Turkish Journal of Analysis and Number Theory, 2024, Vol. 12, No. 1, 1-7
Available online at http://pubs.sciepub.com/tjant/12/1/1
Published by Science and Education Publishing
DOI:10.12691/tjant-12-1-1

On Beal's Conjecture for Matrix Solutions and Multiplicative Commutative Groups of Rare Matrices

Joachim Moussounda Mouanda*

Blessington Christian University, Mathematics Department Nkayi, Republic of Congo
*Corresponding author: mmoussounda@yahoo.fr

Received January 16, 2024; Revised February 18, 2024; Accepted February 25, 2024

Abstract We introduce a new family of Toeplitz matrices called Rare matrices. We construct multiplicative commutative groups of Rare matrices and we establish connections with circulant matrices. We show that, in general, for every positive integer n, the equation $X^n+Y^{2n}=Z^n, n\geq 2,$ has an infinite number of matrix triple solutions $(A,B,C)\in M_n(\mathbb{N})^3$ with the matrices A, B and C do not have a common matrix factor. In other words, Beal's conjecture is not always true for matrix solutions.

Mathematics Subject Classification(2010) 15A24, 11D72, 15A16, 11A51.

Keywords: *Matrix equations, Diophantine Equations, Matrix inversion, Factorization*

Cite This Article: Joachim Moussounda Mouanda, "On Beal's Conjecture for Matrix Solutions and Multiplicative Commutative Groups of Rare Matrices." *Turkish Journal of Analysis and Number Theory*, vol. 12, no. 1 (2024): 1-7. doi: 10.12691/tjant-12-1-1.

1. Introduction

In 1993, Andrew Beal, a banker and amateur mathematician, while investigating generalizations of Fermat's Last Theorem, conjectured that if

$$a^x+b^y=c^z, a,b,c,x,y,z\in\mathbb{N}, x,y,z\geq 3, \quad (1.1)$$

then *a*, *b* and c have a common prime factor. Similar conjectures have been made before Beal's conjecture. For example, in 1914, Brun stated several similar problems [1]. In 1995, Darmon and Granville showed that if the positive integers x, y, and z are such that

$$1/x+1/y+1/z<1,$$

then there are only finitely many triples of coprime integers A,B, C satisfying

$$A^x+B^y=C^z.$$

This is known as the Fermat-Catalan Conjecture formulated by Darmon and Granville. For the case

$$x,y,z\geq 2,$$

with at least one of them is greater than 2, we have 10 well known examples:

$$\left\{\begin{array}{l} 1^m+2^3=3^2 (m\geq 1)\\ 2^5+7^2=3^4\\ 7^3+13^2=2^9\\ 2^7+17^3=71^2\\ 3^5+11^4=122^2\end{array}\right\}$$
$$\left\{\begin{array}{l} 17^7+76271^3=21063928^2\\ 1414^3+2213459^2=65^7\\ 9262^3+15312283^2=113^7\\ 43^8+96222^3=30042907^2\\ 33^8+1549034^2=15613^3.\end{array}\right\}$$

It is straightforward to observe that *a*,*b* and c, in each equation, do not have a common prime factor. As we can see, one of the exponents (x,y,z) is 2 while Beal's Conjecture requires all three exponents (x,y,z) to be 3 or greater [2]. It is well known that the equation (1.1) has an infinite number of positive integer solutions. For example, the solutions

$$3^{3n}+[2(3^n)]^3=3^{3n+2}, n\geq 1,$$

has bases with a common factor of 3, the solution $7^3+7^4=14^3$ has bases with a common factor of 7, and the solution $2^n+2^n=2^{n+1}$ has bases with a common factor of 2. There are infinitely many more well known solutions which are

$$[b(a^n-b^n)^k]^n+(a^n-b^n)^{kn+1}$$
$$=[a(a^n-b^n)^k]^n, a>b, b\geq 1, k\geq 1, n\geq 3,$$

and

$$[a(a^n+b^n)^k]^n+[b(a^n+b^n)^k]^n$$
$$=(a^n+b^n)^{kn+1}, a\geq 1, b\geq 1, k\geq 1, n\geq 3.$$

In 1997, Beal initially offered a prize of 5,000.00 US dollars for a published correct proof or counterexample in an internationally renowned refereed mathematics journal. This prize was raised to 50,000.00 US dollars [3]. Recently, Andrew Beal changed his mind by raising this prize from 50,000.00 US dollars to 1,000,000.00 US dollars [4]. Beal's conjecture still remain unsolved. However, partial results have been proved by many authors [4,5,8]. In 2022, for the first time, Mouanda constructed a new family of Toeplitz matrices called Rare matrices which allowed him to show that the Diophantine matrix equation

$$X_1^m+X_2^m+....+X_{n-1}^m=X_n^m, m\geq 2, n\geq 3,$$

has an infinite number of matrix solutions in $M_m(\mathbb{N})$ [6].

In this paper, we investigate the matrix approach of Beal's conjecture. In section 2, we introduce the new elementary properties of Rare matrices and we show that every positive rational number $\alpha\in\mathbb{Q}^+$ generates a multiplicative commutative group $\mathcal{R}_n(\alpha)$ of Rare matrices. In section 3, we establish the connections between these groups and circulant matrices. In section 4, we discuss the Integer Factorization problem. In section 5, we notice that

$$\begin{pmatrix}0&0&0&a&0&0\\0&0&1&0&0&0\\0&0&0&0&0&a\\0&0&0&0&1&0\\1&0&0&0&0&0\\0&1&0&0&0&0\end{pmatrix}^3+\begin{pmatrix}0&1&0&0&0&0\\0&0&1&0&0&0\\0&0&0&1&0&0\\0&0&0&0&1&0\\0&0&0&0&0&1\\b&0&0&0&0&0\end{pmatrix}^6=\begin{pmatrix}0&1&0&0&0&0\\0&0&1&0&0&0\\0&0&0&1&0&0\\0&0&0&0&1&0\\0&0&0&0&0&1\\a+b&0&0&0&0&0\end{pmatrix}^6$$

with

$$a,b\in\mathbb{N}.$$

The matrix structures of the above equation allow us to prove that, in general, Beal's conjecture is not true for matrix solutions.

Theorem 1.1. For every positive integer $n\in\mathbb{N}, n\geq 3$, the equation

$$X^n+Y^{2n}=Z^n, \tag{1.2}$$

has an infinite number of matrix solutions

$$(A,B,C)\in M_n(\mathbb{N})^3$$

with the matrices A, B and C do not have a common matrix factor. We have the same observations for the matrix solutions of the equations

$$X^{2n}+Y^{2n}=Z^{2n}, X^{2n}+Y^n=Z^n,$$
$$X^n+Y^n=Z^{2n}, n\geq 3, n\in\mathbb{N}. \tag{1.3}$$

2. Multiplicative Commutative Groups of Rare Matrices

In this section, we introduce the structures and properties of Rare matrices. We also construct multiplicative commutative groups of Rare matrices.

Let

$$M_n(\mathbb{C})=\left\{\begin{pmatrix}a_{1,1}&a_{1,2}&a_{1,3}&\ddots&a_{1,n-1}&a_{1,n}\\a_{2,1}&a_{2,2}&a_{2,3}&a_{2,4}&\ddots&a_{2,n}\\\ddots&\ddots&\ddots&\ddots&\ddots&\ddots\\\ddots&\ddots&\ddots&\ddots&\ddots&\ddots\\a_{n-1,1}&\ddots&\ddots&a_{n-1,n-2}&a_{n-1,n-1}&a_{n-1,n}\\a_{n,1}&a_{n,2}&\ddots&\ddots&a_{n,n-1}&a_{n,n}\end{pmatrix}: a_{i,j}\in\mathbb{C}\right\}$$

be the set of n-by-n complex matrices. The set $M_n(\mathbb{C})$ is not commutative.

Definition 2.1. A finite matrix $A=[a_{i,j}]_{i,j=1}^n$ is called a Toeplitz matrix if

$$a_{i+1,j+1}=a_{i,j}.$$

Each descending diagonal from left to right of a Toeplitz matrix is constant. For instance, the matrix

$$\begin{pmatrix}9&7&3&4&8\\8&9&7&3&4\\4&8&9&7&3\\3&4&8&9&7\\7&3&4&8&9\end{pmatrix},\begin{pmatrix}0&1&0&0&0\\0&0&1&0&0\\0&0&0&1&0\\0&0&0&0&1\\10&0&0&0&0\end{pmatrix},\begin{pmatrix}0&0&1&0&0\\0&0&0&1&0\\0&0&0&0&1\\11&0&0&0&0\\0&11&0&0&0\end{pmatrix}$$

are Toeplitz matrices with positive integers coefficients.

Definition 2.2. The nxn-Toeplitz 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 and 0. For example, the matrix

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

is called a Rare matrix of order n and index 2. Rare matrices have been first introduced by Mouanda in 2022 during his investigation on the matrix solutions of the Fermat matrix equation

$$X^n + Y^n = Z^n, n \geq 3$$ [6].

A simple calculation shows that

$$\begin{pmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 2 & 0 & 0 & 0 & 0 \end{pmatrix}^{-1} = \begin{pmatrix} 0 & 0 & 0 & 0 & \frac{1}{2} \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{pmatrix}$$

and

$$\begin{pmatrix} 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 3 & 0 & 0 & 0 & 0 \\ 0 & 3 & 0 & 0 & 0 \end{pmatrix}^{-1} = \begin{pmatrix} 0 & 0 & 0 & \frac{1}{3} & 0 \\ 0 & 0 & 0 & 0 & \frac{1}{3} \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 & 0 & \frac{1}{3} \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{pmatrix}^2.$$

We are interested on the investigation of the physical mutations of the coefficient α inside the matrix

$$\begin{pmatrix} 0 & 1 & 0 & 0 & \dots & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & \dots & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & \dots & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \dots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \dots & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & \dots & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 1 \\ \alpha & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 \end{pmatrix}^k \in M_n(\mathbb{C}), \alpha \neq 0, k \in \mathbb{N}.$$

After simple calculations, we find out that

$$\begin{pmatrix} 0 & 1 & 0 & 0 & \dots & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & \dots & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & \dots & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \dots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \dots & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & \dots & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 1 \\ \alpha & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 \end{pmatrix}^2 = \begin{pmatrix} 0 & 0 & 1 & 0 & \dots & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & \dots & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \dots & 1 & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \dots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \dots & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 1 \\ \alpha & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 \\ 0 & \alpha & 0 & 0 & \dots & 0 & 0 & 0 & 0 \end{pmatrix}$$

and

$$\begin{pmatrix} 0 & 1 & 0 & 0 & \dots & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & \dots & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & \dots & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \dots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \dots & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & \dots & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 1 \\ \alpha & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 \end{pmatrix}^3 = \begin{pmatrix} 0 & 0 & 0 & 1 & \dots & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \dots & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \dots & 0 & 1 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \dots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 1 \\ \alpha & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 \\ 0 & \alpha & 0 & 0 & \dots & 0 & 0 & 0 & 0 \\ 0 & 0 & \alpha & 0 & \dots & 0 & 0 & 0 & 0 \end{pmatrix}.$$

We can see that the coefficient α is keeping moving through diagonals when the value of k increases. This is an interesting phenomenon. Let us investigate more properties of Rare matrices.

Remark 2.3. 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

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

We can see that

$$A_\alpha^{-1} = \underbrace{A_1^T}_{\alpha}, A_\alpha^n = \alpha I_n, (\beta A_\alpha)^{-1} = \frac{1}{\beta} A_\alpha^{-1}, \beta \neq 0.$$

These observations allow us to say that

$$A_\alpha^{nk+q} = A_\alpha^{nk} A_\alpha^q = (A_\alpha^n)^k A_\alpha^q = (\alpha I_n)^k$$

$$A_\alpha^q = \alpha^k A_\alpha^q, q < n, A_\alpha \times \frac{1}{\alpha} A_\alpha^{n-1} \chi = I_n.$$

Therefore,

$$\begin{pmatrix} 0 & 1 & 0 & 0 & \dots & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & \dots & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & \dots & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \dots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \dots & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & \dots & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 1 \\ \alpha & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 \end{pmatrix}^{kn+q} = \alpha^k \begin{pmatrix} 0 & 1 & 0 & 0 & \dots & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & \dots & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & \dots & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \dots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \dots & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & \dots & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 1 \\ \alpha & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 \end{pmatrix}^q, q < n.$$

Suppose that

$$A_\alpha^j = T_j, 1 \leq j \leq n.$$

We can observe that

$$A_\alpha^n = T_n = \alpha I_n, A_\alpha^{nk} = T_n^k = \alpha^k I_n,$$

$$A_\alpha^{nk+q} = T_n^k T_q = \alpha^k T_q, q < n, n, q, k \in \mathbb{N}.$$

Definition 2.4. A (binary) operation on a non empty set G is a function

$$\mu : G \times G \to G.$$

An operation $*$ on a set G is associative if

$$(a * b) * c = a * (b * c),$$

for every a, b, c $\in G$.

Definition 2.5. A semigroup (G,*) is a nonempty set G equipped with an associative operation $*$. A group is a semigroup G containing an element e such that:

(i) $e*a=a=a*e$ for all $a\in G$;

(ii) for every $a\in G$, there is an element $b\in G$ with

$$a*b=e=b*a.$$

A pair of elements a and b in a semigroup commutes if $a*b=b*a$. A group (or semigroup) is abelian if every pair of its elements commutes.

We can now prove that every positive rational number generates a commutative group of Rare matrices.

Theorem 2.6. Let

$$\alpha\in\mathbb{Q}^{+}$$

be a positive rational number such that

$\alpha\neq 0$

and let

$$A_\alpha=\begin{pmatrix} 0 & 1 & 0 & 0 & \dots & 0 & 0 & 0 & 0\\ 0 & 0 & 1 & 0 & \dots & 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 1 & \dots & 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0\\ \vdots & \vdots & \vdots & \vdots & \dots & \vdots & \vdots & \vdots & \vdots\\ 0 & 0 & 0 & 0 & \dots & 0 & 1 & 0 & 0\\ 0 & 0 & 0 & 0 & \dots & 0 & 0 & 1 & 0\\ 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 1\\ \alpha & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 \end{pmatrix}\in M_n(\mathbb{Q}^{+}), n\geq 3,$$

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

$$\mathcal{R}_n(\alpha)=\left\{A_\alpha^k,(A_{\frac{1}{\alpha}}^T)^k:k\in\mathbb{N}\right\}\subset M_n(\mathbb{Q}^{+}),\alpha\in\mathbb{Q}^{+},$$

is a multiplicative commutative group.

Proof. Let

$$\alpha\in\mathbb{Q}^{+},\alpha\neq 0,$$

be a positive rational number. Remark 2.3 allows us to claim that

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

Therefore,

$$\mathcal{R}_n(\alpha)=\left\{A_\alpha^k,(A_{\frac{1}{\alpha}}^T)^k:k\in\mathbb{N}\right\}=\left\{A_\alpha^k,A_\alpha^{-k}:k\in\mathbb{N}\right\}\subset M_n(\mathbb{Q}^{+}),\alpha\in\mathbb{Q}^{+}$$

is a multiplicative commutative group. This yields us the desired result.

New Notation: Denote by

$$\mathcal{R}_n(\mathbb{Q}^{+})=\left\{\mathcal{R}_n(\alpha):\alpha\in\mathbb{Q}^{+}\right\}$$

the set of multiplicative commutative groups of nxn-Rare matrices. This set can be considered as the representations classes of positive rational numbers. In this set, every positive rational number α can be identified as the group $\mathcal{R}_n(\alpha)$.

We can denote by

$[\alpha]_{\mathcal{R}_n(\mathbb{Q}^{+})}=\mathcal{R}_n(\alpha)$, the representation class of α in $\mathcal{R}_n(\mathbb{Q}^{+})$. Also, we can notice that

$$\left\{\alpha^k A_\alpha^q:1\leq q<n,k\in\mathbb{N}\right\}\subset\mathcal{R}_n(\alpha),n\in\mathbb{N},n\geq 2$$

with A_α^q is a Rare matrix of order n and index q. Assume that

$$T_k=A_\alpha^k\Rightarrow T_k^n T_q=\alpha^k A_\alpha^q,1\leq q<n.$$

Theorem 2.6 allows us to say that

$$\mathcal{R}_n(\alpha)=\left\{A_\alpha^k,A_\alpha^{-k}:k\in\mathbb{N}\right\}=\left\{A_\alpha^k:k\in\mathbb{Z}\right\}\subset M_n(\mathbb{Q}^{+}),\alpha\in\mathbb{Q}^{+}.$$

3. Connections with Circulant Matrices

In section, we show that the elements of the group $[1]_{\mathcal{R}_n(\mathbb{Q}^{+})}$ allow the construction of circulant matrices of order n. Suppose that $n=5$ and $\alpha=1$. In this case, we have

$$T_1=A_1=\begin{pmatrix} 0 & 1 & 0 & 0 & 0\\ 0 & 0 & 1 & 0 & 0\\ 0 & 0 & 0 & 1 & 0\\ 0 & 0 & 0 & 0 & 1\\ 1 & 0 & 0 & 0 & 0 \end{pmatrix},T_2=\begin{pmatrix} 0 & 0 & 1 & 0 & 0\\ 0 & 0 & 0 & 1 & 0\\ 0 & 0 & 0 & 0 & 1\\ 1 & 0 & 0 & 0 & 0\\ 0 & 1 & 0 & 0 & 0 \end{pmatrix},T_3=\begin{pmatrix} 0 & 0 & 0 & 1 & 0\\ 0 & 0 & 0 & 0 & 1\\ 1 & 0 & 0 & 0 & 0\\ 0 & 1 & 0 & 0 & 0\\ 0 & 0 & 1 & 0 & 0 \end{pmatrix},$$

$$T_4=\begin{pmatrix} 0 & 0 & 0 & 0 & 1\\ 1 & 0 & 0 & 0 & 0\\ 0 & 1 & 0 & 0 & 0\\ 0 & 0 & 1 & 0 & 0\\ 0 & 0 & 0 & 1 & 0 \end{pmatrix},T_5=\begin{pmatrix} 1 & 0 & 0 & 0 & 0\\ 0 & 1 & 0 & 0 & 0\\ 0 & 0 & 1 & 0 & 0\\ 0 & 0 & 0 & 1 & 0\\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}=I_5.$$

Therefore,

$$[1]_{\mathcal{R}_5(\mathbb{Q}^{+})}=\mathcal{R}_5(1)=\left\{I_5,T_1,T_2,T_3,T_4\right\}=U_5$$

is a commutative group of circulant matrices, since

$T_1T_4=I_5$

and

$T_2T_3=I_5$.

We could use the elements of the finite group

$[1]_{\mathcal{R}_5(\mathbb{Q}^{+})}$

to construct circulant matrices of order 5. Indeed, let

$\{a_0,\dots,a_4\}$

be a finite set of complex numbers. A simple calculation shows that

$$\begin{pmatrix} a_0 & a_1 & a_2 & a_3 & a_4\\ a_4 & a_0 & a_1 & a_2 & a_3\\ a_3 & a_4 & a_0 & a_1 & a_2\\ a_2 & a_3 & a_4 & a_0 & a_1\\ a_1 & a_2 & a_3 & a_4 & a_0 \end{pmatrix}=\sum_{k=0}^{4}a_kT_k=\sum_{k=0}^{4}a_kA_1^k.$$

In the same way, we could use the elements of the group

$[1]_{\mathcal{R}_n(\mathbb{Q}^+)} = \mathcal{R}_n(1) = \{I_n, T_1, T_2, ..., T_{n-2}, T_{n-1}\} = U_n, T_j T_{n-j} = I_n$ to construct circulant matrices of order n+1. Indeed,

$$\begin{pmatrix} a_0 & a_1 & \ddots & a_{n-1} & a_n \\ a_n & a_0 & a_1 & \ddots & a_{n-1} \\ a_{n-1} & a_n & a_0 & a_1 & \ddots \\ \ddots & a_{n-1} & a_n & a_0 & a_1 \\ a_1 & \ddots & a_{n-1} & a_n & a_0 \end{pmatrix} = \sum_{k=0}^{n} a_k T_k = \sum_{k=0}^{n} a_k A_1^k.$$

4. Integer Factorization

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. 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 [9].

If we know the value of the matrix A_α, it is very easy to construct the elements of the group $\mathcal{R}_n(\alpha)$. However, constructing the matrix A_α once we know the value of the element $T_k^n = \alpha^k I_n$ of the group $\mathcal{R}_n(\alpha)$, k for sufficiently large (k has 650 digits), could be a difficult problem. This difficulty could lead to serious studies in cryptography. For example, given

$T_k^{10} = 272,440,639,012,851 \times I_{10} = A_\alpha^{10k} = \alpha^k I_{10}$.

Find $\alpha, p, k, A_\alpha, T_k^{10}$ and construct the commutative group $[\alpha]_{\mathcal{R}_n(\mathbb{Q}^+)} = \mathcal{R}_n(\alpha)$.

A simple calculation shows that

$$\alpha^k = 771^5 \Rightarrow \alpha = 771, k = 5.$$

We can now construct A_{771}, A_{771}^{-1}. Indeed,

$$A_{771} = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 771 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

and

$$A_{771}^{-1} = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \frac{1}{771} \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}.$$

Now we can claim that

$[771]_{\mathcal{R}_n(\mathbb{Q}^+)} = \mathcal{R}_{10}(771) = \left\{A_{771}^k, A_{771}^{-k} : k \in \mathbb{N}\right\} \subset M_{10}(\mathbb{Q}^+).$

What we learn in this section is that every element of the group $\mathcal{R}_n(\alpha)$ allows us to identify α. In other words, we could say that knowing one element of the group $\mathcal{R}_n(\alpha)$ allows us to identify α. Let us keep in mind that the elements of the group $\mathcal{R}_n(\alpha)$ for k sufficiently large make difficult to identify α. These elements completely hide the identity of α. Another example: Given

$T_k^{14} = 302,875,106,592,253 \times I_{14} = A_\alpha^{14k} = \alpha^k I_{14}$.

Construct the representation class $[\alpha]_{\mathcal{R}_{14}(\mathbb{Q}^+)}$. Answer: $\alpha^k = 13^{13} \Rightarrow \alpha = k = 13.$

As we can see, the element T_k^{14} allows us to identify the value of *a*. In our case, $\alpha = 13.$

$$[13]_{\mathcal{R}_{14}(\mathbb{Q}^+)} = \left\{ \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 13 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}^k : k \in \mathbb{Z} \right\}.$$

5. Proof of the Main Result

Multiplicative commutative groups

$$\mathcal{R}_n(\alpha), \alpha \in \mathbb{Q}^+, n \geq 3,$$

of Rare matrices, previously introduced in section 2, are powerful tools which can be used for finding the matrix solutions of the Diophantine equation

$X^n + Y^m = Z^k, n, m, k \geq 3$.

Let us notice that

$$\begin{pmatrix} 0 & 0 & 0 & a & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & a \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \end{pmatrix}^3 + \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ b & 0 & 0 & 0 & 0 & 0 \end{pmatrix}^6 = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ a+b & 0 & 0 & 0 & 0 & 0 \end{pmatrix}^6$$

with

$$a,b\in\mathbb{N}.$$

We can say that every pair (a,b) of positive integers generates a matrix solution of the equation

$$X^3+Y^6=Z^6.$$

The above matrix solutions of this equation do not have a common factor. Triples of positive integers which are solutions of the equation

$$x^2+y^2=z^2$$

are called Pythagorean triples. Let us notice that

$$\begin{pmatrix}0&1&0&0&0&0\\0&0&1&0&0&0\\0&0&0&1&0&0\\0&0&0&0&1&0\\0&0&0&0&0&1\\3&0&0&0&0&0\end{pmatrix}^{12}+\begin{pmatrix}0&1&0&0&0&0\\0&0&1&0&0&0\\0&0&0&1&0&0\\0&0&0&0&1&0\\0&0&0&0&0&1\\16&0&0&0&0&0\end{pmatrix}^{6}=\begin{pmatrix}0&1&0&0&0&0\\0&0&1&0&0&0\\0&0&0&1&0&0\\0&0&0&0&1&0\\0&0&0&0&0&1\\5&0&0&0&0&0\end{pmatrix}^{12},$$

since 9 + 16 = 25. We can deduce that if *a,b* and c are positive integers such that

$$a^2+b^2=c^2,$$

then

$$\begin{pmatrix}0&1&0&0&0&0\\0&0&1&0&0&0\\0&0&0&1&0&0\\0&0&0&0&1&0\\0&0&0&0&0&1\\a&0&0&0&0&0\end{pmatrix}^{12}+\begin{pmatrix}0&1&0&0&0&0\\0&0&1&0&0&0\\0&0&0&1&0&0\\0&0&0&0&1&0\\0&0&0&0&0&1\\b^2&0&0&0&0&0\end{pmatrix}^{6}=\begin{pmatrix}0&1&0&0&0&0\\0&0&1&0&0&0\\0&0&0&1&0&0\\0&0&0&0&1&0\\0&0&0&0&0&1\\c&0&0&0&0&0\end{pmatrix}^{12}.$$

Due to the fact that there is an infinite number of Pythagorean triples [7] implies that the matrix equation $X^{12}+Y^6=Z^{12}$ has an infinite number of matrix solutions which do not have common matrix factors. The elementary properties and the structure of the elements of the multiplicative commutative groups $\mathcal{R}_n(\alpha^2)$ and $\mathcal{R}_n(\alpha)$ allow us to prove our main result.

Proof of Theorem 1.1

Let (a,b,c) be a Pythagorean triple of positive integers. Therefore, $a^2+b^2=c^2$.

Let

$$(A_{a^2},B_b,C_{c^2})\in M_n(\mathbb{N})$$

be a triple of Rare matrices of order and n index 1 defined by

$$A_{a^2}=\begin{pmatrix}0&1&0&0&\dots&0&0&0&0\\0&0&1&0&\dots&0&0&0&0\\0&0&0&1&\dots&0&0&0&0\\0&0&0&0&\dots&0&0&0&0\\\vdots&\vdots&\vdots&\vdots&\dots&\vdots&\vdots&\vdots&\vdots\\0&0&0&0&\dots&0&1&0&0\\0&0&0&0&\dots&0&0&1&0\\0&0&0&0&\dots&0&0&0&1\\a^2&0&0&0&\dots&0&0&0&0\end{pmatrix},B_b=\begin{pmatrix}0&1&0&0&\dots&0&0&0&0\\0&0&1&0&\dots&0&0&0&0\\0&0&0&1&\dots&0&0&0&0\\0&0&0&0&\dots&0&0&0&0\\\vdots&\vdots&\vdots&\vdots&\dots&\vdots&\vdots&\vdots&\vdots\\0&0&0&0&\dots&0&1&0&0\\0&0&0&0&\dots&0&0&1&0\\0&0&0&0&\dots&0&0&0&1\\b&0&0&0&\dots&0&0&0&0\end{pmatrix}$$

and

$$C_{c^2}=\begin{pmatrix}0&1&0&0&\dots&0&0&0&0\\0&0&1&0&\dots&0&0&0&0\\0&0&0&1&\dots&0&0&0&0\\0&0&0&0&\dots&0&0&0&0\\\vdots&\vdots&\vdots&\vdots&\dots&\vdots&\vdots&\vdots&\vdots\\0&0&0&0&\dots&0&1&0&0\\0&0&0&0&\dots&0&0&1&0\\0&0&0&0&\dots&0&0&0&1\\c^2&0&0&0&\dots&0&0&0&0\end{pmatrix}\in M_n(\mathbb{N}),n\geq 3.$$

Remark 2.3 allows us to claim that

$$A_{a^2}^n=\begin{pmatrix}a^2&0&0&0&\dots&0&0&0&0\\0&a^2&0&0&\dots&0&0&0&0\\0&0&a^2&0&\dots&0&0&0&0\\0&0&0&a^2&\dots&0&0&0&0\\\vdots&\vdots&\vdots&\vdots&\dots&\vdots&\vdots&\vdots&\vdots\\0&0&0&0&\dots&a^2&0&0&0\\0&0&0&0&\dots&0&a^2&0&0\\0&0&0&0&\dots&0&0&a^2&0\\0&0&0&0&\dots&0&0&0&a^2\end{pmatrix},$$

$$B_b^{2n}=\begin{pmatrix}b^2&0&0&0&\dots&0&0&0&0\\0&b^2&0&0&\dots&0&0&0&0\\0&0&b^2&0&\dots&0&0&0&0\\0&0&0&b^2&\dots&0&0&0&0\\\vdots&\vdots&\vdots&\vdots&\dots&\vdots&\vdots&\vdots&\vdots\\0&0&0&0&\dots&b^2&0&0&0\\0&0&0&0&\dots&0&b^2&0&0\\0&0&0&0&\dots&0&0&b^2&0\\0&0&0&0&\dots&0&0&0&b^2\end{pmatrix}$$

and

$$C_{c^2}^n=\begin{pmatrix}c^2&0&0&0&\dots&0&0&0&0\\0&c^2&0&0&\dots&0&0&0&0\\0&0&c^2&0&\dots&0&0&0&0\\0&0&0&c^2&\dots&0&0&0&0\\\vdots&\vdots&\vdots&\vdots&\dots&\vdots&\vdots&\vdots&\vdots\\0&0&0&0&\dots&c^2&0&0&0\\0&0&0&0&\dots&0&c^2&0&0\\0&0&0&0&\dots&0&0&c^2&0\\0&0&0&0&\dots&0&0&0&c^2\end{pmatrix}.$$

It follows that

$$A_{a^2}^n+B_b^{2n}=C_{c^2}^n$$

Therefore, the triple

$$(A_{a^2},B_b,C_{c^2})$$

is a matrix solution of the equation $X^n+Y^{2n}=Z^n$. Due to the fact that every Pythagorean triple generates a matrix solution of this equation implies that this equation has an infinite number of matrix solutions. As we can see, the matrices

$$A_{a^2},B_b$$

and

$$C_{c^2}$$

do no have a common matrix factor. We have many similar observations. For instance, the triple

$$(A_a, B_{b^2}, C_c)$$

is a matrix solution of the Diophantine equation $X^{2n}+Y^n=Z^{2n}$.
Again the matrices

A_a, B_{b^2}

and

C_c

do no have a common matrix factor. The same phenomenon can be observed to the matrix triple

$$(A_a, B_b, C_c)$$

which is a solution of the matrix equation

$$X^{2n}+Y^{2n}=Z^{2n}.$$

We have the same observation for the matrix solutions of the equation $X^n+Y^n=Z^{2n}$. In this case, we could use the matrix triple (A_{a^2}, B_{b^2}, C_c).

We could even construct sequences of matrix triple solutions of the equation $X^{2n}+Y^n=Z^{2n}$ and end up having the same observations. For example, we could use the sequence $(A_n, B_{2n+1}, C_{n+1})_{n\geq 2}$ of matrix triple solutions of this equation. We observe that the matrices A_n, B_{2n+1} and C_{n+1} do no have a common matrix factor. This yields us the desired result.

Remark 5.1. Let α be a positive integer. Then,

$$\begin{pmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & \alpha^n & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 \end{pmatrix}^5 = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & \alpha & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 \end{pmatrix}^{5n}, n \in \mathbb{N}, n \geq 1.$$

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,

$$\begin{pmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & a & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 \end{pmatrix}^{5n} + \begin{pmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & R_n(a,b) & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 \end{pmatrix}^5 = \begin{pmatrix} 0 & a+b & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 \end{pmatrix}^{5n}$$

with

$$R_n(a,b) = \sum_{k=1}^{n} \frac{n!}{k!(n-k)!} a^{n-k} b^k, a, b, n \in \mathbb{N}, n \geq 2.$$

Finally, the Diophantine equation $X^{5n}+Y^5=Z^{5n}$ admits an infinite number of matrix solutions, which do no have a common matrix factor, for every positive integer n.

References

[1] V. Brun, Über hypothesenbildung, Arc. Math. Naturvidenskab 34 (1914), 1–14.

[2] H. Darmon and A. Granville, On the equations $Z^m = F(x, y)$ and $Ax^p + By^q = Cz^r$, in Bull. London Math. Soc., 27, 513-543(1995).

[3] Daniel Mauldin, R. A Generalization of Fermat's Last Theorem: The Beal Conjecture and Prize Problem. Notices of the American Mathematical Society, 44, 1436-1439(1997).

[4] Castelvecchi, D. "Mathematics Prize Ups the Ante to 1 Million US dollars". June 4, 2013.

[5] Leandro Torres Di Gregorio. Developments on Beal Conjecture from Pythagoras and Fermat's Equations. Pure and Applied Mathematics Journal. Vol.2, No.5, 149-155(2013).

[6] J. Moussounda Mouanda, On Matrix Solutions in $M_n(\mathbb{N})$ of the Diophantine Equation $X_1^m + ... + X_{n-1}^m = X_n^m, n \geq 3, m \geq 2$. https://www.researchgate.net/publication, 2022.

[7] J. Moussounda Mouanda, On Fermat's Last Theorem and Galaxies of sequences of positive integers, American Journal of Computational Mathematics, 12(2022), 162-189.

[8] R.C. A Proof to Beal's Conjecture. Bulletin of Mathematical Sciences and Applications, 89-93(2014).

[9] R. Rivest, A. Shamir and L. Adleman, "A Method for Obtaining DigitalSignatures and Public Key Cryptosystems." Comm. ACM 21, 120-126,1978.