Journal of Advances in Mathematics and Computer Science

Volume 39, Issue 5, Page 1-14, 2024; Article no.JAMCS.114693

ISSN: 2456-9968

(Past name: British Journal of Mathematics & Computer Science, Past ISSN: 2231-0851)

On Construction Structures of Matrix Solutions of Exponential Diophantine Equations

Joachim Moussounda Mouanda [a*]

[a] *Department of Mathematics, Blessington Christian University, Nkayi, Republic of Congo.*

Author's contribution

The sole author designed, analyzed, interpreted and prepared the manuscript.

Article Information

DOI: 10.9734/JAMCS/2024/v39i51886

Open Peer Review History:
This journal follows the Advanced Open Peer Review policy. Identity of the Reviewers, Editor(s) and additional Reviewers, peer review comments, different versions of the manuscript, comments of the editors, etc are available here: http://www.sdiarticle5.com/review-history/114693

Original Research Article

Received: 20/01/2024
Accepted: 21/03/2024
Published: 03/04/2024

Abstract

We show that the matrix exponential Diophantine equation $(X^n - I_{q\times n})(Y^n - I_{q\times n}) = Z^2$, admits at least $4 \times n^2$ different construction structures of matrix solutions. We also prove that the matrix exponential Diophantine equation $(X^n - I_{n\times m})(Y^m - I_{n\times m}) = Z^2$, admits at least $4 \times n \times m$ different construction structures of matrix solutions in $M_{n\times m}(\mathbb{N})$ for every pair (n, m) of positive integers such that $n \neq m$. We show the connection between the construction structures of matrix solutions of an exponential Diophantine equation and Integer factorization. We show that the matrix Diophantine equation $X^n + Y^m = Z^q, n, m, q \in \mathbb{N}$, admits at least $8 \times n \times m \times q$ different construction structures of matrix solutions in $M_{n\times m\times q}(\mathbb{N})$.

Keywords: Matrices of integers; Diophantine equations; exponential Diophantine equations.

Mathematics Subject Classification 2010: 15B36, 11D72, 11D61.

**Corresponding author: E-mail: mmoussounda@yahoo.fr;*

1 Introduction and Main Result

Let a and b be two different fixed positive integers. The exponential Diophantine equation

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

has been studied by many authors [1, 2, 3, 4, 5, 6, 7]. In 2020, Noubissie, Togbe and Zhang showed that the equation (1.1) with $b\equiv 3(\text{mod } 8)$, b prime and a even has no solution in positive integers n, x [8]. Recent Mouanda's work on matrix solutions of Diophantine equations (Fermat's Diophantine equation) shows that these Diophantine equations always admit, in each case, an infinite number of matrix solutions [9]-[11].

In this paper, we show that matrix exponential Diophantine equations always have a finite number of construction structures of matrix solutions.

Theorem 1.1. *Let n be a positive integer. The matrix exponential Diophantine equation*

$$(X^n-I_{q\times n})(Y^n-I_{q\times n})=Z^2, X\neq Y, q\in\mathbb{N},$$

admits at least $4\times n^2$ different construction structures of matrix solutions.

We show that the matrix exponential Diophantine equation

$$(X^n-I_{n\times m})(Y^m-I_{n\times m})=Z^2,$$

admits at least $4\times n\times m$ different construction structures of matrix solutions in $M_{n\times m}(\mathbb{N})$ for every pair (n,m) of positive integers such that $n\neq m$. We establish the connection between the construction structures of matrix solutions of an exponential Diophantine equation and Integer factorization. We introduce an algorithm which allows us to show that the matrix Diophantine equation $X^n+Y^m=Z^q, n, m, q\in\mathbb{N}$, admits at least $8\times n\times m\times q$ different construction structures of matrix solutions in $M_{n\times m\times q}(\mathbb{N})$.

2 Proof of the Main Result

In this section, we show that the matrix solutions of Diophantine equations rely on the construction structures of matrices and it is possible to compute the number of construction structures of matrix solutions of Diophantine equations.

Definition 2.1. *A positive integer which is the product of two prime numbers is called a semiprime.*

Definition 2.2. *[9]. The $n\times n$-matrices of the form*

$$c\begin{pmatrix} 0 & 1 & 0 & 0 & \dots & 0 & 0 & 0 & 0\\ 0 & 0 & 1 & 0 & \dots & 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 1 & \dots & 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0\\ \vdots & \vdots & \vdots & \vdots & \dots & \vdots & \vdots & \vdots & \vdots\\ 0 & 0 & 0 & 0 & \dots & 0 & 1 & 0 & 0\\ 0 & 0 & 0 & 0 & \dots & 0 & 0 & 1 & 0\\ 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 1\\ a & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 \end{pmatrix}, c\begin{pmatrix} 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & b\\ 1 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0\\ 0 & 1 & 0 & 0 & \dots & 0 & 0 & 0 & 0\\ 0 & 0 & 1 & 0 & \dots & 0 & 0 & 0 & 0\\ \vdots & \vdots & \vdots & \vdots & \dots & \vdots & \vdots & \vdots & \vdots\\ 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & \dots & 1 & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & \dots & 0 & 1 & 0 & 0\\ 0 & 0 & 0 & 0 & \dots & 0 & 0 & 1 & 0 \end{pmatrix}$$

,$a\neq 0, c\neq 0, b\neq 0, a, b, c\in\mathbb{C}$, are called Rare matrices of order n and index 1.

The index defines the number of non-zero complex coefficients of the matrix different to 1. It well known that Rare matrices have interesting properties.

Remark 2.3. *[9]. Let*

$$A_\alpha = \begin{pmatrix} 0 & 1 & 0 & 0 & \dots & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & \dots & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & \dots & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \dots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \dots & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & \dots & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 1 \\ \alpha & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 \end{pmatrix} \in M_n(\mathbb{C}), \alpha \neq 0,$$

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

$$A_\alpha^n = \begin{pmatrix} \alpha & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 \\ 0 & \alpha & 0 & 0 & \dots & 0 & 0 & 0 & 0 \\ 0 & 0 & \alpha & 0 & \dots & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & \alpha & \dots & 0 & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \dots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \dots & \alpha & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \dots & 0 & \alpha & 0 & 0 \\ 0 & 0 & 0 & 0 & \dots & 0 & 0 & \alpha & 0 \\ 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & \alpha \end{pmatrix}, A_\alpha^{-1} = \begin{pmatrix} 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & \frac{1}{\alpha} \\ 1 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & \dots & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & \dots & 0 & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \dots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \dots & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \dots & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & \dots & 0 & 0 & 1 & 0 \end{pmatrix},$$

$$A_\alpha^{-1} = A_{\frac{1}{\alpha}}^T, A_\alpha^n = \alpha I_n, (\beta A_\alpha)^{-1} = \frac{1}{\beta} A_\alpha^{-1}, \beta \neq 0.$$

These observations imply that

$$A_\alpha^{nk+q} = A_\alpha^{nk} A_\alpha^q = (A_\alpha^n)^k A_\alpha^q = (\alpha I_n)^k A_\alpha^q = \alpha^k A_\alpha^q, q < n, A_\alpha \times \frac{1}{\alpha} A_\alpha^{n-1} = I_n.$$

It is well known that the set $\left\{A_\alpha^k : k \in \mathbb{Z}\right\}$ is a commutative group [9].

Definition 2.4. *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 $B^m - \beta \times I_n = 0$.*

This definition is equivalent to say that there exists a positive integer m such that B^m is a Rare matrix of order n and index 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 $M_n(\mathbb{N})$. A matrix Diophantine equation can admit several construction structures. For example, let x be a positive integer. Consider the matrix

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

A simple calculation shows that $A_x^6 = x \times I_{12}$. Therefore, $A_x \in D_{12}(\mathbb{N})$. The structure of the matrix A_x allows us to construct the matrix solutions of the exponential Diophantine equation $(X^6 - I_{12})(Y^6 - I_{12}) = Z^2$. Indeed,

$$(A_{x^2+1}^6 - I_{12})(A_{y^2+1}^6 - I_{12}) = x^2y^2 \times I_{12} = B_{x,y}^2$$

where $B_{x,y}$ is the matrix of the form

$$B_{x,y} = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & xy \\ 0 & xy & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & xy & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & xy & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & xy & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & xy & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & xy & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & xy & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & xy & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & xy & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & xy & 0 \\ xy & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} \in D_{12}(\mathbb{N}).$$

The choice of $B_{x,y}$ is not unique. The matrix $B_{x,y}$ can generate other matrices which can be used. This can be achieved by just simple permutations of the entries xy inside the matrix $B_{x,y}$. We can claim that the triples $(A_{x^2+1}, A_{y^2+1}, B_{x,y}), x, y \in \mathbb{N}$, are matrix solutions of the matrix equation

$$(X^6 - I_{2\times 6})(Y^6 - I_{2\times 6}) = Z^2.$$

The matrix exponential Diophantine equation $(X^6 - I_{2\times 6})(Y^6 - I_{2\times 6}) = Z^2$ admits at least 144 construction structures of matrix solutions. Indeed, the matrices

$$A_{x,2} = \begin{pmatrix} 0 & 0 & x & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & x & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix},$$

$$A_{x,3} = \begin{pmatrix} 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & x & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & x & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix},$$

$$A_{x,4} = \begin{pmatrix} 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & x & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & x & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix},$$

$$A_{x,5} = \begin{pmatrix} 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & x & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & x & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix},$$

$$A_{x,6} = \begin{pmatrix} 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & x & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & x \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

are construction structures of matrix solutions of the exponential Diophantine equation

$$(X^6 - I_{2\times 6})(Y^6 - I_{2\times 6}) = Z^2.$$

We can choose the construction structure of X and Y inside the set

$$\left\{ A_{x,i}, A_{x,i}^T : i \in \{1,2,3,4,5,6\} \right\}.$$

Therefore, there are at least $12 \times 12 = 144$ construction structures of matrix solutions of this equation for a fixed choice of Z. The permutations of the coefficients of $B_{x,y}$ give us different choices of Z. In order to compute the exact number of choices of Z, we need to find out the number of permutations of the coefficients of $B_{x,y}$ which make Z^2a Rare matrix of order n and index 0.

Notation: Let

$$A_\alpha = A_{\alpha,1} = \begin{pmatrix} 0 & 1 & 0 & 0 & \dots & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & \dots & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & \dots & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \dots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \dots & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & \dots & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 1 \\ \alpha & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 \end{pmatrix} \in M_n(\mathbb{C}), \alpha \neq 0,$$

be a Rare matrix of order n and index 1. Denote by

$$A_{\alpha,2} = \begin{pmatrix} 0 & \alpha & 0 & 0 & \dots & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & \dots & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & \dots & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \dots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \dots & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & \dots & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 \end{pmatrix}, A_{\alpha,3} = \begin{pmatrix} 0 & 1 & 0 & 0 & \dots & 0 & 0 & 0 & 0 \\ 0 & 0 & \alpha & 0 & \dots & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & \dots & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \dots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \dots & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & \dots & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 \end{pmatrix}$$

$$A_{\alpha,4} = \begin{pmatrix} 0 & 1 & 0 & 0 & \dots & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & \dots & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & \alpha & \dots & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \dots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \dots & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & \dots & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 \end{pmatrix}, ..., A_{\alpha,n-2} = \begin{pmatrix} 0 & 1 & 0 & 0 & \dots & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & \dots & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & \dots & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \dots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \dots & 0 & \alpha & 0 & 0 \\ 0 & 0 & 0 & 0 & \dots & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 \end{pmatrix},$$

$$A_{\alpha,n-1} = \begin{pmatrix} 0 & 1 & 0 & 0 & \dots & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & \dots & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & \dots & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \dots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \dots & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & \dots & 0 & 0 & \alpha & 0 \\ 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 \end{pmatrix}, A_{\alpha,n} = \begin{pmatrix} 0 & 1 & 0 & 0 & \dots & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & \dots & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & \dots & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \dots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \dots & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & \dots & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & \alpha \\ 1 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 \end{pmatrix}.$$

Let us notice that every $A_{\alpha,j} \in D_n(\mathbb{N}), 1 \leq j \leq n$ and $A_{\alpha,j}$ is invertible. In fact, the set $\left\{A_{\alpha,j}^k : k \in \mathbb{Z}\right\}$ is a commutative group of matrices for all $1 \leq j \leq n$. The elements of the set $D_n(\mathbb{N})$ play an important role on solving the matrix exponential Diophantine equation

$$(X^n - I_{q\times n})(Y^n - I_{q\times n}) = Z^2, X \neq Y.$$

The difficulty of knowing which one can be selected for solving this equation can be challenging for n sufficiently large with q and n are prime numbers. In other words, when $q \times n$ is a sufficiently large semiprime, it is difficult to find the matrix solutions of this Diophantine equation. This difficulty could lead to serious cryptography problems. This equation admits at least $4n^2$ different construction structures of matrix solutions.

Proof of Theorem 1.1

Let α be a positive integer and let

$$A_{\alpha+1}=\begin{pmatrix} 0 & 0 & 0 & 0 & 1 & \dots & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & \dots & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & \dots & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & \dots & 0 & 0 & 1 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \dots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 & 1 \\ \alpha+1 & 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 & 0 \\ 0 & \alpha+1 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 & 0 \\ \ddots & \ddots & \ddots & \ddots & \ddots & \dots & \ddots & \ddots & \ddots & \ddots & \ddots \\ 0 & \ddots & 0 & \underbrace{\alpha+1}_{q^{th}diagonal} & 0 & \dots & 0 & 0 & 0 & 0 & 0 \end{pmatrix} \in M_{q\times n}(\mathbb{N})$$

be a Rare matrix of order $q \times n$ and index q. A simple calculation shows that

$$A_{\alpha+1}^n = (\alpha+1) \times I_{q\times n}.$$

Therefore,

$$A_{\alpha+1}^n - I_{q\times n} = \alpha \times I_{q\times n}.$$

This implies that

$$(A_{x^2+1}^n - I_{q\times n})(A_{y^2+1}^n - I_{q\times n}) = x^2y^2 \times I_{q\times n} = B_{x,y}^2, \forall x, y \in \mathbb{N}$$

with

$$B_{x,y}=\begin{pmatrix} 0 & 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 & xy \\ 0 & xy & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & \dots & 0 & 0 & xy & 0 & 0 \\ 0 & 0 & 0 & xy & 0 & \dots & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & \dots & xy & 0 & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \dots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & xy & \dots & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & \dots & 0 & xy & 0 & 0 & 0 \\ 0 & 0 & xy & 0 & 0 & \dots & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & xy & 0 \\ xy & 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 & 0 \end{pmatrix} \in M_{q\times n}(\mathbb{N}).$$

The construction structure of the matrix $A_{\alpha+1}$ allows the construction of the matrix solutions of the exponential Diophantine equation

$$(X^n - I_{q\times n})(Y^n - I_{q\times n}) = Z^2, X \neq Y.$$

This matrix satisfies $A_{\alpha+1}^n = (\alpha+1) \times I_{q\times n}$. The construction structure of any matrix $B \in M_{q\times n}(\mathbb{N})$ which satisfies $B^n = \beta \times I_{q\times n}, \beta \in \mathbb{N}$, allows the construction of the matrix solutions of this exponential Diophantine

equation as well. Therefore, the construction structures of the matrices

$$A_{\alpha+1,2} = \begin{pmatrix} 0 & 0 & 0 & 0 & 1+\alpha & \dots & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & \dots & 1+\alpha & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & \dots & 0 & \underbrace{\alpha+1}_{q^{th}element} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & \dots & 0 & 0 & 1 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \dots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 & 0 \\ \ddots & \ddots & \ddots & \ddots & \ddots & \dots & \ddots & \ddots & \ddots & \ddots & \ddots \\ 0 & \ddots & 0 & \underbrace{1}_{q^{th}diagonal} & 0 & \dots & 0 & 0 & 0 & 0 & 0 \end{pmatrix},$$

$$A_{\alpha+1,3} = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 & \dots & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & \dots & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & \dots & 0 & \underbrace{1}_{q^{th}element} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & \dots & 0 & 0 & 1+\alpha & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \dots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 & 0 \\ \ddots & \ddots & \ddots & \ddots & \ddots & \dots & \ddots & \ddots & \ddots & \ddots & \ddots \\ 0 & \ddots & 0 & \underbrace{1}_{q^{th}diagonal} & 0 & \dots & 0 & 0 & 0 & 0 & 0 \end{pmatrix}, ...,$$

$$A_{\alpha+1,n} = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 & \dots & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & \dots & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & \dots & 0 & \underbrace{1}_{q^{th}element} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & \dots & 0 & 0 & 1 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \dots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 & \underbrace{\alpha+1}_{q^{th}element} \\ 1 & 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 & 0 \\ \ddots & \ddots & \ddots & \ddots & \ddots & \dots & \ddots & \ddots & \ddots & \ddots & \ddots \\ 0 & \ddots & 0 & \underbrace{1}_{q^{th}diagonal} & 0 & \dots & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

allows the construction of the matrix solutions of the exponential Diophantine equation

$$(X^n - I_{q\times n})(Y^n - I_{q\times n}) = Z^2, X \neq Y.$$

We can choose the construction structure of X and Y inside the set

$$\left\{A_{\alpha+1,i}, A_{\alpha+1,i}^T : i \in \{1,2,...,n\}\right\}.$$

Therefore, there are $4 \times n^2$ construction structures of matrix solutions of this exponential Diophantine equation. □

3 Connections between Matrix Exponential Diophantine Equations and Integer Factorization

In 1977, Rivest-Shamir-Adleman introduced a public key encryptosystem for secure data transmission called RSA [12]. Integer factorization is the decomposition, when possible, of a positive integer into a product of smaller integers and prime factorization is the decomposition, when possible, of a positive integer into a product of smaller prime numbers [13]- [16]. Integer factorization of sufficiently large semiprimes is very complex. It is well known that when the numbers are sufficiently large no integer factorization algorithm is known. The difficulty of this problem is very important for the algorithms used in cryptography such as RSA public key encryption and RSA digital signature [17]. Many branches of mathematics (elliptic curves, algebraic number theory and quantum computing) are interested in the difficulty of integer factorization of sufficiently large numbers. In 2019, Fabrice Boudot, Pierrick Gaudry, Aurore Guillevic, Nadia Heninger, Emmanuel Thome and Paul Zimmermann factored a 240-digit number (RSA-240) [18]. Integer factorization of sufficiently large semiprimes, the product of two prime numbers, is very hard [19]. Many cryptographic protocols (RSA) are based on integer factorization difficulty of sufficiently large numbers [20, 21]. It is still unknown that the exponential Diophantine equation

$$(a^n - 1)(b^m - 1) = x^2, x, n, m \in \mathbb{N}, n \neq m, a > 1, b > 1, x \neq 0, n \neq 0, \tag{3.1}$$

admits at all any positive integer solutions. However, in this section, we show that the matrix exponential Diophantine equation

$$(X^n - I_{n\times m})(Y^m - I_{n\times m}) = Z^2$$

has an infinite number of matrix solutions in $M_{n\times m}(\mathbb{N})$ for every pair (n, m) of positive integers such that $n \neq m$.

Theorem 3.1. *Let n, m be two positive integers such that $n \neq m$. The matrix exponential Diophantine equation*

$$(X^n - I_{n\times m})(Y^m - I_{n\times m}) = Z^2,$$

admits at least $4 \times n \times m$ construction structures of matrix solutions.

Proof. Let α, β be two positive integers. Let

$$A_{\alpha+1} = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 & \dots & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & \dots & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & \dots & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & \dots & 0 & 0 & 1 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \dots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 & 1 \\ \alpha+1 & 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 & 0 \\ 0 & \alpha+1 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 & 0 \\ \ddots & \ddots & \ddots & \ddots & \ddots & \dots & \ddots & \ddots & \ddots & \ddots & \ddots \\ 0 & \ddots & 0 & \underbrace{\alpha+1}_{m^{th}diagonal} & 0 & \dots & 0 & 0 & 0 & 0 & 0 \end{pmatrix} \in M_{n\times m}(\mathbb{N})$$

be a Rare matrix of order $n \times m$ and index m. Let

$$B_{\beta+1} = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 & \dots & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & \dots & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & \dots & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & \dots & 0 & 0 & 1 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \dots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 & 1 \\ \beta+1 & 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 & 0 \\ 0 & \beta+1 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 & 0 \\ \ddots & \ddots & \ddots & \ddots & \ddots & \dots & \ddots & \ddots & \ddots & \ddots & \ddots \\ 0 & \ddots & 0 & \underbrace{\beta+1}_{n^{th}diagonal} & 0 & \dots & 0 & 0 & 0 & 0 & 0 \end{pmatrix} \in M_{n\times m}(\mathbb{N})$$

be a Rare matrix of order $n \times m$ and index n. A simple calculation shows that

$$A^n_{\alpha+1} = (\alpha+1) \times I_{n\times m}, B^m_{\beta+1} = (\beta+1) \times I_{n\times m}.$$

Therefore,

$$A^n_{\alpha+1} - I_{n\times m} = \alpha \times I_{n\times m}, B^m_{\beta+1} - I_{n\times m} = \beta \times I_{n\times m}.$$

This implies that

$$(A^n_{\alpha+1} - I_{n\times m})(B^m_{\beta+1} - I_{n\times m}) = \alpha\beta \times I_{n\times m}.$$

Assume that $\alpha = x^2$ and $\beta = y^2$. One has

$$(A^n_{x^2+1} - I_{n\times m})(B^m_{y^2+1} - I_{n\times m}) = x^2y^2 \times I_{n\times m} = H^2_{x,y}$$

with

$$H_{x,y} = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 & xy \\ 0 & xy & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & \dots & 0 & 0 & xy & 0 & 0 \\ 0 & 0 & 0 & xy & 0 & \dots & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & \dots & xy & 0 & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \dots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & xy & \dots & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & \dots & 0 & xy & 0 & 0 & 0 \\ 0 & 0 & xy & 0 & 0 & \dots & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & xy & 0 \\ xy & 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 & 0 \end{pmatrix} \in M_{n\times m}(\mathbb{N}), x, y \in \mathbb{N}.$$

Therefore, the triples $(A_{x^2}, B_{y^2}, H_{x,y}), x, y \in \mathbb{N}$, are matrix solutions of the exponential Diophantine equation

$$(X^n - I_{n\times m})(Y^m - I_{n\times m}) = Z^2.$$

The matrix A_α generates at least $2n$ different construction structures of matrix solutions and the matrix B_β generates at least $2m$ different construction structures of matrix solutions. Finally, the matrices A_α and B_β generate together at least $4 \times n \times m$ different construction structures of matrix solutions of the matrix exponential Diophantine equation

$$(X^n - I_{n\times m})(Y^m - I_{n\times m}) = Z^2.$$

□

There are several connections between the construction structures of matrix solutions of the exponential Diophantine equations and Integer factorization.

Example: Find the smallest number of construction structures of matrix solutions of the exponential Diophantine equation

$$(X^n - I_{30,068,443})(Y^n - I_{30,068,443}) = Z^2.$$

The difficulty of solving this exponential Diophantine equation is linked to the difficulty of factorizing the number 30,068,443.

The number $30,068,443 = 7,919 \times 3,797$ is a semiprime, since the numbers 7,919 and 3,797 are prime numbers. For example, if we can choose $n = 3,797$, in this case, we have to solve the matrix Diophantine equation

$$(X^{3,797} - I_{30,068,443})(Y^{3,797} - I_{30,068,443}) = Z^2.$$

Let

$$A_{x^2+1} = \begin{pmatrix} 0 & 1 & 0 & 0 & \dots & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & \dots & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & \dots & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \dots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \dots & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & \dots & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 1 \\ x^2+1 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 \end{pmatrix} \in M_{30,068,443}(\mathbb{C}), x \neq 0, x \in \mathbb{N},$$

be a Rare matrix of order 30,068,443 and index 1. The matrix $A_{x^2+1}^{7,919}$ has a construction structure of matrix solutions. This matrix generates 3,797 construction structures of matrix solutions of Diophantine equations. Theorem 3.1 allows us to claim that the exponential Diophantine equation

$$(X^n - I_{30,068,443})(Y^n - I_{30,068,443}) = Z^2$$

admits at least $4 \times 3,797 \times 3,797 = 57,668,836$ construction structures of matrix solutions.

4 Construction Structures of Matrix Solutions of the Diophantine Equations $X^n + Y^m = Z^q$

Let α be a positive integer and let

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

be a matrix. This matrix has a construction structure of matrix solutions of Diophantine equations, since $Q_\alpha^3 = \alpha \times I_3$. We can notice that

$$\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & \alpha \\ 1 & 0 & 0 \end{pmatrix}^6 + \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 2\alpha+1 \\ 1 & 0 & 0 \end{pmatrix}^3 = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & \alpha+1 \\ 1 & 0 & 0 \end{pmatrix}^6.$$

The triples $(Q_\alpha, Q_{2\alpha+1}, Q_{\alpha+1})$ are matrix solutions of the Diophantine equation $X^6 + Y^3 = Z^6$. In general, these matrix solutions do not have a common matrix factor. We can deduce that

$$\begin{pmatrix} 0 & \alpha & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}^6 + \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 2\alpha+1 & 0 & 0 \end{pmatrix}^3 = \begin{pmatrix} 0 & \alpha+1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}^6.$$

The Diophantine equation $X^6 + Y^3 = Z^6$ admits several construction structures.

Remark 4.1. *Let α be a positive integer. Then,*

$$\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & \alpha^n \\ 1 & 0 & 0 \end{pmatrix}^3 = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & \alpha \\ 1 & 0 & 0 \end{pmatrix}^{3n}, n \in \mathbb{N}, n \geq 1.$$

Recall that

$$(a+b)^n = a^n + \sum_{k=1}^{n} \frac{n!}{k!(n-k)!} a^{n-k} b^k, a, b, n \in \mathbb{N}.$$

Then,

$$\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & a \\ 1 & 0 & 0 \end{pmatrix}^{3n} + \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & (\sum_{k=1}^{n} \frac{n!}{k!(n-k)!} a^{n-k} b^k) \\ 1 & 0 & 0 \end{pmatrix}^3 = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & a+b \\ 1 & 0 & 0 \end{pmatrix}^{3n}, n \geq 2.$$

Finally, the the Diophantine equation $X^{3n} + Y^3 = Z^{3n}$ admits an infinite number of matrix solutions for every positive integer n.

Theorem 4.2. *Let n, m, q be three positive integers. The matrix Diophantine equation*

$$X^n + Y^m = Z^q$$

admits at least $8 \times n \times m \times q$ different construction structures of matrix solutions.

Proof. Let α, β, δ be three positive integers. Let

$$A_\alpha = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 & \dots & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & \dots & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & \dots & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & \dots & 0 & 0 & 1 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \dots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 & 1 \\ \alpha & 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 & 0 \\ 0 & \alpha & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 & 0 \\ \ddots & \ddots & \ddots & \ddots & \ddots & \dots & \ddots & \ddots & \ddots & \ddots & \ddots \\ 0 & \ddots & 0 & \underbrace{\alpha}_{(m\times q)^{th} diagonal} & 0 & \dots & 0 & 0 & 0 & 0 & 0 \end{pmatrix} \in M_{n\times m\times q}(\mathbb{N})$$

be a Rare matrix of order $n \times m \times q$ and index $m \times q$. Let

$$B_\beta = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 & \dots & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & \dots & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & \dots & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & \dots & 0 & 0 & 1 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \dots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 & 1 \\ \beta & 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 & 0 \\ 0 & \beta & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 & 0 \\ \ddots & \ddots & \ddots & \ddots & \ddots & \dots & \ddots & \ddots & \ddots & \ddots & \ddots \\ 0 & \ddots & 0 & \underbrace{\beta}_{(n\times q)^{th} diagonal} & 0 & \dots & 0 & 0 & 0 & 0 & 0 \end{pmatrix} \in M_{n\times m\times q}(\mathbb{N})$$

be a Rare matrix of order $n \times m \times q$ and index $n \times q$. Let

$$C_\delta = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 & \dots & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & \dots & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & \dots & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & \dots & 0 & 0 & 1 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \dots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 & 1 \\ \delta & 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 & 0 \\ 0 & \delta & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 & 0 \\ \ddots & \ddots & \ddots & \ddots & \ddots & \dots & \ddots & \ddots & \ddots & \ddots & \ddots \\ 0 & \ddots & 0 & \underbrace{\delta}_{(n\times m)^{th}diagonal} & 0 & \dots & 0 & 0 & 0 & 0 & 0 \end{pmatrix} \in M_{n\times m\times q}(\mathbb{N})$$

be a Rare matrix of order $n \times m \times q$ and index $n \times m$. A simple calculation shows that

$$A^n_\alpha = \alpha \times I_{n\times m\times q}, B^m_\beta = \beta \times I_{n\times m\times q}, C^q_\delta = \delta \times I_{n\times m\times q}.$$

Therefore,

$$A^n_x + B^m_y = C^q_{x+y}, \forall x, y \in \mathbb{N}.$$

Finally, the triples $(A_x, B_y, C_{x+y}), x, y \in \mathbb{N}$, are matrix solutions of the matrix Diophantine equation

$$X^n + Y^m = Z^q.$$

The matrix A_α generates at least $2n$ different construction structures of matrix solutions, the matrix B_β generates at least $2m$ different construction structures of matrix solutions and the matrix C_δ generates at least $2q$ different construction structures of matrix solutions. Finally, the matrices A_α, B_β and C_δ generate at least together $8 \times n \times m \times q$ different construction structures of matrix solutions of the matrix Diophantine equation

$$X^n + Y^m = Z^q.$$

□

Disclaimer

This paper is an extended version of a preprint document of the same author. The preprint document is available in this link: https://www.researchgate.net/publication/378846648_On_Construction_Structures_of_Matrix_Solutions_of_Linear_or_Exponential_Diophantine_Equations [As per journal policy, preprint article can be published as a journal article, provided it is not published in any other journal]

Competing Interests

Author has declared that no competing interests exist.

References

[1] Cohn JHE. The Diophantine equation $(a^n - 1)(b^n - 1) = x^2$. Period. Math. Hungar. 2002;44(2):169-175.

[2] 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.

[3] Lan L, Szalay L. On the exponential Diophantine equation $(a^n - 1)(b^n - 1) = x^2$. Publ. Math. Debrecen. 2010;77:1-6.

[4] Ishii K. On the exponential Diophantine equation $(a^n - 1)(b^n - 1) = x^2$. Publ. Math. Debrecen. 2016;89:253-256.

[5] Szalay L. On the Diophantine equation $(2^n - 1)(3^n - 1) = x^2$. Publ. Math. Debrecen. 2000;57:1-9.

[6] Xioyan G. A note on the Diophantine equation $(a^n - 1)(b^n - 1) = x^2$. Period. Math. Hungar. 2013;66:87-93.

[7] Yuan P, Zhang Z. On the Diophantine equation $(a^n - 1)(b^n - 1) = x^2$. Publ. Math. Debrecen. 2012;80:327-331.

[8] Noubissie A, Togb A, Zhongfeng Zhang. On the exponential Diophantine equation $(a^n - 1)(b^n - 1) = x^2$. Bulletin of the Belgian Mathematical Society - Simon Stevin. 2020;27(2):161-166.

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

[10] Bashmakova IG. Diophantus of Alexandria. Arithmetics and the Book of Polygonal Numbers. Moscow: Nauka (in Russian). 1974;85-86:215-217.

[11] Bennett MA, Skinner CM. Ternary Diophantine equation via Galois representations and modular forms. Canad. J. Math. 2004;56:23-54.

[12] Rivest R. Shamir A, Adleman L. A method for obtaining digital signatures and public-key cryptosystems. MIT Memo MIT/LCS/TM-82; 1977.

[13] Carmichael RD. On the numerical factor of the arithmetic form $\alpha^n \pm \beta^n$, Ann. Math. 1913;(2)15:30-70.

[14] Luca F. A note on the Pell equation. Indian J. Math. 1997;39:99-105.

[15] Luca F, Walsh PG. The product of like-indexed terms in binary recurrences. J. Number Theory. 2002;96:152-173.

[16] Robert W. van der Waall. 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.

[17] Rivest R, Shamir A, Adleman L. A method for obtaining digital signatures and public key cryptosystems. Comm. ACM. 1978;21:120-126.

[18] Boudot F, Gaudry P, Guillevic A, Heninger N, Thome E, Zimmermann P. Comparing the difficulty of factorization and discrete logarithm: A 240-digit experiment. Advances in Cryptology - CRYPTO 2020, Santa Barbara CA, United States. 2020;62-91.

[19] Meijer AR. Groups, factoring, and cryptography. Math. Mag. 1996;69:103-109.

[20] Coutinho SC. The mathematics of ciphers: Number theory and RSA cryptography. Wellesley, MA: A K Peters; 1999.

[21] Dickson LE. History of the theory of numbers. New York: Chelsea. 1966;2:518-519.

Peer-review history:
The peer review history for this paper can be accessed here (Please copy paste the total link in your browser address bar)
http://www.sdiarticle5.com/review-history/114693