JP Journal of Algebra, Number Theory and Applications
© 2026 Pushpa Publishing House, Prayagraj, India
https://pphmjopenaccess.com
https://doi.org/10.17654/0972555526001 P-ISSN: 0972-5555
Volume 65, Number 1, January 2026, Pages 1-20 E-ISSN: 3049-2084

MATRIX SOLUTIONS FOR THE NON-LINEAR EXPONENTIAL DIOPHANTINE EQUATION $(X^a + \alpha I_q)^m + (Y^b + \beta I_q)^n = Z^2$, $\alpha, \beta \in \mathbb{Z}, a, b, m, n, q \in \mathbb{N}, X, Y, Z \in M_q(\mathbb{N})$

Kolo F. Soro*, **Eric D. Akéké and Jean R. Tsiba**

UFR-ST
Mathematics and Computer Sciences
Alassane Ouattara University
Bouaké, Côte d'Ivoire
e-mail: koloetienne180@gmail.com

UFR-MI
Mathematics and Applications Laboratory
Félix Houphouët-Boigny University
Abidjan, Côte d'Ivoire
e-mail: ericdago@yahoo.fr

Received: April 25, 2025; Revised: July 12, 2025; Accepted: September 1, 2025
2020 Mathematics Subject Classification: 15B36, 11D72, 11D61.
Keywords and phrases: Exponential Diophantine equation, Rare matrices.
*Corresponding author

How to cite this article: Kolo F. Soro, Eric D. Akéké and Jean R. Tsiba, Matrix solutions for the non-linear exponential Diophantine equation $(X^a + \alpha I_q)^m + (Y^b + \beta I_q)^n = Z^2$, $\alpha, \beta \in \mathbb{Z}$, $a, b, m, n, q \in \mathbb{N}$, $X, Y, Z \in M_q(\mathbb{N})$, JP Journal of Algebra, Number Theory and Applications 65(1) (2026), 1-20. https://doi.org/10.17654/0972555526001

Published Online: November 17, 2025

Sékou TRAORE Mathematics Laboratory
Mathematics Department
Blessington Christian University
Nkayi, Republic of Congo
e-mail: jrtsiba@hotmail.com

Abstract

We investigate matrix solutions for the non-linear exponential Diophantine equation

$$(X^a + \alpha I_q)^m + (Y^b + \beta I_q)^n = Z^2,$$

where $\alpha, \beta \in \mathbb{Z}$ and $a, b, m, n, q \in \mathbb{N}$ such that q is a common multiple of a and b. We show that this equation admits an infinite number of matrix solutions which do not depend on m and n.

1. Introduction

Finding the solutions of Diophantine equations has many challenges for researchers due to the absence of generalized methods. Certainly, the resolution of Diophantine equations requires integers, in the most cases, the solutions are limited or do not exist. In [4], Ivorra and Kraus studied the equation $ax^p + by^p = cz^2$, where p is a prime number greater or equal to 5. In application, they obtained results concerning the $\mathbb{Q}$-rational points of hyperelliptic curves given by the Diophantine equation $y^2 = x^p + d$, with $d \in \mathbb{Z}$. In [3], Gupta et al. discussed the solutions of the Diophantine equation

$$(x^a + 1)^m + (y^b + 1)^n = z^2, \tag{1}$$

under some conditions. They proved that for a, b, m, n, y and z being elements of a given subset of integers and x a prime divisor of y such that $x \equiv 3$ or $5 \pmod 8$, equation (1) has no solution in this subset. For a long time, some researchers have been interested in the search for matrix solutions of Diophantine equations [1, 2]. Mouanda and his team [5-8] showed that some matrix Diophantine equations admit an infinite number of matrix solutions with positive integers as entries.

The solutions of Diophantine equations have many applications in the field of cryptography and applied algebra.

Our paper is organized as follows. In Section 2, we recall some necessary definitions and relate results. In Section 3, we show that, for positive integers a, b, m, n, q such that $(a, b) \neq (0, 0)$, the common multiple q of a and b, and $\alpha, \beta \in \mathbb{Z}$, the non-linear exponential Diophantine equation

$$(X^a + \alpha I_q)^m + (Y^b + \beta I_q)^n = Z^2,$$

admits an infinite number of matrix solutions which do not depend on the choice of m and n.

2. Preliminaries

We recall some definitions on matrices and observations made by Mouanda in [7].

Definition 2.1 [6]**.** Let $a, b, c \in \mathbb{C}^*$ be complex numbers. Then $n \times n$-matrices of the form

$$c\begin{pmatrix} 0 & 1 & 0 & \cdots & 0 & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 & 0 \\ 0 & 0 & 0 & \cdots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \cdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & 1 & 0 \\ 0 & 0 & 0 & \cdots & 0 & 0 & 1 \\ a & 0 & 0 & \cdots & 0 & 0 & 0 \end{pmatrix} \quad \text{or} \quad c\begin{pmatrix} 0 & 0 & 0 & \cdots & 0 & 0 & b \\ 1 & 0 & 0 & \cdots & 0 & 0 & 0 \\ 0 & 1 & 0 & \cdots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \cdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & 0 & 0 \\ 0 & 0 & 0 & \cdots & 1 & 0 & 0 \\ 0 & 0 & 0 & \cdots & 0 & 1 & 0 \end{pmatrix}$$

are called *Rare matrices* of order n and index 1. The index designates the number of complex coefficients different from 0 and 1.

We have the following interesting properties on Rare matrices.

Remark 2.1 [7]**.** Let

$$A_x = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 & 0 \\ 0 & 0 & 0 & \cdots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \cdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & 1 & 0 \\ 0 & 0 & 0 & \cdots & 0 & 0 & 1 \\ x & 0 & 0 & \cdots & 0 & 0 & 0 \end{pmatrix} \in M_n(\mathbb{C}), \quad x \neq 0$$

be a Rare matrix of order n and index 1. Then

$$A_x^n = \begin{pmatrix} x & 0 & 0 & \cdots & 0 & 0 & 0 \\ 0 & x & 0 & \cdots & 0 & 0 & 0 \\ 0 & 0 & x & \cdots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \cdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & x & 0 & 0 \\ 0 & 0 & 0 & \cdots & 0 & x & 0 \\ 0 & 0 & 0 & \cdots & 0 & 0 & x \end{pmatrix}, \quad A_x^{-1} = \begin{pmatrix} 0 & 0 & 0 & \cdots & 0 & 0 & \frac{1}{x} \\ 1 & 0 & 0 & \cdots & 0 & 0 & 0 \\ 0 & 1 & 0 & \cdots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \cdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & 0 & 0 \\ 0 & 0 & 0 & \cdots & 1 & 0 & 0 \\ 0 & 0 & 0 & \cdots & 0 & 1 & 0 \end{pmatrix},$$

$$A_x^{-1} = A_{\frac{1}{x}}^T, \quad A_x^n = xI_n, \quad (\gamma A_x)^{-1} = \frac{1}{\gamma} A_x^{-1}, \quad \gamma \neq 0.$$

Definition 2.2 [8]**.** A matrix $B \in M_n(\mathbb{N})$ is a *construction structure* of matrix solutions of Diophantine equations if there exist two positive integers m, β such that $B^m - \beta \times I_n = 0$.

Denote by

$$D_n(\mathbb{N}) = \{B \in M_n(\mathbb{N}) : B^m - \beta \times I_n = 0,\ m, \beta \in \mathbb{N}^*\}$$

the set of all construction structures of matrix solutions of Diophantine equations from $M_n(\mathbb{N})$. It is easy to check that for all $B \in D_n(\mathbb{N})$, $\det(B) \neq 0$, where $\det(B)$ denotes the determinant of the matrix B.

Definition 2.3. Let $n, m \in \mathbb{N}^*$, $A = (a_{ij})_{1 \le i, j \le n} \in M_n(\mathbb{C})$ and $B = (b_{ij})_{1 \le i, j \le m} \in M_m(\mathbb{C})$. Then the *Kronecker product* of A and B is the matrix $A \otimes B$ defined by

$$A \otimes B = \begin{pmatrix} a_{11}B & a_{12}B & \cdots & a_{1n}B \\ a_{21}B & a_{22}B & \cdots & a_{2n}B \\ \vdots & \vdots & \cdots & \vdots \\ a_{n1}B & a_{n2}B & \cdots & a_{nn}B \end{pmatrix}.$$

It is known that for $n, m \in \mathbb{N}^*$, $A \in M_n(\mathbb{C})$ and $B \in M_m(\mathbb{C})$, in general, $A \otimes B \neq B \otimes A$. Moreover,

$$I_n \otimes I_m = I_m \otimes I_n = I_{n \times m}.$$

3. Matrix Solutions of the Exponential Diophantine Equation $(X^a + \alpha I_q)^m + (Y^b + \beta I_q)^n = Z^2$

Denote by $R_r(\mathbb{N})$ the set of all Rare matrices of order r and index 1, for $r \geq 2$, that is,

$$R_r(\mathbb{N}) = \left\{ \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 & 0 \\ 0 & 0 & 0 & \cdots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \cdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & 1 & 0 \\ 0 & 0 & 0 & \cdots & 0 & 0 & 1 \\ x & 0 & 0 & \cdots & 0 & 0 & 0 \end{pmatrix} \in M_r(\mathbb{N}),\ x \neq 0 \right\}.$$

Therefore,

$$R_r(\mathbb{N}) \subset D_r(\mathbb{N}) \subset M_r(\mathbb{N}).$$

3.1. Case 1: $a = 0$ **or** $b = 0$

Without restricting the problem, suppose that $b = 0$ and $a \neq 0$. Similar results are obtained for $a = 0$ and $b \neq 0$. For the case where a is an even number, we have the following:

Proposition 3.1. *Let* α *be an integer and* β, a, x *be positive integers such that* $a = 2q$, $q \in \mathbb{N}^*$ *and* $x > |\alpha|$. *Let* $R_a(\mathbb{N})$ *be the set of all Rare matrices of order a and index* 1. *Let* A_x, $A_{\eta_x} \in R_a(\mathbb{N})$, *with*

$$\eta_x = (x + \alpha)^m + (\beta + 1)^n.$$

The terms of the sequence of matrices $(A_x, A_{\eta_x}^q)_{x > |\alpha|}$ *are matrix solutions of the Diophantine equation*

$$(X^a + \alpha I_a)^m + (\beta + 1)^n I_a = Z^2.$$

Proof. Notice that for $x > |\alpha|$, η_x is a non-zero positive integer. Therefore,

$$(A_x^a + \alpha I_a)^m + (\beta + 1)^n I_a = [(x + \alpha) I_a]^m + (\beta + 1)^n I_a$$

because $A_x \in R_a(\mathbb{N})$. Hence,

$$(A_x^a + \alpha I_a)^m + (\beta + 1)^n I_a = (x + \alpha)^m I_a + (\beta + 1)^n I_a.$$

So,

$$(A_x^a + \alpha I_a)^m + (\beta + 1)^n I_a = \eta_x I_a = A_{\eta_x}^a = (A_{\eta_x}^q)^2.$$

Consequently, for $x > |\alpha|$, $(A_x^a + \alpha I_a)^m + (\beta + 1)^n I_a = (A_{\eta_x}^q)^2$ and the result follows. □

Now, we investigate the case where a is an odd number.

Proposition 3.2. *Let* α *be an integer and let* β, a, x *be positive integers such that* $a = 2q + 1$, $q \in \mathbb{N}$ *and* $x > |\alpha|$. *Let* $R_{2a}(\mathbb{N})$ *be the set* *of all Rare matrices of order* $2a$ *and index* 1. *Let* $A_x, A_{\eta_x} \in R_{2a}(\mathbb{N})$ *with*

$$\eta_x = (x+\alpha)^m + (\beta+1)^n.$$

Then, the terms of the sequence of matrices $(A_x^2, A_{\eta_x}^a)_{x>|\alpha|}$ *are matrix solutions of the Diophantine equation*

$$(X^a + \alpha I_{2a})^m + (\beta+1)^n I_{2a} = Z^2.$$

Proof. Suppose that $x > |\alpha|$ and $A_x, A_{\eta_x} \in R_{2a}(\mathbb{N})$. Then

$$[(A_x^2)^a + \alpha I_{2a}]^m + (\beta+1)^n I_{2a} = (A_x^{2a} + \alpha I_{2a})^m + (\beta+1)^n I_{2a}$$

$$= [(x+\alpha) I_{2a}]^m + (\beta+1)^n I_{2a},$$

due to the fact that $A_x \in R_{2a}(\mathbb{N})$. Therefore,

$$[(A_x^2)^a + \alpha I_{2a}]^m + (\beta+1)^n I_{2a} = (x+\alpha)^m I_{2a} + (\beta+1)^n I_{2a}.$$

Hence

$$[(A_x^2)^a + \alpha I_{2a}]^m + (\beta+1)^n I_{2a} = \eta_x I_{2a} = A_{\eta_x}^{2a} = (A_{\eta_x}^a)^2$$

and the result follows. □

3.2. Case 2: $a \neq 0$ and $b \neq 0$

Consider $\alpha, \beta \in \mathbb{Z}$. Then for $x, y, n, m \in \mathbb{N}$ such that $x > |\alpha|$ and $y > |\beta|$, write $\gamma_{m,n}(x, y) = (x+\alpha)^m + (y+\beta)^n$. Then it follows that $\gamma_{m,n}(x, y) > 0$.

Proposition 3.3. *Let* a, b, x, y *be non-zero positive integers and* ℓ *be the least common multiple of a and b. Suppose that* ℓ *is an even number and let* $A_x, A_y, A_{\gamma_{m,n}(x,y)} \in R_\ell(\mathbb{N})$ *be Rare matrices of order* ℓ *and index* 1, *with*

$$\gamma_{m,n}(x, y) = (x + \alpha)^m + (y + \beta)^n.$$

Then, the terms of the sequence of matrices

$$(A_x^r, A_y^s, A_{\gamma_{m,n}(x,y)}^t)_{x>|\alpha|, y>|\beta|}$$

are matrix solutions of the Diophantine equation

$$(X^a + \alpha I_\ell)^m + (Y^b + \beta I_\ell)^n = Z^2, \quad \ell = ar = sb = 2t.$$

Proof. Since $A_x, A_y, A_{\gamma_{m,n}(x,y)} \in R_\ell(\mathbb{N})$ and $\ell = ar = sb = 2t$,

$$[(A_x^r)^a + \alpha I_\ell]^m + [(A_y^s)^b + \beta I_\ell]^n = [A_x^{ra} + \alpha I_\ell]^m + [A_y^{sb} + \beta I_\ell]^n$$

$$= [A_x^\ell + \alpha I_\ell]^m + [A_y^\ell + \beta I_\ell]^n.$$

Due to the fact that $A_x^\ell = xI_\ell$ and $A_y^\ell = yI_\ell$,

$$[(A_x^r)^a + \alpha I_\ell]^m + [(A_y^s)^b + \beta I_\ell]^n = [(x + \alpha)I_\ell]^m + [(y + \beta)I_\ell]^n.$$

Therefore,

$$[(A_x^r)^a + \alpha I_\ell]^m + [(A_y^s)^b + \beta I_\ell]^n = (x + \alpha)^m I_\ell + (y + \beta)^n I_\ell.$$

As $\gamma_{m,n}(x, y) = (x + \alpha)^m + (y + \beta)^n$,

$$[(A_x^r)^a + \alpha I_\ell]^m + [(A_y^s)^b + \beta I_\ell]^n = \gamma_{m,n}(x, y)I_\ell = A_{\gamma_{m,n}(x,y)}^\ell.$$

So,

$$[(A_x^r)^a + \alpha I_\ell]^m + [(A_y^s)^b + \beta I_\ell]^n = A_{\gamma_{m,n}(x,y)}^{2t} = (A_{\gamma_{m,n}(x,y)}^t)^2. \qquad \square$$

In the case where ℓ is an odd number, we have the following:

Proposition 3.4. *Let* a, b, x, y *be non-zero positive integers and* ℓ *be the least common multiple of a and b. Suppose that* ℓ *is an odd number and let* $A_x, A_y, A_{\gamma_{m,n}(x,y)} \in R_{2\ell}(\mathbb{N})$ *be Rare matrices of order* 2ℓ *and index* 1, *with*

$$\gamma_{m,n}(x, y) = (x+\alpha)^m + (y+\beta)^n.$$

Then, the terms of the sequence of matrices

$$(A_x^r, A_y^s, A_{\gamma_{m,n}(x,y)}^{\ell})_{x>|\alpha|, y>|\beta|} \subset (M_{\ell}(\mathbb{N}))^3$$

are matrix solutions of the Diophantine equation

$$(X^a + \alpha I_{2\ell})^m + (Y^b + \beta I_{2\ell})^n = Z^2, \quad 2\ell = ar = bs.$$

Proof. Suppose that $A_x, A_y, A_{\gamma_{m,n}(x,y)} \in R_{2\ell}(\mathbb{N})$. Then

$$[(A_x^r)^a + \alpha I_{2\ell}]^m + [(A_y^s)^b + \beta I_{2\ell}]^n = [A_x^{ar} + \alpha I_{2\ell}]^m + [A_y^{bs} + \beta I_{2\ell}]^n.$$

Since $2\ell = ar = bs$,

$$[(A_x^r)^a + \alpha I_{2\ell}]^m + [(A_y^s)^b + \beta I_{2\ell}]^n = [A_x^{2\ell} + \alpha I_{2\ell}]^m + [A_y^{2\ell} + \beta I_{2\ell}]^n.$$

Due to the fact that $A_x^{2\ell} = xI_{2\ell}$ and $A_y^{2\ell} = yI_{2\ell}$,

$$[A_x^{2\ell} + \alpha I_{2\ell}]^m + [A_y^{2\ell} + \beta I_{2\ell}]^n = [(x+\alpha)I_{2\ell}]^m + [(y+\beta)I_{2\ell}]^n.$$

This implies that

$$[(A_x^r)^a + \alpha I_{2\ell}]^m + [(A_y^s)^b + \beta I_{2\ell}]^n = (x+\alpha)^m I_{2\ell} + (y+\beta)^n I_{2\ell}.$$

So,

$$[(A_x^r)^a + \alpha I_{2\ell}]^m + [(A_y^s)^b + \beta I_{2\ell}]^n = \gamma_{m,n}(x, y) I_{2\ell} = A_{\gamma_{m,n}(x,y)}^{2\ell}.$$

Therefore,

$$[(A_x^r)^a + \alpha I_{2\ell}]^m + [(A_y^s)^b + \beta I_{2\ell}]^n = (A_{\gamma_{m,n}(x,y)}^{\ell})^2. \qquad \square$$

Now, we investigate the Kronecker product of Rare matrices.

Lemma 1. *Let* x, r, p *be non-zero positive integers such that* $r \geq 2$ *and* $A_x \in R_r(\mathbb{N})$ *be a Rare matrix of order r and index* 1. *Then*

$$(A_x \otimes I_p)^r = (I_p \otimes A_x)^r = xI_{rp}.$$

Proof. Suppose $A_x \in R_r(\mathbb{N})$ with $r \geq 2$. Then $A_x^r = xI_r$.

(a) We show that $(I_p \otimes A_x)^r = xI_{rp}$. Notice that

$$(I_p \otimes A_x)^r = \begin{pmatrix} A_x & 0 & 0 & \cdots & 0 & 0 & 0 \\ 0 & A_x & 0 & \cdots & 0 & 0 & 0 \\ 0 & 0 & A_x & \cdots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \cdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & A_x & 0 & 0 \\ 0 & 0 & 0 & \cdots & 0 & A_x & 0 \\ 0 & 0 & 0 & \cdots & 0 & 0 & A_x \end{pmatrix}^r$$

$$= \begin{pmatrix} xI_r & 0 & 0 & \cdots & 0 & 0 & 0 \\ 0 & xI_r & 0 & \cdots & 0 & 0 & 0 \\ 0 & 0 & xI_r & \cdots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \cdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & xI_r & 0 & 0 \\ 0 & 0 & 0 & \cdots & 0 & xI_r & 0 \\ 0 & 0 & 0 & \cdots & 0 & 0 & xI_r \end{pmatrix}.$$

Therefore,

$$(I_p \otimes A_x)^r = xI_p \otimes I_r = xI_{rp}.$$

(b) Next, we show that $(A_x \otimes I_p)^r = xI_{rp}$. Notice that

$$A_x \otimes I_p = \begin{pmatrix} 0 & I_p & 0 & \cdots & 0 & 0 & 0 \\ 0 & 0 & I_p & \cdots & 0 & 0 & 0 \\ 0 & 0 & 0 & \cdots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \cdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & I_p & 0 \\ 0 & 0 & 0 & \cdots & 0 & 0 & I_p \\ xI_p & 0 & 0 & \cdots & 0 & 0 & 0 \end{pmatrix}.$$

Therefore,

$$A_x \otimes I_p = \begin{pmatrix} 0 & 0 & \cdots & 0 & 0 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & \cdots & 0 & 0 & 0 & 1 & \ddots & & 0 \\ \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots \\ 0 & 0 & \ddots & 0 & 0 & 0 & 0 & \ddots & 1 & 0 \\ 0 & 0 & \ddots & 0 & 0 & 0 & 0 & \ddots & 0 & 1 \\ x & 0 & \ddots & 0 & 0 & 0 & 0 & \ddots & 0 & 0 \\ 0 & x & \ddots & 0 & 0 & 0 & 0 & \ddots & 0 & 0 \\ \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & & \ddots & x & 0 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & \cdots & 0 & x & 0 & 0 & \cdots & 0 & 0 \end{pmatrix} \in M_{rp}(\mathbb{N}).$$

Consequently, $A_x \otimes I_p$ is a Rare matrix of order *rp* and index *p*. So, $A_x \otimes I_p$ is the *p*th power of a Rare matrix E_x of order *rp* and index 1. Hence

$$(A_x \otimes I_p)^r = (E_x^p)^r = E_x^{rp} = xI_{rp}. \qquad \square$$

It is well known that for every $r \geq 2$, the matrix $A_x \in R_r(\mathbb{N})$ generates *r* construction structures $A_{x,i}$, $i \in \{1, ..., r\}$, of matrix solutions of Diophantine equations, by the permutations of *x* and 1 between the columns of A_x.

Denoting by

$$CS(A_x) = \{A_{x,i},\ A_{x,i}^T,\ i \in \{1, \ldots, r\}\}, \quad x \neq 0$$

the set of all construction structures associated to A_x, we have the following remark:

Remark 3.1. Let x, r and p be integers such that $x \geq 1$, $p \geq 2$ and $r \geq 2$. Then for every Rare matrix $A_x \in R_r(\mathbb{N})$ of order r and index 1, and $K_x \in CS(A_x)$,

(1) $(K_x \otimes I_p)^r = K_x^r \otimes I_p = xI_{rp}$ and $(I_p \otimes K_x)^r = I_p \otimes K_x^r = xI_{rp}$.

(2) $(K_x \otimes I_p)^T = K_x^T \otimes I_p$ and $(I_p \otimes K_x)^T = I_p \otimes K_x^T$.

Consequently, for all $p \geq 2$ and $K_x \in CS(A_x)$, the matrices denoted by $B_{K_x}(p) = I_p \otimes K_x$ and $D_{K_x}(p) = K_x \otimes I_p$ are construction structures of matrix solutions of Diophantine equations. Now, we investigate the matrices obtained from the permutations of x and 1 between the columns of $B_{K_x}(p)$ and $D_{K_x}(p)$. It should be noted that there are $\binom{rp}{p}$ associated matrices to $B_{K_x}(p)$ and $\binom{rp}{p}$ associated matrices to $D_{K_x}(p)$ by the permutations of x and 1 between the columns. However, many of these matrices are not construction structures of matrix solutions of Diophantine equations. In fact, among the associated matrices to $B_{K_x}(p)$, in those for which the permutations are made in the blocks K_x are construction structures of matrix solutions of Diophantine equations. In this case, the number of such matrices is r^p. The matrices associated to $D_{K_x}(p)$ in which we have x in p consecutive columns, or x in the first k columns and in the last $p - k$

columns, $1 \le k \le p-1$, are construction structures of matrix solutions of Diophantine equations. The number of such matrices is rp. Denote those matrices by

$$H_{K_{x,i}}(p), \quad i \in \{1, ..., rp + r^p\}, \quad \forall K_x \in CS(A_x).$$

The construction structures set of matrix solutions

$$CS^*(A_x(p)) = \{H_{K_{x,i}}(p), i \in \{1, ..., rp + r^p\}, K_x \in CS(A_x)\}$$

has exactly $2r^2p + 2r^{p+1}$ elements. Notice that for every $K_x \in CS(A_x)$ and every $p \ge 2$, there are many over structures of matrix solutions generated by $B_{K_x}(p)$ and $D_{K_x}(p)$, which are not in $CS^*(A_x(p))$.

Example 3.1. Assume that $K_x = A_x = \begin{pmatrix} 0 & 1 \\ x & 0 \end{pmatrix} \in R_2(\mathbb{N})$. So,

$$D_{K_x}(3) = \begin{pmatrix} 0 & I_3 \\ xI_3 & 0 \end{pmatrix} \quad \text{and} \quad B_{K_x}(3) = \begin{pmatrix} K_x & 0 & 0 \\ 0 & K_x & 0 \\ 0 & 0 & K_x \end{pmatrix}.$$

Denote by $D_i = H_{K_{x,i}}(3), i \in \{1, ..., 6\}$, the six associated matrices to $D_{K_x}(3)$. In particular,

$$D_1 = \begin{pmatrix} 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ x & 0 & 0 & 0 & 0 & 0 \\ 0 & x & 0 & 0 & 0 & 0 \\ 0 & 0 & x & 0 & 0 & 0 \end{pmatrix}, \quad D_2 = \begin{pmatrix} 0 & 0 & 0 & x & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & x & 0 & 0 & 0 & 0 \\ 0 & 0 & x & 0 & 0 & 0 \end{pmatrix},$$

$$D_3 = \begin{pmatrix} 0 & 0 & 0 & x & 0 & 0 \\ 0 & 0 & 0 & 0 & x & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & x & 0 & 0 & 0 \end{pmatrix}, \quad D_4 = \begin{pmatrix} 0 & 0 & 0 & x & 0 & 0 \\ 0 & 0 & 0 & 0 & x & 0 \\ 0 & 0 & 0 & 0 & 0 & x \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \end{pmatrix},$$

$$D_5 = \begin{pmatrix} 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & x & 0 \\ 0 & 0 & 0 & 0 & 0 & x \\ x & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \end{pmatrix}, \quad D_6 = \begin{pmatrix} 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & x \\ x & 0 & 0 & 0 & 0 & 0 \\ 0 & x & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \end{pmatrix}.$$

Denote by $B_i = H_{K_{x,i}}(3),\ i \in \{1, ..., 8\}$, the eight associated matrices to $B_{K_x}(3)$. In particular,

$$B_1 = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ x & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & x & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & x & 0 \end{pmatrix}, \quad B_2 = \begin{pmatrix} 0 & x & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & x & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & x & 0 \end{pmatrix},$$

$$B_3 = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ x & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & x & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & x & 0 \end{pmatrix}, \quad B_4 = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ x & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & x & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & x \\ 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix},$$

$$B_5 = \begin{pmatrix} 0 & x & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & x & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & x & 0 \end{pmatrix}, \quad B_6 = \begin{pmatrix} 0 & x & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & x & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & x \\ 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix},$$

$$B_7 = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ x & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & x & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & x \\ 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}, \quad B_8 = \begin{pmatrix} 0 & x & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & x & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & x \\ 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}.$$

Moreover, the matrices

$$E_1 = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & x & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & x & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ x & 0 & 0 & 0 & 0 & 0 \end{pmatrix} \quad \text{and} \quad E_2 = \begin{pmatrix} 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & x & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ x & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & x & 0 & 0 & 0 \end{pmatrix}$$

associated, respectively, to $B_{K_x}(3)$ and $D_{K_x}(3)$ satisfy $E_i^2 = (E_i^T)^2 = xI_6$, for $i \in \{1, 2\}$, but $E_1, E_2, E_1^T, E_2^T \notin CS^*(A_x(3))$.

Proposition 3.5. *Let a, b and p be positive integers such that $p \geq 2$, $a \neq 0$ and $b \neq 0$. Let ℓ be the least common multiple of a and b. Suppose that ℓp is an even number. Let $(x_k)_{k \in \mathbb{N}}$ and $(y_k)_{k \in \mathbb{N}}$ be two increasing sequences of non-zero positive integers. Assume that*

$$N_0 = \max\{|\alpha|, |\beta|\}, \quad k_0 = \min\{k \in \mathbb{N} : x_k \geq N_0 \text{ and } y_k \geq N_0\}$$

and let $(z_k)_{k \in \mathbb{N}}$ be the sequence defined by

$$\forall k \in \mathbb{N}, \quad z_k = (x_k + \alpha)^m + (y_k + \beta)^n.$$

Then the terms of the sequence of matrices $(E_{x_k}^r, F_{y_k}^s, G_{z_k}^t)_{k \geq k_0}$ *are matrix solutions of the Diophantine equation*

$$(X^a + \alpha I_{\ell p})^m + (Y^b + \beta I_{\ell p})^n = Z^2, \quad \ell p = ar = sb = 2t,$$

where $E_{x_k} \in CS^*(A_{x_k}(p))$, $F_{y_k} \in CS^*(A_{y_k}(p))$ *and* $G_{z_k} \in CS^*(A_{z_k}(p))$, *with* $(A_{x_k}, A_{y_k}, A_{z_k})$ *a triple of Rare matrices of order* ℓ *and index* 1.

Proof. Suppose that

$$(E_{x_k}, F_{y_k}, G_{z_k}) \in CS^*(A_{x_k}(p)) \times CS^*(A_{y_k}(p)) \times CS^*(A_{z_k}(p)).$$

This implies that

$$E_{x_k}^{\ell p} = x_k I_{\ell p}, \quad F_{y_k}^{\ell p} = y_k I_{\ell p} \quad \text{and} \quad G_{z_k}^{\ell p} = z_k I_{\ell p}.$$

It follows that

$$[(E_{x_k}^r)^a + \alpha I_{\ell p}]^m + [(F_{y_k}^s)^b + \beta I_{\ell p}]^n = [E_{x_k}^{ra} + \alpha I_{\ell p}]^m + [F_{y_k}^{sb} + \beta I_{\ell p}]^n.$$

Due to the fact that $\ell p = ra = sb$, we have

$$[(E_{x_k}^r)^a + \alpha I_{\ell p}]^m + [(F_{y_k}^s)^b + \beta I_{\ell p}]^n = [E_{x_k}^{\ell p} + \alpha I_{\ell p}]^m + [F_{y_k}^{\ell p} + \beta I_{\ell p}]^n.$$

Since $E_{x_k}^{\ell p} = x_k I_{\ell p}$ and $F_{y_k}^{\ell p} = y_k I_{\ell p}$,

$$[(E_{x_k}^r)^a + \alpha I_{\ell p}]^m + [(F_{y_k}^s)^b + \beta I_{\ell p}]^n = [(x_k + \alpha) I_{\ell p}]^m + [(y_k + \beta) I_{\ell p}]^n.$$

Therefore,

$$[(E_{x_k}^r)^a + \alpha I_{\ell p}]^m + [(F_{y_k}^s)^b + \beta I_{\ell p}]^n = (x_k + \alpha)^m I_{\ell p} + (y_k + \beta)^n I_{\ell p}.$$

So, as $z_k = (x_k + \alpha)^m + (y_k + \beta)^n$, we can claim that

$$[(E_{x_k}^r)^a + \alpha I_{\ell p}]^m + [(F_{y_k}^s)^b + \beta I_{\ell p}]^n = z_k I_{\ell p} = G_{z_k}^{\ell p} = G_{z_k}^{2t} = (G_{z_k}^t)^2. \quad \square$$

Consequently, if ℓp is an even number, then there are at least

$$N_{\min} = (2\ell^2 p^3 + (\ell p)^{p+1})^3$$

construction structures of matrix solutions of the Diophantine equation

$$(X^a + \alpha I_{\ell p})^m + (Y^b + \beta I_{\ell p})^n = Z^2.$$

Each construction structure allows us to construct a sequence of matrix solutions. We are going to look at the case where ℓp is an odd number.

Proposition 3.6. *Let a, b and p be positive integers such that $p \geq 2$, $a \neq 0$ and $b \neq 0$. Let ℓ be the least common multiple of a and b. Suppose that ℓp is an odd number. Let $(x_k)_{k\in\mathbb{N}}$ and $(y_k)_{k\in\mathbb{N}}$ be two increasing sequences of non-zero positive integers. Assume that*

$$N_0 = \max\{|\alpha|, |\beta|\}, \quad k_0 = \min\{k \in \mathbb{N} : x_k \geq N_0 \text{ and } y_k \geq N_0\}$$

and let $(z_k)_{k\in\mathbb{N}}$ be the sequence defined by

$$\forall k \in \mathbb{N}, \quad z_k = (x_k + \alpha)^m + (y_k + \beta)^n.$$

Then, the terms of the sequence of matrices are matrix $(E_{x_k}^r, F_{y_k}^s, G_{z_k}^{p\ell})_{k\geq k_0}$ solutions of the Diophantine equation

$$(X^a + \alpha I_{2\ell p})^m + (Y^b + \beta I_{2\ell p})^n = Z^2, \quad 2\ell p = ar = bs,$$

where $E_{x_k} \in CS^*(A_{x_k}(p))$, $F_{y_k} \in CS^*(A_{y_k}(p))$ and $G_{z_k} \in CS^*(A_{z_k}(p))$ with $(A_{x_k}, A_{y_k}, A_{z_k})$ a triple of Rare matrices of order 2ℓ and index 1.

Proof. Since $A_{x_k}, A_{y_k}, A_{z_k}$ are Rare matrices of order 2ℓ and index 1,

$$E_{x_k}^{2\ell p} = x_k I_{2\ell p}, \quad F_{y_k}^{2\ell p} = y_k I_{2\ell p} \quad \text{and} \quad G_{z_k}^{2\ell p} = z_k I_{2\ell p}.$$

So,

$$[(E_{x_k}^r)^a + \alpha I_{2\ell p}]^m = [E_{x_k}^{ra} + \alpha I_{2\ell p}]^m$$

and

$$[(F_{y_k}^s)^b + \beta I_{2\ell p}]^n = [F_{y_k}^{sb} + \beta I_{2\ell p}]^n.$$

Due to the fact that $2\ell p = ra = sb,$ we have

$$E_{x_k}^{ra} = E_{x_k}^{2\ell p} = x_k I_{2\ell p} \quad \text{and} \quad F_{y_k}^{sb} = F_{y_k}^{2\ell p} = y_k I_{2\ell p}.$$

Therefore, as $z_k = (x_k + \alpha)^m + (y_k + \beta)^n,$

$$[(E_{x_k}^r)^a + \alpha I_{2\ell p}]^m + [(F_{y_k}^s)^b + \beta I_{2\ell p}]^n = z_k I_{2\ell p} = G_{z_k}^{2\ell p}.$$

As $G_{z_k}^{2\ell p} = z_k I_{2\ell p},$

$$[(E_{x_k}^r)^a + \alpha I_{2\ell p}]^m + [(F_{y_k}^s)^b + \beta I_{2\ell p}]^n = (G_{z_k}^{\ell p})^2. \qquad \square$$

We can observe that if ℓp is an odd number, then there are at least

$$N_{\min} = (8\ell^2 p^3 + (2\ell p)^{p+1})^3$$

construction structures of matrix solutions of the Diophantine equation

$$(X^a + \alpha I_{2\ell p})^m + (Y^b + \beta I_{2\ell p})^n = Z^2.$$

From all the above, we obtain our main result.

Theorem 3.1. *Let a and b be positive integers such that* $(a, b) \neq (0, 0).$ *Let* ℓ *be the least common multiple of a and b, and q be a multiple of* ℓ *different from zero. Then for* $\alpha, \beta \in \mathbb{Z}$ *and* $m, n \in \mathbb{N},$ *the exponential Diophantine equation*

$$(X^a + \alpha I_q)^m + (Y^b + \beta I_q)^n = Z^2,$$

admits an infinite number of matrix solutions from the set

$$GL_q(\mathbb{N}) = \{A \in M_q(\mathbb{N}) : \det(A) \neq 0\},$$

where $q = \ell p$, *if* ℓp *is an even number and* $q = 2\ell p$, *if* ℓp *is an odd number with* $p \in \mathbb{N}$.

Proof. For $a = 0$ or $b = 0$, the result follows from Propositions 3.1 and 3.2. When $a \neq 0$ and $b \neq 0$, Propositions 3.5 and 3.6 complete the proof. □

Acknowledgements

The authors thank the anonymous referees for carefully reading the paper. They are grateful to J. M. Mouanda for his contribution to improve the final version.

References

[1] J. L. Brenner and J. De Pillis, Fermat's equation $A^p + B^p = C^p$ for matrices of integers, Math. Mag. 45(1) (1972), 12-15.

[2] E. D. Bolker, Solutions of $A^k + B^k = C^k$ in $n \times n$ integral matrices, Amer. Math. Monthly 75(1) (1968), 759-760.

[3] Deepak Gupta, Satish Kumar and Sudhanshu Aggarwal, Solution of non-linear exponential, Diophantine equation $(x^a + 1)^m + (y^b + 1)^n = z^2$, Journal of Emerging Technologies and Innovative Research 9(9) (2022), 154-157.

[4] W. Ivorra and A. Kraus, Quelques résultats sur les équations $ax^p + by^p = cz^2$, Canad. J. Math. 58 (2006), 115-153.

[5] J. M. Mouanda, D. Dehainsala and K. Kangni, On matrix elliptic curves and matrix solutions of the exponential Diophantine equation $(X^{24} - I_{24})(Y^{24} - I_{24}) = Z^2$, Japan Journal of Research 5(3) (2024), 1-6.

[6] J. M. Mouanda, On Beal's conjecture for matrix solutions and multiplication commutative groups of rare matrices, Turkish Journal of Analysis and Number Theory 12(1) (2024), 1-7.

[7] J. M. Mouanda, On construction structures of matrix solutions of exponential Diophantine equations, Journal of Advances in Mathematics and Computer Science 39(5) (2024), 1-14.

[8] J. M. Mouanda, On multiverses (or parallel universes) of matrix triple solutions of the Diophantine equation $X^3 + Y^6 = Z^6$, London Journal of Research in Science: Natural and Formal 24(9) (2024), 75-85.