Scientific Research Publishing

American Journal of Computational Mathematics, 2025, 15(4), 498-505
https://www.scirp.org/journal/ajcm
ISSN Online: 2161-1211
ISSN Print: 2161-1203

On Matrix Strong Exponential Diophantine *m*-Tuples of Order *n*

Djagwa Dehainsala[1], Joachim Moussounda Mouanda[2]

[1]Mathematics Department, N'Djamena University, N'Djamena, Tchad
[2]Mathematics Department, Blessington Christian University, Nkayi, Republic of Congo
Email: djagwa73@gmail.com, mmoussounda@yahoo.fr

How to cite this paper: Dehainsala, D. and Mouanda, J.M. (2025) On Matrix Strong Exponential Diophantine *m*-Tuples of Order *n*. *American Journal of Computational Mathematics*, **15**, 498-505.
https://doi.org/10.4236/ajcm.2025.154022

Received: July 25, 2025
Accepted: November 29, 2025
Published: December 2, 2025

Abstract

We construct matrix strong exponential Diophantine m-tuples of order n. We construct matrix strong exponential Diophantine 540-tuples of order n. We show that matrix strong Diophantine m-tuples generate matrix strong exponential Diophantine m-tuples of order n and we construct matrix elliptic curves.

Keywords

Matrices of Integers, Diophantine m-Tuples, Elliptic Curves

1. Introduction and Main Result

A set of m positive integers (rational numbers) $\{a_1, a_2, \cdots, a_m\}$ is called a (rational) Diophantine m-tuple if $a_i a_j + 1$ is a perfect square for all $1 \le i < j \le m$. The problem of finding four numbers such that the product of any two of them increased by unity is a perfect square was first solved by the Greek mathematician Diophantus of Alexandria [1]. He found a set of four positive rational numbers $\left\{\frac{1}{16}, \frac{33}{16}, \frac{17}{4}, \frac{105}{16}\right\}$ which satisfy this property. The first set of four positive integers with the above property $\{1,3,8,120\}$ was introduced by Pierre de Fermat. In 1753, Leonhard Euler found an infinite number of sets of four positive integers $\{a, b, a+b+2r, 4r(r+a)(r+b)\}$ where $ab+1=r^2$, $a,b \in \mathbb{N}$. In other words, every Diophantine pair can be extended to a Diophantine quadruple. Euler was able to add the fifth positive rational $\frac{777480}{8288641}$ to Fermat's set [2]. In 1969, Baker and Davenport proved that it is not possible to add a fifth positive integer to Fermat's set. The Fibonacci sequence $(F_k)_{k\ge 0}$ has several strong connections with

the Diophantine quadruples. In 1977, Hoggatt and Bergum conjectured that the set $\{F_{2k}, F_{2k+2}, F_{2k+4}, 4F_{2k+1}F_{2k+2}F_{2k+3}\}$ is a Diophantine quadruple [3]. In 1979, Arkin, Hoggatt and Strauss proved that every Diophantine triple can be extended to a Diophantine quadruple [4]. More precisely, let $\{a,b,c\}$ be a Diophantine triple such that

$$ab+1=r^2, ac+1=s^2, bc+1=t^2.$$

Define $d=a+b+c+2abc+2rst$. Then the set $\{a,b,c,d\}$ is a Diophantine quadruple since

$$ad+1=(at+rs)^2, bd+1=(bs+rt)^2, dc+1=(cr+st)^2.$$

In 1980, Veluppillai extended the triple $\{2,4,12\}$ to a Diophantine quadruple [5]. In 1998, Kedlaya extended the following triples [6]:

$$\{1,3,120\}, \{1,8,120\}, \{1,8,15\}, \{1,15,35\}, \{1,24,35\}, \{2,12,24\}$$

to Diophantine quadruples. In 1997 and 1998 [7] [8] proved that the sets $\{k-1,k+1,4k\}$ and $\{F_{2k}, F_{2k+2}, F_{2k+4}\}$ can be extended respectively to a Diophantine quadruple. In 1998, Dujella and Petho [9] proved that the pair $\{1,3\}$ cannot be extended to a Diophantine quintuple. In 1999, Dujella proved the Hoggatt-Bergum conjecture, and this result also implies that if $\{F_{2k}, F_{2k+2}, F_{2k+4}, d\}$ is a Diophantine quadruple, then d cannot be a Fibonacci number [8]. In 2008, Fujita proved that, for $k \geq 2$, the Diophantine pair $\{k-1,k+1\}$ cannot be extended to a Diophantine quintuple [10]. The question of finding the existence of Diophantine quintuples was one of the oldest outstanding unsolved problems in Number Theory. In 2004, Dujella showed that there are no Diophantine sextuplets and there are at most a finite number of Diophantine quintuples exist [11]. In 2019, He, Togbe and Zieglé [12] proved that Diophantine quintuples do not exist. A set of m nonzero positive rational numbers $\{a_1, \cdots, a_m\}$ is called a strong Diophantine m-tuple if $a_i a_j + 1$ is a perfect square for all $i, j = 1, 2, \cdots, m$. It is quiet clear that there does not exist a strong Diophantine pair consisting of integers. However, in 2008, Dujella and PetričCevic [13] proved that there exist infinitely many strong Diophantine triples of positive rational numbers and it is not known whether any strong Diophantine quadruple exists. We are dealing with one specific variant of the described problems, namely with matrix strong Diophantine m-tuples. A set of m matrices with positive integers (rational number) as entries $\{A_1, A_2, \cdots, A_m\}$, is called a (rational) matrix Diophantine m-tuple if $A_i A_j + I_n, A_j A_i + I_n$ are (rational) matrix squares, with positive integers as entries, for all $1 \leq i, j \leq m$, $i \neq j$, $A_i \in M_n(\mathbb{N})$. A set of m matrices with positive integers (rational numbers) as entries

$$\{A_1, A_2, \cdots, A_m\} \subset M_n(\mathbb{N}),$$

is called a matrix (rational) strong Diophantine m-tuple if $A_i A_j + I_n, A_j A_i + I_n$ are matrix squares for all $i, j = 1, \cdots, m$. In 2023, Mouanda [14] [15] proved that there exists an infinite number of matrix strong Diophantine 540-tuples with positive integers entries and constructed the associated matrix elliptic curves.

In this paper, we construct matrix strong exponential Diophantine *m*-tuples, defined in Section 2. We construct matrix exponential Diophantine 540-tuples of order n. We show that matrix strong Diophantine *m*-tuples generate matrix strong exponential Diophantine *m*-tuples.

Theorem 1.1. *Every matrix strong Diophantine m-tuple* $\{A_1, A_2, \cdots, A_m\}$ *generates a matrix strong exponential Diophantine m-tuples*

$$\{X_1, X_2, \cdots, X_m\} \subset M_{nq}(\mathbb{N}), A_i \in M_q(\mathbb{N}),$$

of order n.

We construct matrix elliptic curves described in Section 3.

2. Proof of the Main Result

In this section, we introduce new concepts linked to Diophantine *m*-tuples. In particular, we investigate Diophantine *m*-tuples of the form

$$\left\{\left(x_1^n - 1\right), \left(x_2^n - 1\right), \cdots, \left(x_m^n - 1\right)\right\}, n \in \mathbb{N}, n \geq 1.$$

This concept is completely new and we are interested on knowing the possible length of m. This will allow us to explore new types of Diophantine *m*-tuples. Finite sets of positive integers which satisfy the Diophantine equation

$$\left(x^n - 1\right)\left(y^n - 1\right) + 1 = z^2$$

never been explored before.

Definition 2.1. *A set of* m *positive integers* (*rational numbers*) $\{a_1, a_2, \cdots, a_m\}$ *is called an exponential* (*rational*) *Diophantine m-tuple of order* n *if* $\left(a_i^n - 1\right)\left(a_j^n - 1\right) + 1$ *is a* (*rational*) *perfect square for all* $1 \leq i, j \leq m$, $i \neq j$.

Definition 2.2. *A set of* m *positive integers* (*rational numbers*) $\{a_1, a_2, \cdots, a_m\}$ *is called a strong exponential* (*rational*) *Diophantine m-tuple of order* n *if* $\left(a_i^n - 1\right)\left(a_j^n - 1\right) + 1$ *is a* (*rational*) *perfect square for all* $1 \leq i, j \leq m$.

Strong exponential Diophantine *m*-tuples of order n of positive integers do not exist.

Assume that $n = 1$. The set $\{2, 4, 9, 121\}$ is an exponential Diophantine quadruple of order 1. Every quadruple generates an exponential Diophantine quadruple of order 1. Indeed, if set $\{a, b, c, d\}$ is a Diophantine quadruple, then the set $\{a+1, b+1, c+1, d+1\}$ is an exponential Diophantine quadruple of order 1. In fact, there is no exponential Diophantine quintuple

$$\{(x_1 - 1), (x_2 - 1), (x_3 - 1), (x_4 - 1), (x_5 - 1)\}$$

of order 1 of positive integers.

Assume $n = 2$, the set $\{2, 3, 11\}$ is an exponential Diophantine triple of order 2. It is not known if there exists any exponential Diophantine quadruple of order 2.

Assume $n = 3$. In 2023, Adjibad Mustapha showed that the set $\{11, 13\}$ is an exponential Diophantine pair of order 3. That is, $\left(11^3 - 1\right)\left(13^3 - 1\right) + 1 = 1709^2$. It is not known if there exists any exponential Diophantine triple of order 3. We also

introduce the matrix version of this new concept. 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.

Definition 2.3. *A set of* m *matrices* $\{A_1, A_2, \cdots, A_m\}$ *with positive integers* (*rational numbers*) *as entries is called a matrix* (*rational*) *exponential Diophantine m-tuple of order* n *if* $\left(A_i^n - I_q\right)\left(A_j^n - I_q\right) + I_q$ *are matrix* (*rational*) *squares with positive integers* (*rational number*) *as entries for all* $i \neq j$.

Definition 2.4. *A set of* m *matrices* $\{A_1, A_2, \cdots, A_m\}$ *with positive integers* (*rational numbers*) *as entries is called a matrix* (*rational*) *strong exponential Diophantine m-tuple of order* n *if* $\left(A_i^n - I_q\right)\left(A_j^n - I_q\right) + I_q$ *are* (*rational*) *matrix squares with positive integers as entries for all* $1 \leq i, j \leq m$.

Every Diophantine quadruple $\{a, b, c, d\}$ generates a matrix exponential Diophantine quadruple of order 2 (or 3). Indeed, let

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

be a Rare matrix of order 6 and index 3. A simple calculation shows that $A_x^2 = (x+1) I_6$. Therefore, the set

$$\{A_a, A_b, A_c, A_d\}$$

is a matrix exponential Diophantine quadruple of order 2. In the other hand, let

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

be a Rare matrix of order 6 and index 2. A simple calculation shows that $B_x^3 = (x+1) I_6$. Therefore, the set

$$\{B_a, B_b, B_c, B_d\}$$

is a matrix exponential Diophantine quadruple of order 3. We can now prove that exponential Diophantine quintuples do not exist.

Theorem 2.5. *There does not exist an exponential Diophantine quintuple of*

order n of positive integers.

Proof. A set of m positive integers $\{a_1, a_2, \cdots, a_m\}$ is called an exponential Diophantine *m*-tuple of order n if $\left(a_i^n - 1\right)\left(a_j^n - 1\right) + 1$ is a perfect square for all $1 \le i, j \le m$ with $i \ne j$. In other words, the set $\left\{a_1^n - 1, a_2^n - 1, \cdots, a_m^n - 1\right\}$ is a Diophantine *m*-tuple for a given n. Due to the fact that Diophantine quintuples do not exist implies that $m \le 4$.

Mouanda and Dehainsala, proved that there exists an infinite number of matrix strong Diophantine 540-tuples [15]. It is now possible to construct matrix exponential Diophantine 540-tuples of order n.

Theorem 2.6. *There exist infinitely many matrix exponential Diophantine* 540-*tuples of order* n.

Proof. Let $W = \left\{A_i : i = 1, 2, 3, \cdots, 540\right\} \subset M_q\left(\mathbb{N}\right)$ be a matrix strong Diophantine 540-tuple. Let α be a positive integer and let

$$X_\alpha = \begin{pmatrix} 0 & 0 & 1 & \cdots & 0 & 0 & 0 \\ 0 & 0 & 0 & \cdots & 0 & 0 & 0 \\ 0 & 0 & 0 & \cdots & 1 & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & 0 & 1 \\ \alpha+1 & 0 & 0 & \cdots & 0 & 0 & 0 \\ 0 & \alpha+1 & 0 & \cdots & 0 & 0 & 0 \end{pmatrix} \in M_{2n}\left(\mathbb{N}\right)$$

be a complex matrix. It is well known that $X_\alpha^n = \left(\alpha+1\right) I_{2n}$. Therefore,

$$X_{A_i} = \begin{pmatrix} 0 & 0 & I_q & \cdots & 0 & 0 & 0 \\ 0 & 0 & 0 & \cdots & 0 & 0 & 0 \\ 0 & 0 & 0 & \cdots & I_q & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & 0 & I_q \\ A_i + I_q & 0 & 0 & \cdots & 0 & 0 & 0 \\ 0 & A_i + I_q & 0 & \cdots & 0 & 0 & 0 \end{pmatrix} \in M_{2nq}\left(\mathbb{N}\right).$$

This implies that $X_{A_i}^n = \left(A_i + I_q\right) I_{2nq}$. We can claim that

$$X_{A_i}^n - I_{2nq} = A_i I_{2nq}.$$

Thus

$$\left(X_{A_i}^n - I_{2nq}\right)\left(X_{A_j}^n - I_{2nq}\right) + I_{2nq} = \left(A_i A_j + I_q\right) I_{2nq} = B_{i,j}^2 I_{2nq}.$$

The set $\left\{X_{A_i} : i = 1, \cdots, 540\right\}$ is a matrix strong exponential Diophantine 540-tuple of order n. It is well known that there exist infinitely many matrix strong Diophantine 540-tuples. Finally, there exist infinitely many matrix strong exponential Diophantine 540-tuples of order n.

We can now prove our main result, Theorem 1.1.

Proof. Let $W = \left\{A_i : i = 1, 2, 3, \cdots, m\right\} \subset M_q\left(\mathbb{N}\right)$ be a matrix strong Diophantine *m*-tuple. Let α be a positive integer and let

$$X_\alpha = \begin{pmatrix} 0 & 0 & 1 & \cdots & 0 & 0 & 0 \\ 0 & 0 & 0 & \cdots & 0 & 0 & 0 \\ 0 & 0 & 0 & \cdots & 1 & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & 0 & 1 \\ \alpha+1 & 0 & 0 & \cdots & 0 & 0 & 0 \\ 0 & \alpha+1 & 0 & \cdots & 0 & 0 & 0 \end{pmatrix} \in M_{2n}(\mathbb{N})$$

be a complex matrix. It is well known that $X_\alpha^n = (\alpha+1) I_{2n}$. Therefore,

$$X_{A_i} = \begin{pmatrix} 0 & 0 & I_q & \cdots & 0 & 0 & 0 \\ 0 & 0 & 0 & \cdots & 0 & 0 & 0 \\ 0 & 0 & 0 & \cdots & I_q & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & 0 & I_q \\ A_i + I_q & 0 & 0 & \cdots & 0 & 0 & 0 \\ 0 & A_i + I_q & 0 & \cdots & 0 & 0 & 0 \end{pmatrix} \in M_{2nq}(\mathbb{N}).$$

This implies that $X_{A_i}^n = (A_i + I_q) I_{2nq}$. We can claim that

$$X_{A_i}^n - I_{2nq} = A_i I_{2nq}.$$

Thus

$$\left(X_{A_i}^n - I_{2nq}\right)\left(X_{A_j}^n - I_{2nq}\right) + I_{2nq} = \left(A_i A_j + I_q\right) I_{2nq} = B_{i,j}^2 I_{2nq}.$$

The set $\left\{X_{A_i} : i = 1, \cdots, m\right\} \subset M_{2nq}(\mathbb{N})$ is a matrix strong exponential Diophantine m-tuple of order n. Finally, every matrix strong Diophantine m-tuples generates a matrix strong exponential Diophantine m-tuple of order n.

3. Matrix Elliptic Curves

Elliptic curves play an important role in cryptography. Perhaps by extending this work to matrices, we could investigate and introduce another new concept called matrix cryptography. In this section, we explore new types of matrix elliptic curves. We investigate matrix elliptic curves which do not have any positive integer points. Let $\left\{a_1, a_2, \cdots, a_m\right\}$ be an exponential Diophantine m-tuple of order 3. Let

$$E : y^2 = \left(a_1^3 - 1\right)\left(x^3 - 1\right) + 1$$

and

$$E_0 : y^2 = \left[\left(a_1^3 - 1\right)\left(x^3 - 1\right) + 1\right]\left[\left(a_2^3 - 1\right)\left(a_3^3 - 1\right) + 1\right]\left[\left(a_4^3 - 1\right)\left(a_5^3 - 1\right) + 1\right]$$

be two elliptic curves. Every element of the set $\left\{a_2, \cdots, a_m\right\}$ generates a point on E and every element of the set $\left\{a_6, a_7, \cdots, a_m\right\}$ generates a point on E_0.

Let $\left\{X_i : i = 1, \cdots, 540\right\} \subset M_p(\mathbb{N})$ be a matrix strong exponential Diophantine 540-tuple of order 3. Every matrix of the set $\left\{X_i : i = 2, \cdots, 540\right\}$ generates a matrix point of the matrix elliptic curve

$$E: Y^2 = \left(X_1^3 - I_p\right)\left(X^3 - I_p\right) + I_p.$$

However, every matrix of the set $\{X_i : i = 6, \cdots, 540\}$ generates a matrix point of the matrix elliptic curve

$$E_0: Y^2 = \left[\left(X_1^3 - I_p\right)\left(X^3 - I_p\right) + I_p\right]\left[\left(X_2^3 - I_p\right)\left(X_3^3 - I_p\right) + I_p\right]\left[\left(X_4^3 - I_p\right)\left(X_5^3 - I_p\right) + I_p\right].$$

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

[1] Bashmakova, I.G. (1971) Diophantus of Alexandria, Arithmetics and the Book of Polygonal Numbers. Nauka.

[2] Euler, L. (1738) Theorematum quorundam arithmeticorum demonstrations. *Novi Commentarii academiae scientiarum Petropolitanae*, **10**, 125-146.

[3] Hoggatt, V.E. and Bergum, G.E. (1977) A Problem of Fermat and the Fibonacci Sequence. *The Fibonacci Quarterly*, **15**, 323-330. https://doi.org/10.1080/00150517.1977.12430412

[4] Arkin, J., Hoggatt, V.E. and Straus, E.G. (1979) On Euler's Solution to a Problem of Diophantus. *The Fibonacci Quarterly*, **17**, 333-339. https://doi.org/10.1080/00150517.1979.12430206

[5] Veluppillai, M. (1980) The Equations $z^2 - 3y^2 = -2$ and $z^2 - 6x^2 = -5$, A Collection of Manuscripts Related to the Fibonacci Sequence. The Fibonacci Association, Santa Clara, 71-75.

[6] Kedlaya, K. (1998) Solving Constrained Pell Equations. *Mathematics of Computation*, **67**, 833-842. https://doi.org/10.1090/s0025-5718-98-00918-1

[7] Dujella, A. (1997) The Problem of the Extension of a Parametric Family of Diophantine Triples. *Publicationes Mathematicae Debrecen*, **51**, 311-322. https://doi.org/10.5486/pmd.1997.1886

[8] Dujella, A. (1999) A Proof of the Hoggatt-Bergum Conjecture. *Proceedings of the American Mathematical Society*, **127**, 1999-2005. https://doi.org/10.1090/s0002-9939-99-04875-3

[9] Dujella, A. and Petho, A. (1998) A Generalization of a Theorem of Baker and Davenport. *The Quarterly Journal of Mathematics*, **49**, 291-306. https://doi.org/10.1093/qmathj/49.3.291

[10] Fujita, Y. (2008) The Extensibility of Diophantine Pairs $\{k-1, k+1\}$. *Journal of Number Theory*, **128**, 322-353. https://doi.org/10.1016/j.jnt.2007.03.013

[11] Dujella, A. (2004) There Are Only Finitely Many Diophantine Quintuples. *Journal für die reine und angewandte Mathematik* (*Crelles Journal*), **2004**, 183-214. https://doi.org/10.1515/crll.2004.003

[12] He, B., Togbé, A. and Zieglé, V. (2019) There Is No Diophantine Quintuple. *Transactions of the American Mathematical Society*, **371**, 6665-6709.

[13] Dujella, A. and Petričcević, V. (2008) Strong Diophantine Triples. *Experimental Mathematics*, **17**, 83-89. https://doi.org/10.1080/10586458.2008.10129020

[14] Mouanda, J.M. and Vincent, K.K. (2024) On Matrix Strong Diophantine 27-Tuples and Matrix Elliptic Curves. *Mathematics and Systems Science*, **2**, Article 2624. https://doi.org/10.54517/mss.v2i2.2624

[15] Dehainsala, D. and Mouanda, J.M. (2025) On Matrix Strong Diophantine 540-Tuples, Matrix Elliptic Curves and Matrix Hyperelliptic Curves. *Advances in Pure Mathematics*, **15**, 751-762. https://doi.org/10.4236/apm.2025.1511041