Lehmer sequence with pair (α, β).

We write the Lehmer pair in (3.4) as $((\sqrt{u}-\sqrt{v})/2, (\sqrt{u}+\sqrt{v})/2)$, then it is easy to see that

$$(u, v) = (4AX_1^2/\lambda, -4BY_1^2/\lambda). \tag{*}$$

Since t is odd, from the first equality of (3.4), we have

$$\lambda^{\frac{1}{2}(t-1)}a = \left|(X_1\sqrt{A})^{t-1} + \binom{t}{2}(X_1\sqrt{A})^{t-3}(Y_1\sqrt{-B})^2 + \cdots + \binom{t}{t-1}(Y_1\sqrt{-B})^{t-1}\right|. \tag{3.5}$$

Using (*) we get

$$a = \frac{1}{2^{t-1}}\left|u^{(t-1)/2} + \binom{t}{2}u^{(t-3)/2}v + \cdots + \binom{t}{t-1}v^{(t-1)/2}\right|; \tag{3.6}$$

and similarly we have

$$b = \frac{1}{2^{t-1}}\left|tu^{(t-1)/2} + \binom{t}{3}u^{(t-3)/2}v + \cdots + v^{(t-1)/2}\right|. \tag{3.7}$$

If $X|^*A$, then $a|^*A$ since $X = X_1a$. Suppose that $q \in \mathbb{P}$ with $q|a$. Since $a|^*A$, we know from (3.5) that $q|\binom{t}{t-1}(Y_1\sqrt{-B})^{t-1}$. Since $\gcd(A,B) = \gcd(X,Y) = 1$, $q|t$. By Lemma 2.6 and the first equality of (3.4), we have that $(\alpha^t + \beta^t)/(\alpha+\beta)$ has no primitive divisor, i.e. $(\alpha^t + \beta^t)/(\alpha+\beta)$ is t-defective.

Similarly, if $Y|^*B$ then $(\alpha^t - \beta^t)/(\alpha-\beta)$ is t-defective.

For $t = 1$, our theorem clearly holds. For $t \geq 3$ and odd, by using Lemmas 2.3, 2.4 and 2.5, Tables 2 and 4 in [2] we get only 4 cases, namely $t = 3, 5, 7$ or 9. Since $A, B > 1$, we shall get the following 4 exceptional cases:

Case 1. $t = 7$. We have $(u,v) = (3,-5), (5,-7), (13,-3)$ or $(14,-22)$. By using Equations (3.6) and (3.7) we get the following cases:

$$\begin{aligned}
3\cdot 13^2 + 5\cdot 1^2 &= 4\cdot 2^7;\\
5\cdot 41^2 + 7\cdot 7^2 &= 4\cdot 3^7;\\
13\cdot 71^2 + 3\cdot 1^2 &= 4\cdot 4^7 \text{ (or } = 4\cdot 2^{14});\\
7\cdot 1169^2 + 11\cdot 1^2 &= 2\cdot 9^7 \text{ (or } = 2\cdot 3^{14}).
\end{aligned}$$

Case 2. $t = 9$. We have $(u,v) = (5,-3)$ or $(7,-5)$. For $(u,v) = (5,-3)$ we get

$$5\cdot 19^2 + 3\cdot 9^2 = 4\cdot 2^9.$$

For $(u,v) = (7,-5)$, there is no solution.

Case 3. $t = 3$. We have $(u,v) = (1+q, 1-3q), q \in \mathbb{N}$ with $q > 1$ or $(3^l + q, 3^l - 3q)$ with $3 \nmid q$, $(l,q) \neq (1,1)$, $l \in \mathbb{N}$. When $(u,v) = (1+q, 1-3q)$, from (3.7) we have $b = 1$. Similarly, when $(u,v) = (3^l + q, 3^l - 3q)$ we have $b = 3^l$. Thus, combining these two cases we have

$$\frac{\lambda}{4}(q+3^l)(2q-3^l)^2+\frac{\lambda}{4}(3q-3^l)(3^l)^2=\lambda q^3,$$

where $q\in\mathbb{N}$ with $l\geq 0$; if $l=0$ then, $q>1$; if $l\geq 1$, then $q>3^{l-1}$ with $3\nmid q$; and

$$q\equiv\begin{cases}(-1)^{l+1}\pmod 4), & \text{for } \lambda=1,\\ (-1)^l \pmod 4), & \text{for } \lambda=2,\ q>1,\\ 0 \pmod 2), & \text{for } \lambda=4.\end{cases}$$

Case 4. $t=5$. We have $(u,v)=(F_{l-2\varepsilon},F_{l-2\varepsilon}-4F_l)$ for $l\geq 3$ or $(L_{l-2\varepsilon},L_{l-2\varepsilon}-4L_l)$ for $l\geq 0$ and $l\neq 1$, where $\varepsilon\in\{-1,1\}$.

If $(u,v)=(F_{l-2\varepsilon},F_{l-2\varepsilon}-4F_l)$, $l\geq 3$, then from Equations (3.7) and (3.6) we have

$$\begin{aligned} b &= |F_{l-2\varepsilon}^2-3F_{l-2\varepsilon}F_l+F_l^2|;\\ a &= |F_{l-2\varepsilon}^2-5F_{l-2\varepsilon}F_l+5F_l^2|.\end{aligned}$$

It is easy to show by induction that $F_{l-2\varepsilon}^2-3F_{l-2\varepsilon}F_l+F_l^2=(-1)^l$. Thus we have $b=1$ and $a=|4F_l^2-2F_{l-2\varepsilon}F_l+(-1)^l|$. Hence, by Lemma 2.9 we have

$$\frac{\lambda}{4}F_{l-2\varepsilon}a^2+\frac{\lambda}{4}L_{l+\varepsilon}\cdot 1^2=\lambda F_l^5, l\in\mathbb{N} \text{ with } l\geq 3, \tag{3.8}$$

where $a=|4F_l^2-2F_{l-2\varepsilon}F_l+(-1)^l|$.

In (3.8), we can easily see that if $l\equiv 5\varepsilon \pmod 6$ then $F_{l-2\varepsilon}\equiv L_{l+\varepsilon}\equiv 2 \pmod 4$, if $l\equiv 2\varepsilon \pmod 6$ then $F_{l-2\varepsilon}\equiv L_{l+\varepsilon}\equiv 0 \pmod 4$, and if $l\not\equiv 2\varepsilon \pmod 3$ then $F_{l-2\varepsilon}\equiv L_{l+\varepsilon}\equiv 1 \pmod 2$. Hence, we have

$$l\equiv\begin{cases}2\varepsilon \pmod 6), & \text{for } \lambda=1,\\ 5\varepsilon \pmod 6), & \text{for } \lambda=2,\\ 0,\varepsilon \pmod 3), & \text{for } \lambda=4.\end{cases}$$

Similarly, if $(4AX_1^2/\lambda,-4BY_1^2/\lambda)=(L_{l-2\varepsilon},L_{l-2\varepsilon}-4L_l)$, for $l\geq 0$ and $l\neq 1$, where $\varepsilon\in\{-1,1\}$, l is a non-negative integer, then from (3.7) we calculate $b=5$ and we get the following exceptional cases:

$$\frac{\lambda}{4}L_{l-2\varepsilon}c^2+\frac{\lambda}{4}\cdot 5F_{l+\varepsilon}\cdot 5^2=\lambda L_l^5, \tag{3.9}$$

where $c=|4L_l^2-2L_{l-2\varepsilon}L_l+5(-1)^{l+1}|$. Hence we have

$$l\equiv\begin{cases}5\varepsilon \pmod 6), & \text{for } \lambda=1,\\ 2\varepsilon \pmod 6), & \text{for } \lambda=2,\\ 0,\varepsilon \pmod 3), l\neq 1, & \text{for } \lambda=4.\end{cases}$$

This completes the proof. ■

Note that condition "$X|^*A$ and $Y|^*B$" in Theorems A and B is improved in Theorem 3.1 to "$X|^*A$ or $Y|^*B$".

4. Some Corollaries of the Main Theorem

Applying Theorem 3.1 we will obtain the following results.

Corollary 4.1. *Suppose $Z \notin \{3, 5, 7, 9, 14\}$. Then Equation (1.5) has at most $2^{\omega(k)-1}$ solutions (X, Y, Z) with $X|^*A$ or $Y|^*B$. Moreover, the solution (X, Y, Z) satisfies $Z < \frac{2}{\pi}\sqrt{AB}\log(2e\sqrt{AB})$.*

Proof. Suppose $Z \notin \{3, 5, 7, 9, 14\}$. Then from Theorem 3.1 we have that in the class $\mathcal{S}$, there is a unique solution $(X, Y, Z) = (X_{\lambda\mathcal{S}}, Y_{\lambda\mathcal{S}}, Z_{\lambda\mathcal{S}})$. So, Equation (1.5) has at most $2^{\omega(k)-1}$ solutions (X, Y, Z) satisfying $X^*|A$ or $Y^*|B$, since the solution of Equation (1.5) can be put into at most $2^{\omega(k)-1}$ classes. Also, by Lemma 2.2, we know that the minimal solution $(X_{\lambda\mathcal{S}}, Y_{\lambda\mathcal{S}}, Z_{\lambda\mathcal{S}})$ satisfies $2Z_{\lambda\mathcal{S}}$ divides $h(-4AB)$, where $h(-4AB)$ is the class number of primitive binary quadratic forms with the discriminant $-4AB$. Hence, by Lemma 2.1, we get

$$Z = Z_{\lambda\mathcal{S}} \leq \frac{1}{2}h(-4AB) < \frac{2}{\pi}\sqrt{AB}\log(2e\sqrt{AB}).$$ ■

Let $l, m, a, b, c \in \mathbb{N}$ with $a > 1$, $b > 1$, $c > 1$ and $\gcd(la, mb) = 1$, and let $\lambda \in \{1, 2, 4\}$ be such that $\lambda = 4$ if c is even. Le [20] showed that the Diophantine equation

$$la^x + mb^y = \lambda c^z, \quad x > 1, y > 1, z > 1 \tag{4.1}$$

has at most $2^{\omega(c)+1}$ solutions (x, y, z) with $l = m = \lambda = 1$ and c odd. From Theorem 3.1, we have

Corollary 4.2. *Except the following possible cases:*

$$5 \cdot 19^2 + 3^5 = 2^{11},\ 1 \cdot 61^2 + 3 \cdot 5^3 = 2^{12},\ 11 \cdot 19^2 + 5^3 = 2^{12},$$

$$(2^e + 3^l)(2^{e+1} - 3^l)^2 + (3 \cdot 2^e - 3^l) \cdot 3^{2l} = 2^{3e+2},\ e, l \in \mathbb{N} \textit{ with } (e, l) \neq (1, 1), (2, 2),$$

Equation (4.1) has at most 4 solutions (x, y, z) with $c = 2$.

Proof. Since $\lambda = 4$ when $c = 2$, from Equation (4.1) we have

$$la^x + mb^y = 2^{z+2}, \quad a > 1, b > 1, x > 1, y > 1, z > 1. \tag{4.2}$$

We classify all solutions (x, y, z) of (4.2) as follows: Class 1. x even, y even; Class 2. x even, y odd; Class 3. x odd, y even; Class 4. x odd, y odd. For each class, Equation (4.2) can be written as

$$la^i(a^{(x-i)/2})^2 + mb^j(b^{(y-j)/2})^2 = 2^{z+2}, \tag{4.3}$$

where $i, j \in \{0, 1, 2\}$, both i and j cannot be zero. By Theorem 3.1, except some cases, Equation (4.3) has at most one solution (x, y, z).

Now, we consider the exceptional cases described in Theorem 3.1. Since (4.2) required $a > 1$ and $b > 1$, it is easy to check that the case "$5 \cdot 19^2 + 3^5 = 2^{11}$" and the case "$(2^e + 3^l)(2^{e+1} - 3^l)^2 + (3 \cdot 2^e - 3^l) \cdot 3^{2l} = 2^{3e+2}$, $e, l \in \mathbb{N}$ with $2^e > 3^{l-1}$ and $(e, l) \neq (1, 1), (2, 2)$" are exceptional cases. For the other cases, it suffices to check the cases when $L_l = 2^n$ for some $n \in \mathbb{N}$ and $F_l = 2^m$ for some $m \in \mathbb{N}$. By Lemmas 2.7 and 2.8 we only have to consider four cases: $F_3 = 2$, $F_6 = 8$, $L_0 = 2$ and $L_3 = 4$.

For the first two cases, since (4.2) requires $a > 1$ and $b > 1$, from (3.8) that if there is an exceptional case then $L_{l+\varepsilon}$ must be a square, for $\varepsilon = \pm 1$. But this is clearly impossible.

For the case $L_0 = 2$, we have $3 \cdot 1^2 + 5 \cdot 5^2 = 2^7$, which is not in the form of (4.1). For the case $L_3 = 4$, we have

$$\begin{aligned} 11 \cdot 19^2 + 5^3 &= 2^{12}; \\ 1 \cdot 61^2 + 3 \cdot 5^3 &= 2^{12}. \end{aligned}$$

Note that Theorem 3.1 requires $A > 1$, we cannot apply Theorem 3.1 to the last case. That means it is another exceptional case. ■

It is easy to get the following corollary.

Corollary 4.3. *Except some possible exceptional cases described in Theorem 3.1, Equation* (4.1) *has at most* $2^{\omega(c)+1}$ *solutions* (x, y, z)*. Moreover, the solution* (x, y, z) *satisfies*

$$z < \frac{2ab\sqrt{lm}}{\pi} \log(2eab\sqrt{lm}).$$

5. Other Results

In addition, we shall consider the following three special types of Equation (4.1).

$$a^x + 2 = c^z, \quad x, z \in \mathbb{N},\ a > 1,\ c > 1; \tag{5.1}$$

(5.2) $$a^x + 4 = c^z, \quad x, z \in \mathbb{N},\ a > 1,\ c > 1;$$

(5.3) $$a^x + 2^y = c^z, \quad x, y, z \in \mathbb{N},\ a > 1,\ c > 1 \text{ with } a \text{ and } c \text{ are odd.}$$

In 1984 and 1986, Cao [5, 7], showed that

(1) Suppose that $a, c \in \mathbb{P}$ and $a + 2 = c$ (i.e., a and c are twin primes). Then Equation (5.1) has only solution $(x, z) = (1, 1)$.

(2) Suppose that $a, c \in \mathbb{P}$ and either $at^2 \pm 4 = c$ or $ct^2 \pm 4 = a$ for some $t \in \mathbb{N}$. Then Equation (5.2) has no solutions with $x > 1, z > 1$.

(3) Suppose that $a, c \in \mathbb{P}, at^2 + 4 = c$ and $a \not\equiv 1 \pmod 8$, for some $t \in \mathbb{N}$. Then Equation (5.3) has only the solution $t = a^k, (x, y, z) = (2k + 1, 2, 1)$, where $k \in \mathbb{Z}$ with $k \geq 0$.

Results (1), (2) and (3) can also be found in [6]. By using a lower bound for linear forms in logarithms of algebraic numbers, Terai [25] showed that

(4) Suppose that $a + 2 = c$ with $a \geq 3394$ or $a^2 + 2 = c$ with $a \geq 3$. Then Equation (5.1) has no solutions with $z > 1$ (Theorems 3 and 4 of [25]).

(5) Suppose that $a^\mu + 2 = c$ with $\mu = 1$ or 3, $a \equiv 3$ or $5 \pmod 8$, and $a \geq 1697$ if $\mu = 1$. Then Equation (5.3) has only the solution $(x, y, z) = (\mu, 1, 1)$ (Theorems 5 and 6 of [25]).

Also, some other results on Equation (5.3) can be found in [12] and its references.

Lemma 5.1. [(8, 9, 14)] *Let $a, b \in \mathbb{N}$ with ab not a square. Suppose that $c \in \{1, 2, 4\}, 1 < a \neq c$ and there exist $x, y \in \mathbb{N}$ such that*

$$ax^2 - by^2 = c, \quad x|^*a \quad \text{or} \quad y|^*b.$$

Then

$$\frac{ax^2 + by^2}{2} + xy\sqrt{ab} = \begin{cases} \frac{1}{2}\varepsilon \text{ or } \frac{1}{2}\varepsilon^3, & \text{for } c = 1, \\ \varepsilon \text{ or } \varepsilon^3, & \text{for } c = 2, \\ \Omega \text{ or } \frac{1}{4}\Omega^3, & \text{for } c = 4, \end{cases}$$

except $(a, b, c, x, y) = (5, 1, 4, 5, 11)$. Here $\varepsilon = u_0 + v_0\sqrt{ab}$ and $\Omega = U_0 + V_0\sqrt{ab}$ are the least positive integer solution of Pell's equation $u^2 - abv^2 = 1$ and $U^2 - abV^2 = 4$, respectively.

By applying the above Cao's result on Equations (5.1) and (5.2) we have the following two lemmas.

Lemma 5.2. *Let* $a, c \in \mathbb{N}$ *and* $at^2 + 2 = c$*, where* $t \in \mathbb{N}$*. If Diophantine Equation (5.1) has a solution* (x, z) *with* $xz \equiv 1 \pmod 2$*, then* $t = a^{k-1}, x = 2k - 1, z = 1$*, for some* $k \in \mathbb{N}$*.*

Proof. Since $2 \nmid xz$, Equation (5.1) can be written as

$$(at^2 + 2)((at^2 + 2)^{(z-1)/2})^2 - a(a^{(x-1)/2})^2 = 2. \tag{5.4}$$

Note that it can be shown that ac is not a square. By Lemma 5.1, (5.4) gives

$$\begin{aligned} &\frac{(at^2 + 2)((at^2 + 2)^{(z-1)/2})^2 + a(a^{(x-1)/2})^2}{2} \\ &+ ((at^2 + 2)^{(z-1)/2})(a^{(x-1)/2})\sqrt{a(at^2 + 2)} \\ = \ &\varepsilon \text{ or } \varepsilon^3, \end{aligned} \tag{5.5}$$

where $\varepsilon = u_0 + v_0\sqrt{a(at^2 + 2)}$ is the least positive integral solution of Pell's equation $u^2 - a(at^2 + 2)v^2 = 1$. From [13], we know that $\varepsilon = at^2 + 1 + t\sqrt{a(at^2 + 2)}$. Hence, (5.5) gives

$$\begin{aligned} &\frac{(at^2 + 2)((at^2 + 2)^{(z-1)/2})^2 + a(a^{(x-1)/2})^2}{2} = at^2 + 1, \\ &((at^2 + 2)^{(z-1)/2})(a^{(x-1)/2}) = t, \end{aligned} \tag{5.6}$$

or

$$\begin{aligned} &\frac{(at^2+2)((at^2+2)^{(z-1)/2})^2+a(a^{(x-1)/2})^2}{2} = (at^2+1)(4(at^2)^2+8at^2+1), \\ &((at^2 + 2)^{(z-1)/2})(a^{(x-1)/2}) = t(4(at^2)^2 + 8at^2 + 3). \end{aligned} \tag{5.7}$$

Clearly, (5.6) gives $z = 1, t = a^{(x-1)/2}$, i.e. $t = a^{k-1}, x = 2k - 1$, where $k \in \mathbb{N}$. And we easily check that (5.7) is impossible. ■

Lemma 5.3. *Let* $a, c \in \mathbb{N}$ *and* $at^2 \pm 4 = c$*, where* $t \in \mathbb{N}$*. If the Diophantine equation* (5.2) *has a solution* (x, z) *with* $xz \equiv 1 \pmod 2$*, then* $z = 1$*.*

Proof. Assume that $2 \nmid xz$. Then Equation (5.2) can be written as

$$(at^2 \pm 4)((at^2 \pm 4)^{(z-1)/2})^2 - a(a^{(x-1)/2})^2 = 4. \tag{5.8}$$

Note that it can be shown that ac is not a square. By Lemma 5.1, (5.8) gives

$$\begin{aligned} &\frac{(at^2 \pm 4)((at^2 \pm 4)^{(z-1)/2})^2 + a(a^{(x-1)/2})^2}{2} \\ &+ ((at^2 \pm 4)^{(z-1)/2})(a^{(x-1)/2})\sqrt{a(at^2 \pm 4)} \\ = \ &\Omega \text{ or } \tfrac{1}{4}\Omega^3, \end{aligned} \tag{5.9}$$

where $\Omega = U_0 + V_0\sqrt{ab}$ is the least positive integral solution of Pell's equation $U^2 - abV^2 = 4$. From [13], we know that $\Omega = at^2 \pm 2 + t\sqrt{a(at^2 \pm 4)}$. By using the same argument as in the proof of Lemma 5.2, we get $z = 1$. ■

Nagell [21] showed the following lemma.

Lemma 5.4. *The equation* $x^2 + 2 = y^n, n > 1$ *has only the positive integral solution* $(x, y, n) = (5, 3, 3)$. *The equation* $x^2 + 4 = y^n, n > 1$ *has the only positive integral solutions* $(x, y, n) = (2, 2, 3)$ *or* $(11, 5, 3)$.

Cao and Dong [15] extended the above lemma and provided an elementary proof.

Lemma 5.5. *The equation* $x^2 + 2^m = y^n$, *y odd,* $m > 2$, $n > 1$ *has only the positive integral solutions* $(x, y, m, n) = (7, 3, 5, 4)$ *and* $(x, y, n) = (2^{m-2} - 1, 2^{m-2} + 1, 2)$.

In 1986, Cao [4] claimed that Lemma 5.5 is valid and using Lemma 5.5, Sun and Cao [24] gave all solutions of the Diophantine equation $x^2 + 2^m = y^n,\ x, y, m, n \in \mathbb{N}$, $2|y$, $n > 1$. But in [4], Cao did not give a detail proof. Six years later, Cohn [16] only solved the case $2 \nmid m$. In 1997, Le [19] proved that Lemma 5.5 holds for sufficiently large n. In 1999, Cohn [17] proved that Lemma 5.5 is true in general. In fact, using a result of Y. Bilu, G. Hanrot and P. Voutier [2], and M. Abouzaid [1], we can obtain a simple proof of Lemma 5.5.

Theorem 5.6. *If* $a, c \in \mathbb{N}$ *and* $a^{2k-1} + 2 = c$, *for some* $k \in \mathbb{N}$, *then Equation* (5.1) *has the only solution* $(x, z) = (2k - 1, 1)$.

Proof. Suppose $xz \equiv 1 \pmod 2$. Then Equation (5.1) has the only solution $(x, z) = (2k - 1, 1)$ by Lemma 5.2.

Suppose $x \equiv 0 \pmod 2$. If $z > 1$, then by Lemma 5.4, we have $(a^{\frac{x}{2}}, c, z) = (5, 3, 3)$ which contradicts to the hypothesis that $a^{2k-1} + 2 = c$. If $z = 1$, then by the given assumption we must have $x = 2k - 1$ which is odd. Thus it contradicts to even x.

Suppose $x \equiv 1 \pmod 2$ and $z \equiv 0 \pmod 2$. Then it is clear that both a and c are odd. From (5.1) we have $a + 2 \equiv 1 \pmod 8$. Hence $a = 2^s a_1 - 1$ for some $s \geq 3$ and $a_1 \in \mathbb{N}$ with $a_1 \not\equiv 0 \pmod 2$. Then Equation (5.1) can be written as

$$(2^s a_1 - 1)^x + 2 = ((2^s a_1 - 1)^{2k-1} + 2)^z.$$

Since $x \equiv 1 \pmod 2$ and $z \equiv 0 \pmod 2$, we have

$$(2^s a_1 - 1) + 2 \equiv ((2^s a_1 - 1) + 2)^z \equiv 1 \pmod{2^{s+1}}.$$

Then $a_1 \equiv 0 \pmod 2$, which is impossible. ∎

Theorem 5.7. *If $a, c \in \mathbb{N}$ and $at^2 \pm 4 = c$, where $t \in \mathbb{N}$, then Equation* (5.2) *has only the solution $z = 1$ except $2^5 + 4 = 6^2$.*

Proof.

Case 1. Suppose that $xz \equiv 1 \pmod 2$. Then Equation (5.2) has only the solution $z = 1$ by Lemma 5.3.

Case 2. Suppose that $x \equiv 0 \pmod 2$. Then by Lemma 5.4, we see that Equation (5.2) is impossible since $at^2 \pm 4 = c$.

Case 3. Suppose that $x \equiv 1 \pmod 2$ and $z \equiv 0 \pmod 2$. If $x = 1$, then since $at^2 \pm 4 = c$, from (5.2) we have $t^2 = \frac{c\pm4}{c^z-4} \leq \frac{c+4}{c^2-4} \leq \frac{3}{5}$. Then (5.2) has no solution. So we may assume $x \geq 3$. Suppose both a and c are odd. Then (5.2) gives

$$c^{z/2} - 2 = a_1^x,\ c^{z/2} + 2 = a_2^x,\ a = a_1a_2,\ a_2 > a_1 \geq 1,$$

and so $a_2^x - a_1^x = 4$. Hence,

$$\begin{aligned} 4 = a_2^x - a_1^x &= (a_2 - a_1)(a_2^{x-1} + a_2^{x-2}a_1 + \cdots + a_2a_1^{x-2} + a_1^{x-1}) \\ &\geq a_2^{x-1} + a_2^{x-2}a_1 + \cdots + a_2a_1^{x-2} + a_1^{x-1} > 4, \end{aligned}$$

which is impossible.

Suppose that a or c is even. Then both of them are even. If $z > 2$, then (5.2) gives that $4 \| a^x$. This contradicts to $x \geq 3$. So $z = 2$. Since a and c are even, from $\frac{a^x}{4} + 1 = \left(\frac{c}{2}\right)^2$ we have $2\|c$. From $c = at^2 \pm 4$ we have $2\|a$ and t is odd. By (5.2) we have $a^x = c^2 - 4 = a^2t^4 \pm 8at^2 + 12$. Thus, $a|12$. Hence $a = 2$ or 6. For $a = 2$ we only get $2^5 + 4 = 6^2$. For $a = 6$, (5.2) becomes $2^{x-2}3^{x-1} = 3t^4 \pm 4t^2 + 1$. After taking modulo 3, only $2^{x-2}3^{x-1} = 3t^4 - 4t^2 + 1 = (3t^2 - 1)(t^2 - 1)$ can happen. Since t is odd, $3t^2 - 1 \equiv 2 \pmod 4$. Thus $2\|3t^2 - 1$. As $3 \nmid 3t^2 - 1$ we have $2 = 3t^2 - 1$ and hence $t^2 = 1$. Then $2^{x-2}3^{x-1} = 0$ which is absurd.

This completes the proof. ∎

Theorem 5.8. *If $a, c \in \mathbb{N}$ with $a \not\equiv 1 \pmod 8$ and $at^2 + 2 = c$, where $t \in \mathbb{N}$ with $2^{s+1}|t^2 - 1$ if $2^s\|a + 1$ for some $1 < s \in \mathbb{N}$, then the solutions of Diophantine Equation* (5.3) *are: $(x, y, z, t) = (2k-1, 1, 1, a^{k-1})$; and $(x, y, z, t) = (2, l + 2, 2, 1)$, $a = 2^l - 1$ and $c = 2^l + 1$, where $k \in \mathbb{N}$ and $1 < l \in \mathbb{N}$.*

Proof. We first observe that if $a + 1 \equiv 0 \pmod 8$, then $a + 1 = 2^sa_1$ with $s \geq 3$ and a_1 is odd. Then we have

$$(5.10)\quad a^x \equiv \begin{cases} 2^sa_1 - 1 & \text{if } x \text{ odd} \\ 1 & \text{if } x \text{ even} \end{cases} \equiv \begin{cases} 2^s - 1 & \text{if } x \text{ odd} \\ 1 & \text{if } x \text{ even} \end{cases} \pmod{2^{s+1}}.$$

By the hypothesis of the theorem we have $t^2 \equiv 1 \pmod{2^{s+1}}$. Since $c = at^2 + 2$,

$$(5.11) \qquad c^z \equiv \begin{cases} 2^s a_1 + 1 & \text{if } z \text{ odd} \\ 1 & \text{if } z \text{ even} \end{cases} \equiv \begin{cases} 2^s + 1 & \text{if } z \text{ odd} \\ 1 & \text{if } z \text{ even} \end{cases} \pmod{2^{s+1}}.$$

Suppose $x \equiv 0 \pmod 2$ and $z = 1$. Equation (5.3) becomes

$$(5.12) \qquad a^x + 2^y = at^2 + 2.$$

When $y = 1$. From Equation (5.12) we have $a^x = at^2$. Since x is even, a must be a perfect square. Hence $a \equiv 1 \pmod 8$, which is not the case. It is easy to check that (5.12) is impossible when $y = 2$. So we may assume that $y \geq 3$. Note that t is odd since a is odd. Equation (5.12) gives $1 \equiv a + 2 \pmod 8$ or equivalently $a + 1 \equiv 0 \pmod 8$. By (5.10) and (5.11) we have $1 + 2^y \equiv 2^s + 1 \pmod{2^{s+1}}$. Then we get $y = s$. Since a is odd, from (5.12) we have $a | 2^{s-1} - 1$. Thus $2^{s-1} \geq a + 1 \geq 2^s$, which is impossible.

Suppose $x \equiv 0 \pmod 2$ and $z > 1$. Rewrite Equation (5.3) as $(a^{x/2})^2 + 2^y = c^z$. By Lemmas 5.4 and 5.5, we have

$$\begin{aligned}(a^{x/2}, c, z, y) = \ & (5,3,3,1),\ (2,2,3,2),\ (11,5,3,2),\ (7,3,5,4) \\ & \text{or } (2^{m-2} - 1, 2^{m-2} + 1, 2, m) \text{ for } m \geq 3.\end{aligned}$$

Only the last case is possible. When $m = 3$, we get $a = 1$ which is not the case. When $m \geq 4$, we have $a^{x/2} = 2^{m-2} - 1 \equiv -1 \pmod 4$. It implies that $\frac{x}{2}$ must be odd. Since $2^{m-2} = a^{x/2} + 1 = (a+1)(a^{\frac{x}{2}-1} - \cdots - a + 1) = (a+1) \times$ (an odd integer), $a + 1 = 2^{m-2}$. Hence $x = 2$. So $t = 1$, $a = 2^l - 1$, $c = 2^l + 1$, $y = l + 2$ and $z = 2$, where $l > 1$.

Suppose $xz \equiv 1 \pmod 2$. Equation (5.3) becomes $a + 2^y \equiv c = at^2 + 2 \pmod 8$. Thus t is odd and hence $2^y \equiv 2 \pmod 8$. It gives $y = 1$. So, equation (5.3) has the only solution $t = a^{k-1}$, $x = 2k - 1$ and $z = 1$, where $k \in \mathbb{N}$ by Lemma 5.2.

Finally, suppose $x \equiv 1 \pmod 2$ and $z \equiv 0 \pmod 2$. If $y \geq 3$, then Equation (5.3) becomes $a \equiv 1 \pmod 8$. This contradicts to the assumption. If $y = 2$, then (5.3) gives

$$c^{z/2} - 2 = a_1^x,\ c^{z/2} + 2 = a_2^x,\ a = a_1 a_2,$$

and so $a_2^x - a_1^x = 4$, which is impossible. If $y = 1$, then Equation (5.3) gives $a + 1 \equiv 0 \pmod 8$. By (5.10) and (5.11) we have $2^s - 1 + 1 \equiv 1 \pmod{2^{s+1}}$. It is impossible. ■

Corollary 5.9. *If* $a, c \in \mathbb{N}$ *with* $a \not\equiv 1 \pmod 8$ *and* $a^{2k-1} + 2 = c$*, where* $k \in \mathbb{N}$*, then Diophantine Equation* (5.3) *has the only solutions* $(x, y, z) = (2k-1, 1, 1)$ *and* $(k, a, c, x, y, z) = (1, 2^l - 1, 2^l + 1, 2, l + 2, 2)$*, where* $1 < l \in \mathbb{N}$.

Proof. By taking $t = a^{k-1}$ for some $k \in \mathbb{N}$, we have that if $2^s \parallel a + 1$ then $t^2 - 1 = a^{2k-2} - 1 \equiv 0 \pmod{2^{s+1}}$. Then Theorem 5.5 applies. ■

Corollary 5.9 is an improvement of Theorems 5 and 6 in [25].

Acknowledgment

We would like to thank the referee for pointing out that tables 1-4 in [2] were not complete and referred us to the paper of Abouzaid [1] in which a complete list of n-defective Lucas and Lehmer pairs is given. Our work was mainly based on the n-defectiveness with $n = 3, 5, 7$ and 9. Since for these n, Bilu et al.'s results agree with those of Abouzaid, our argument is safe and sound. We also would like to thank Professor Abouzaid for his valuable information.

References

1. M. Abouzaid, Les nombres de Lucas et Lehmer sans diviseur primitif, *J. de Théorie des Nombres de Bordeaux*, **18** (2006), 299-313.
2. 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.
3. Y. Bugeaud and T. N. Shorey, On the number of solutions of the generalized Ramanujan-Nagell equation, *J. reine angew. Math.*, **539** (2001), 55-74.
4. Zhenfu Cao, The equation $x^2 + 2^m = y^n$ and Hugh Edgar's problem, *Chinese Sci. Bull.*, **31(22)** (1986), 1578-1579.
5. Zhenfu Cao, On a problem of Hall, *J. Math. Res. & Exposition*, **7(3)** (1987), 411-413.
6. Zhenfu Cao, *Introduction to Diophantine equations*, (in Chinese), Harbin Inst. Tech. Press, 1989; MR 92e: 11018.
7. Zhenfu Cao, Hugh Edgar's problem on exponential Diophantine equations, *J. Math.*, **9(2)** (1989), 173-178.
8. Zhenfu Cao, On the equation $ax^m - by^n = 2$ (in Chinese), *Chinese Sci. Bull.*, **35** (1990), 558-559.
9. Zhenfu Cao, *On the Diophantine equation* $(ax^m - 4c)/(abx - 4c) = by^2$ (in Chinese), J. Harbin Inst. Tech. Suppl. (1991), 110-112; MR 95f:11021.
10. Zhenfu Cao, On the Diophantine equation $ax^2 + by^2 = p^z$, *J. Harbin Inst. Tech.*, **23** (1991), 108-111.
11. Zhenfu Cao, Divisibility of the class numbers of imaginary quadratic fields (in Chinese), *Acta Math. Sinica*, **37** (1994), 50-56.

12. Zhenfu Cao, A note on the Diophantine equation $a^x + b^y = c^z$, *Acta Arith.*, **91** (1999), 85-93.

13. Zhenfu Cao, *Diophantine equation and its application* (in Chinese), Shanghai Jiao Tong Univ. Press, 2000.

14. Zhenfu Cao, On the Diophantine equation $x^p + 2^{2m} = py^2$, *Proc. Amer. Math. Soc.*, **128(7)** (2000), 1927-1931.

15. Zhenfu Cao and Xiaolei Dong, The Diophantine equation $Ax^2 + B = y^n$, *Chinese Sci. Bull.*, **43(13)** (1998), 1141-1142.

16. J. H. E. Cohn, The Diophantine equation $x^2 + 2^k = y^n$, *Arch. Math.* (in Basel), **59** (1992), 341-344.

17. J. H. E. Cohn, The Diophantine equation $x^2 + 2^k = y^n$, II, *Internat. J. Math. and Math. Sci.*, **22(3)** (1999), 459-462.

18. L.-K. Hua, *Introduction to Number Theory*, Springer-Verlag, Berlin, 1982.

19. Maohua Le, The Diophantine equation $x^2 + 2^m = y^n$, *Chinese Sci. Bull.*, **42** (1997), 1515-1517.

20. Maohua Le, An upper bound for the number of solutions of the exponential Diophantine equayion $a^x + b^y = c^z$, *Proc. Japan Acad. Ser. A Math. Sci.*, **75** (1999), 90-91.

21. T. Nagell, Contributions to the theory of a category of Diophantine equations of the second degree with two unknowns, *Nova Acta Soc. Sci. Upsal. Ser. IV* (2), **16** (1955), 1-38.

22. M. Perisastri, A note on the equation $a^x - b^y = 10^z$, *Math. Stud.*, **37** (1969), 211-212.

23. R. Scott, On the equations $p^x - b^y = c$ and $a^x + b^y = c^z$, *J. Number Theory*, **44** (1993), 153-165.

24. Q. Sun and Zhenfu Cao, On the equations $x^2 + D^m = p^n$ and $x^2 + 2^m = y^n$, *Journal of Sichuan University Natural Science Edition*, **25(2)** (1988), 164-169.

25. N. Terai, Applications of a lower bound for linear forms in two logarithms to exponential Diophantine equations, *Acta Arith.*, **90** (1999),17-35.

26. P. Voutier, Primitive divisors of Lucas and Lehmer sequences, *Math. Comp.*, **64** (1995), 869-888.

Zhenfu Cao
Department of Computer Science,
Shanghai Jiao Tong University,
Shanghai 200030, P. R. China
E-mail: zfcao@cs.sjtu.edu.cn

Chuan I Chu
1340 Dunrobin Road,
Naperville, IL 60540,
U.S.A.
E-mail: cichu1340@yahoo.com

Wai Chee Shiu*
Department of Mathematics,
Hong Kong Baptist University,
Kowloon Tong, Hong Kong
E-mail: wcshiu@hkbu.edu.hk