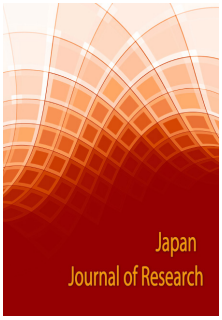
Japan Journal of Research

Original Article



On Matrix Elliptic Curves and Matrix Solutions of the Exponential Diophantine Equation $(X^{24} - I^{24})(Y^{24} - I^{24}) = Z^2$

Joachim Moussounda Mouanda[1], Djagwa Dehainsala[2], Kinvi Kangni[3]

[1]Blessington Christian University, Mathematics Department, Nkayi, Republic of Congo
[2]N'Djamena University, N'Djamena, Tchad
[3]Felix Houphouet Boigny University, Mathematics Department, Abidjan, Ivory Coast

Correspondence
Joachim Moussounda Mouanda
Blessington Christian University, Mathematics Department, Nkayi, Republic of Congo
E-mail: mmoussounda@yahoo.fr

Abstract

We show that the structures of the matrix solutions of the matrix elliptic curves $E_\alpha : Y^2 = X^3 + \alpha \times I_6, \alpha \in \mathbb{N}$ *allow the construction of the matrix solutions of the equations*

$$X^4 + Y^{24} = Z^6, (X^{24} - I_{24})(Y^{24} - I_{24}) = Z^2.$$

***Mathematics Subject Classification(2010)**. 15B36, 11D61.*

- Received Date: 11 Mar 2024
- Accepted Date: 31 Mar 2024
- Publication Date: 10 Apr 2024

Keywords
Matrices of integers, Exponential Diophantine equations

Introduction and Main Result

In the second century A. D, elliptic curves were introduced by the Greek mathematician Diophantus of Alexandria. Properties and functions of elliptic curves have been studies in mathematics for 150 years. In 1920, elliptic curves were studied separately by Cauchy, Lucas, Sylvester, Poincare. In 1984, Lenstra used elliptic curves for factoring integers. More details about elliptic curves can be found in [1]. Let a and b be two different fixed positive integers. The exponential Diophantine equation

$$(a^n - 1)(b^n - 1) = x^2, x, n \in \mathbb{N}, a > 1, b > 1, x \neq 0, n \neq 0, \quad (1.1)$$

has been studied by many authors. In 2000, Szalay studied first the case $(a,b) = (2,3)$ and proved that equation (1.1) has no positive integer solutions. He also showed that, for the case $(a,b) = (2,5)$, equation (1.1) has only the positive integer solution $(n,x) = (1,2)$ and there is no solution for $(a,b) = (2,2^k)$ with $k \geq 2$ expect when $n = 3$ and $k = 2$ [11]. The same year, Hajdu and Szalay showed that there is no solution for $(a,b) = (2,6)$ and $(a,b) = (a,a^k)$, there is no solution with $k \geq 2$ and $kn > 2$ except for the three cases $(a,n,k) \in \{(2,3,2),(3,1,5),(7,1,4)\}$ [5]. In 2002, Cohen investigated the case $a^k = b^l$. He also proved that there is no solutions to (1.1) when $4|n$, expect for $\{a, b\} = \{13, 239\}$ with $n = 4$ [4]. The same year, Walsh and Luca showed that equation (1.1) has finitely positive solutions for fixed (a,b) and proved that the equation has no solution with $n > 2$ for some pairs (a,b) in the range $1 < a < b \leq 100$ [9]. For more details on the equation (1.1), see [3,6-8,10,12,13]. In 2020, Noubissie, Togbe and Zhang showed that the equation (1.1) with b ≡ 3(mod 8), b prime and a even has no solution in positive integers n, x.

Elliptic curves are very important in number theory and constitute an important part of the current research. In 1995, elliptic curves have been used by Wiles to prove the Last Fermat Theorem. Elliptic curves have many applications in elliptic curve cryptography introduced in 1985 by Victor Miller and Neal Koblitz.

In this paper, we show that the structures of the matrix solutions of the matrix elliptic curve $Y^2 = X^3 + I_6$ allow the construction of the matrix solutions of the exponential Diophantine equations:

$$X^4 + Y^{24} = Z^6, (X^{24} - I_{24})(Y^{24} - I_{24}) = Z^2.$$

Theorem 1.1. *Let be a positive integer. Every positive integer x such that* $x > \alpha$ *generates at least 14 matrix points on the matrix elliptic curve*

$$E_\alpha : Y^2 = X^3 + \alpha \times I_6.$$

Theorem 1.2. The matrix Diophantine equation

$$X^4 + Y^{24} = Z^6 \qquad (1.2)$$

has an innite number of matrix solutions which do not have common factors in $M_{24}(\mathbb{N})$.

Theorem 1.3. The matrix exponential Diophantine equation

$$(X^{24} - I_{24})(Y^{24} - I_{24}) = Z^2 \qquad (1.3)$$

has an innite number of matrix solutions in $M_{24}(\mathbb{N})$.

Citation: Mouanda JM, Dehainsala D, Kangni K. On Matrix Elliptic Curves and Matrix Solutions of the Exponential Diophantine Equation $(X^{24} - I_{24})(Y^{24} - I_{24}) = Z^2$. Japan J Res. 2024;5(3):20

Preliminaries

Elliptic Curve Cryptography

Elliptic Curves

Definition 2.1. An elliptic curve is a curve given by an equation of the form $y^2 = p(x)$, where $p(x)$ is a cubic polynomial with no repeated roots.

In the case of an elliptic curve given by the form $y^2 = x^3 + Ax + B$ with the discriminant $\Delta = 4A^3 + 27B^2 \neq 0$, the polynomial $x^3 + Ax + B$ has distinct roots. This allows us to say that the curve is nonsingular. Also, the curve defined by the equation of the form

$$y^2 = Ax^3 + Bx^2 + Cx + D$$

is called the general form of an elliptic curve. Let us add an extra point noted by $\mathcal{O}$ to the curve situated at infinity. Let E be the set defined by

$$E = \{(x, y) : y^2 = x^3 + Ax + B\} \cup \{\mathcal{O}\}.$$

It is possible to use geometry to make the points of an elliptic curve into a group. Let us notice that every line L which has two distinct points of E intersect E on a third point of E. Define the sum of two points P and Q on E, noted as $P \oplus Q$ or just $P + Q$, to be the reflected point on E. Let us see how we can add a point P to itself. Let the point Q approach P. In this case, the line L between P and Q becomes the tangent line to E at P. Then let us take the third intersection point R, reflect across the x-axis, and call the resulting point $P \oplus P$ *or* $2P$. Let $P \in E$. Denote the reflected point of P on E by $-P$. The vertical line L through P and $-P$ does not intersect E in a third point. The fact that there is not point in the plane that works, we create an extra point $\mathcal{O}$ at infinity. We assume that $\mathcal{O}$ is a point on every vertical line.

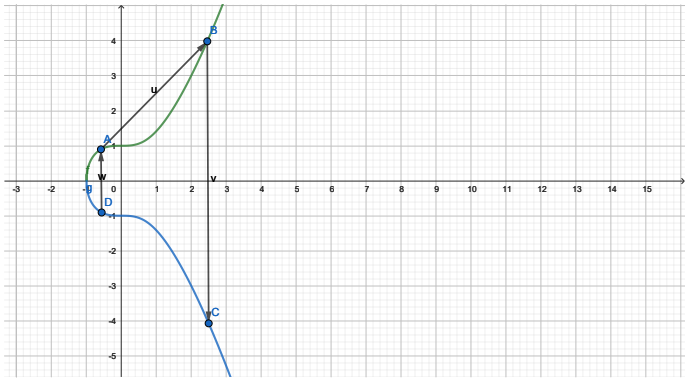


Figure 1: Elliptic Curve

The Algebra of Elliptic Curves

Theorem 2.2. The addition law $\oplus$ on E has the following properties:

$$P \oplus \mathcal{O} = \mathcal{O} \oplus P = P, \forall P \in E$$
$$P \oplus (-P) = \mathcal{O}, \forall P \in E$$
$$P \oplus (Q \oplus R) = (P \oplus Q) \oplus R, \forall P, Q, R \in E\$$
$$P \oplus Q = Q \oplus P, \forall P, Q \in E$$

Let us observe that the addition law makes the points of E into a com- mutative group. An elliptic curve can be seen as a curve that is also naturally a group. In this case, the group law is constructed geometrically. Elliptic curves are not ellipes. Elliptic curves have several applications in many di- verse areas of mathematics (number theory, complex analysis, cryptography and mathematical physics).

Proof of the Main Results

TIn this section, we show that the matrix structures of the matrix solutions of the matrix elliptic curve

$$E_\alpha : Y^2 = X^3 + \alpha \times I_6$$

allow the construction of the matrix solutions of the Diophantine equations

$X^4 + Y^{24} = Z^6$ and $(X^{24} - I_{24})(Y^{24} - I_{24}) = Z^2$.

Proof of Theorem 1.1.

Let x be a positive integer such that $x \neq \alpha$. Let

$$X_x = \begin{pmatrix} 0 & x \\ 1 & 0 \end{pmatrix}$$

be a $2 \times 2 -$ matrix. We can see that

$$X_x^2 = \begin{pmatrix} x & 0 \\ 0 & x \end{pmatrix}.$$

Let

$$A_x = \begin{pmatrix} 0 & X_x & 0 \\ 0 & 0 & X_x \\ I_2 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 & x & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & x \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \end{pmatrix}$$

$$B_x = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ x & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

be two $6 \times 6 -$ matrices. A simple calculation shows that

$$A_x^3 = B_x^6 = \begin{pmatrix} x & 0 & 0 & 0 & 0 & 0 \\ 0 & x & 0 & 0 & 0 & 0 \\ 0 & 0 & x & 0 & 0 & 0 \\ 0 & 0 & 0 & x & 0 & 0 \\ 0 & 0 & 0 & 0 & x & 0 \\ 0 & 0 & 0 & 0 & 0 & x \end{pmatrix} = xI_6. \quad (3.1)$$

The equation (3.1) allows us to construction the matrix solutions in $M_6(\mathbb{N})$ of the matrix elliptic curves

$$E_\alpha : Y^2 = X^3 + \alpha \times I_6:$$

It follows that

$$A_{x-\alpha}^{3}+\alpha\times I_6=xI_6=\begin{pmatrix}0&0&0&0&0&1\\0&0&x&0&0&0\\0&1&0&0&0&0\\0&0&0&0&1&0\\0&0&0&x&0&0\\x&0&0&0&0&0\end{pmatrix}^2=\begin{pmatrix}0&0&0&0&0&x\\0&0&1&0&0&0\\0&x&0&0&0&0\\0&0&0&0&x&0\\0&0&0&1&0&0\\1&0&0&0&0&0\end{pmatrix}^2.$$

It is clear that the matrix points

$$P_{x,\alpha,1}=\left(\begin{pmatrix}0&0&0&x-\alpha&0&0\\0&0&1&0&0&0\\0&0&0&0&0&x-\alpha\\0&0&0&0&1&0\\1&0&0&0&0&0\\0&1&0&0&0&0\end{pmatrix},\begin{pmatrix}0&0&0&0&0&1\\0&0&x&0&0&0\\0&1&0&0&0&0\\0&0&0&0&1&0\\0&0&0&x&0&0\\x&0&0&0&0&0\end{pmatrix}\right),$$

$$P_{x,\alpha,2}=\left(\begin{pmatrix}0&0&0&x-\alpha&0&0\\0&0&1&0&0&0\\0&0&0&0&0&x-\alpha\\0&0&0&0&1&0\\1&0&0&0&0&0\\0&1&0&0&0&0\end{pmatrix},\begin{pmatrix}0&0&0&0&0&1\\0&0&-x&0&0&0\\0&-1&0&0&0&0\\0&0&0&0&1&0\\0&0&0&x&0&0\\x&0&0&0&0&0\end{pmatrix}\right),$$

$$P_{x,\alpha,3}=\left(\begin{pmatrix}0&0&0&x-\alpha&0&0\\0&0&1&0&0&0\\0&0&0&0&0&x-\alpha\\0&0&0&0&1&0\\1&0&0&0&0&0\\0&1&0&0&0&0\end{pmatrix},\begin{pmatrix}0&0&0&0&0&-1\\0&0&x&0&0&0\\0&1&0&0&0&0\\0&0&0&0&1&0\\0&0&0&x&0&0\\-x&0&0&0&0&0\end{pmatrix}\right),$$

$$P_{x,\alpha,4}=\left(\begin{pmatrix}0&0&0&x-\alpha&0&0\\0&0&1&0&0&0\\0&0&0&0&0&x-\alpha\\0&0&0&0&1&0\\1&0&0&0&0&0\\0&1&0&0&0&0\end{pmatrix},\begin{pmatrix}0&0&0&0&0&1\\0&0&-x&0&0&0\\0&-1&0&0&0&0\\0&0&0&0&-1&0\\0&0&0&-x&0&0\\x&0&0&0&0&0\end{pmatrix}\right),$$

$$P_{x,\alpha,5}=\left(\begin{pmatrix}0&0&0&x-\alpha&0&0\\0&0&1&0&0&0\\0&0&0&0&0&x-\alpha\\0&0&0&0&1&0\\1&0&0&0&0&0\\0&1&0&0&0&0\end{pmatrix},\begin{pmatrix}0&0&0&0&0&1\\0&0&x&0&0&0\\0&1&0&0&0&0\\0&0&0&0&-1&0\\0&0&0&-x&0&0\\x&0&0&0&0&0\end{pmatrix}\right),$$

$$P_{x,\alpha,6}=\left(\begin{pmatrix}0&0&0&x-\alpha&0&0\\0&0&1&0&0&0\\0&0&0&0&0&x-\alpha\\0&0&0&0&1&0\\1&0&0&0&0&0\\0&1&0&0&0&0\end{pmatrix},\begin{pmatrix}0&0&0&0&0&-1\\0&0&-x&0&0&0\\0&-1&0&0&0&0\\0&0&0&0&-1&0\\0&0&0&-x&0&0\\-x&0&0&0&0&0\end{pmatrix}\right),$$

$$P_{x,\alpha,7}=\left(\begin{pmatrix}0&0&0&x-\alpha&0&0\\0&0&1&0&0&0\\0&0&0&0&0&x-\alpha\\0&0&0&0&1&0\\1&0&0&0&0&0\\0&1&0&0&0&0\end{pmatrix},\begin{pmatrix}0&x&0&0&0&0\\1&0&0&0&0&0\\0&0&0&x&0&0\\0&0&1&0&0&0\\0&0&0&0&0&1\\0&0&0&0&x&0\end{pmatrix}\right),$$

$$P_{x,\alpha,8}=\left(\begin{pmatrix}0&0&0&x-\alpha&0&0\\0&0&1&0&0&0\\0&0&0&0&0&x-\alpha\\0&0&0&0&1&0\\1&0&0&0&0&0\\0&1&0&0&0&0\end{pmatrix},\begin{pmatrix}0&-x&0&0&0&0\\-1&0&0&0&0&0\\0&0&0&x&0&0\\0&0&1&0&0&0\\0&0&0&0&0&1\\0&0&0&0&x&0\end{pmatrix}\right),$$

$$P_{x,\alpha,9}=\left(\begin{pmatrix}0&0&0&x-\alpha&0&0\\0&0&1&0&0&0\\0&0&0&0&0&x-\alpha\\0&0&0&0&1&0\\1&0&0&0&0&0\\0&1&0&0&0&0\end{pmatrix},\begin{pmatrix}0&x&0&0&0&0\\1&0&0&0&0&0\\0&0&0&-x&0&0\\0&0&-1&0&0&0\\0&0&0&0&0&1\\0&0&0&0&x&0\end{pmatrix}\right),$$

$$P_{x,\alpha,10}=\left(\begin{pmatrix}0&0&0&x-\alpha&0&0\\0&0&1&0&0&0\\0&0&0&0&0&x-\alpha\\0&0&0&0&1&0\\1&0&0&0&0&0\\0&1&0&0&0&0\end{pmatrix},\begin{pmatrix}0&x&0&0&0&0\\1&0&0&0&0&0\\0&0&0&x&0&0\\0&0&1&0&0&0\\0&0&0&0&0&-1\\0&0&0&0&-x&0\end{pmatrix}\right),$$

$$P_{x,\alpha,11}=\left(\begin{pmatrix}0&0&0&x-\alpha&0&0\\0&0&1&0&0&0\\0&0&0&0&0&x-\alpha\\0&0&0&0&1&0\\1&0&0&0&0&0\\0&1&0&0&0&0\end{pmatrix},\begin{pmatrix}0&-x&0&0&0&0\\-1&0&0&0&0&0\\0&0&0&-x&0&0\\0&0&-1&0&0&0\\0&0&0&0&0&1\\0&0&0&0&x&0\end{pmatrix}\right),$$

$$P_{x,\alpha,12}=\left(\begin{pmatrix}0&0&0&x-\alpha&0&0\\0&0&1&0&0&0\\0&0&0&0&0&x-\alpha\\0&0&0&0&1&0\\1&0&0&0&0&0\\0&1&0&0&0&0\end{pmatrix},\begin{pmatrix}0&x&0&0&0&0\\1&0&0&0&0&0\\0&0&0&-x&0&0\\0&0&-1&0&0&0\\0&0&0&0&0&-1\\0&0&0&0&-x&0\end{pmatrix}\right),$$

$$P_{x,\alpha,13}=\left(\begin{pmatrix}0&0&0&x-\alpha&0&0\\0&0&1&0&0&0\\0&0&0&0&0&x-\alpha\\0&0&0&0&1&0\\1&0&0&0&0&0\\0&1&0&0&0&0\end{pmatrix},\begin{pmatrix}0&-x&0&0&0&0\\-1&0&0&0&0&0\\0&0&0&x&0&0\\0&0&1&0&0&0\\0&0&0&0&0&-1\\0&0&0&0&-x&0\end{pmatrix}\right),$$

$$P_{x,\alpha,14} = \left(\begin{pmatrix} 0 & 0 & 0 & x-\alpha & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & x-\alpha \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & -x & 0 & 0 & 0 & 0 \\ -1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -x & 0 & 0 \\ 0 & 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 \\ 0 & 0 & 0 & 0 & -x & 0 \end{pmatrix} \right)$$

are elements of E. Finally, every positive integer greater than α generates at least 14 matrix points of the matrix elliptic curve E_α.

The matrix structures of A_x and B_x allow us to construct the matrix solutions which do not have common factors of the Diophantine equation

$$X^4 + Y^{24} = Z^6. \qquad (3.2)$$

Proof of Theorem 1.2

Let x be a positive integer and let

$$H_x = \begin{pmatrix} 0 & A_x & 0 & 0 \\ 0 & 0 & A_x & 0 \\ 0 & 0 & 0 & A_x \\ I_6 & 0 & 0 & 0 \end{pmatrix}$$

be a 24 24-matrix with

$$A_x = \begin{pmatrix} 0 & 0 & 0 & x & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & x \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

Therefore,

$$Hx = \begin{pmatrix}
0&0&0&0&0&0&0&0&0&x&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&x&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&x&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&x&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&x&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1\\
1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0
\end{pmatrix}$$

A simple calculation shows that

$$H_x^4 = \begin{pmatrix} A_x^3 & 0 & 0 & 0 \\ 0 & A_x^3 & 0 & 0 \\ 0 & 0 & A_x^3 & 0 \\ 0 & 0 & 0 & A_x^3 \end{pmatrix} = \begin{pmatrix} xI_6 & 0 & 0 & 0 \\ 0 & xI_6 & 0 & 0 \\ 0 & 0 & xI_6 & 0 \\ 0 & 0 & 0 & xI_x \end{pmatrix} = xI_{24}$$

$$Jx = \begin{pmatrix}
0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1\\
\mathrm{x}&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0
\end{pmatrix}$$

be a Rare matrix of order 24 and index 1. A simple calculation shows that $J_x^{24} = xI_{24} = H_x^4$. Therefore, $H_x^4 + J_y^{24} = Q_{x,y}^6$ *with*

$$Q_{x,y} = \begin{pmatrix}
0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1\\
\alpha&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&\alpha&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&\alpha&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&\alpha&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0
\end{pmatrix}$$

$\alpha = x + y, x, y \in \mathbb{N}$ The triple (H_x, J_y,$Q_{x,y}$) is a matrix solution of the equation $X^4 + Y^{24} = Z^6$. Finally, the matrix Diophantine equation $X^4 + Y^{24} = Z^6$ has an infinite number of matrix solutions which do not have common factors.

Now, we can introduce the matrix solutions of the matrix exponential Diophantine equation $(X^{24} + I_{24})(Y^{24} + I_{24}) = Z^2$

Proof of Theorem 1.3

Let x be a positive integer and let

$$J_x = \begin{pmatrix}
0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1\\
x&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0
\end{pmatrix}$$

be a Rare matrix of order 24 and index 1. A simple calculation shows that

$$J_x^{24} = xI_{24}.$$

The matrix structure of J_x allows us to claim that

$$(J_{x^2+1}^{24} - I_{24})(J_{y^2+1}^{24} - I_{24}) = B_{x,y}^2$$

where

$$B_{x,y} = xy \begin{pmatrix}
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0
\end{pmatrix}$$

for all positive integers $x,y \in N$ such that $x \neq 0$ and $y \neq 0$. Finally, the elements of the sequences of matrix triples

$$(J_{x^2+1}, J_{y^2+1}, B_{x,y})_{x,y\in\mathbb{N}}$$

are matrix solutions of the exponential Diophantine equation

$$(X^{24} - I_{24})(Y^{24} - I_{24}) = Z^2.$$

We could deduce, from the structure of J_x, the matrix solutions of the exponential Diophantine equation

$$(X^{24} + I_{24})(Y^{24} + I_{24}) = Z^2.$$

In other words, the the elements of the sequences of matrix triples

$$(J_{x^2-1}, J_{y^2-1}, B_{x,y})_{x,y\in\mathbb{N}}$$

are matrix solutions of the exponential Diophantine equation

$$(X^{24} + I_{24})(Y^{24} + I_{24}) = Z^2.$$

References

1. Barsagade MW, Meshram S. Overview of History of Elliptic Curves and its use in cryptography. Inter J Sci Eng Res. 2014;5(4):467-471.
2. A. Noubissie, A. Togbé, Zhongfeng Zhang: On the exponential Diophantine equation (an−1)(bn−1)=x2, Bulletin of the Belgian Mathematical Society - Simon Stevin 27(2)(2020):161-166.
3. Carmichael RD. On the numerical factor of the arithmetic form $\alpha^n \pm \beta^n$. Ann Math. 1913;15(2):30-70.
4. Cohn JE. The Diophantine equation $(a^n-1)(b^n-1) = x^2$. Period Math

Hungar. 2002;44(2):169-175.

5. Hajdu L, Szalay L. On the Diophantine equation $(2^n-1)(6^n-1) = x^2$ and $(a^n-1)((ak)^n-1) = x^2$. Period Math Hungar. 2002;40(2):144-145.
6. Ishii K. On the exponential Diophantine equation $(a^n-1)(b^n-1) = x^2$. Publ Math Debrecen. 2016;89:253-256.
7. Lan L, Szalay L. On the exponential Diophantine equation $(a^n-1)(b^n-1) = x^2$. Publ Math Debrecen. 2010;77:1-6.
8. Luca F. A note on the Pell equation. Indian J Math. 1997;39:99-105.
9. Luca F, Walsh PG. The product of like-indexed terms in binary recurrences. J Number Theory. 2002;96:152-173.
10. van der Waall RW. On the Diophantine equation $x^2+x+1 = 3y^2$, $x^3-1 = 2y^2$, and $x^3+1 = 2y$. Simon Stevin. 1972;46:39-51.
11. Szalay L. On the Diophantine equation $(2^n- 1)(3^n- 1) = x^2$. Publ Math Debrecen. 2000;57(2):1-9.
12. Xioyan G. A Note On the Diophantine equation $(a^n-1)(b^n-1) = x^2$. Period Math Hungar. 2013;66:87-93.
13. Yuan P, Zhang Z. On the Diophantine equation $(a^n-1)(b^n-1) = x^2$. Publ Math Debrecen. 2012;80:327-331.