Scientific Research Publishing

Advances in Pure Mathematics, 2025, 15(11), 751-762
https://www.scirp.org/journal/apm
ISSN Online: 2160-0384
ISSN Print: 2160-0368

On Matrix Strong Diophantine 540-Tuples, Matrix Elliptic Curves and Matrix Hyperelliptic Curves

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 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

Received: September 13, 2025
Accepted: November 25, 2025
Published: November 28, 2025

Abstract

We introduce an algorithm which allows us to prove that there exists an infinite number of matrix strong Diophantine 540-tuples with positive integers as entries. We construct matrix elliptic curves and matrix hyperelliptic curves by using matrix strong Diophantine 540-tuples.

Keywords

Matrices, Diophantine m-Tuples, Elliptic Curves

1. Introduction and Main Result

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 before 1637 [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 $\left\{a,b,a+b+2r,4r\left(r+a\right)\left(r+b\right)\right\}$ where $ab+1=r^2$, $a,b\in\mathbb{N}$. In other words, every Diophantine pair can be extended to a Diophantine quadruple. He was able to add the fifth positive rational $\frac{777480}{8288641}$ to Fermat's set [2]. In 1969, Baker and Davenport proved that that it is impossible to extend Fermat's set to a Diophantine quintuple [3]. The Fibonacci sequence $\left(F_k\right)_{k\geq 0}$ has several strong connections with the Diophantine quadruples. In 1977, Hoggatt and Bergum conjectured that the set

$$\{F_{2k}, F_{2k+2}, F_{2k+4}, 4F_{2k+1}F_{2k+2}F_{2k+3}\}$$

cannot be extended to a Diophantine quintuple [4]. In 1979, Arkin, Hoggatt and Strauss proved that every Diophantine triple can be extended to a Diophantine quadruple [5]. 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

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

In 1980, Veluppillai extended the triple $\{2,4,12\}$ [6]. In 1998, Kedlaya extended the following triples [7]:

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

In 1997 [8] and 1998 [9], it was 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 Peth proved that the pair $\{1,3\}$ cannot be extended to a Diophantine quintuple [10]. 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 [11]. In 2008, Fujita proved that for $k\geq 2$, the Diophantine pair $\{k-1,k+1\}$ cannot be extended to a Diophantine quintuple [12]. 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 sextuples and at most a finite number of Diophantine quintuples exist [13]. In 2019, He, Togbe and Zieglé proved that Diophantine quintuples do not exist [14]. A set of m nonzero positive rational numbers $\{a_1,\cdots,a_m\}$ is called a strong Diophantine m-tuple if a_ia_j+1 is a perfect square for all $i, j=1,2,\cdots,m$. It is quite clear that there does not exist a strong Diophantine pair consisting of integers. However, in 2008, Dujella and Petrič Cević proved that there exist infinitely many strong Diophantine triples of positive rational numbers. It is not known whether there exist any strong Diophantine quadruples. In 2024, Mouanda and Kouakou proved that there exists an infinite number of matrix strong Diophantine 27-tuples [15]. In the second century A. D, elliptic curves were introduced by the Greek mathematician Diophantus of Alexandria. Properties and functions of elliptic curves have been studies in mathematics for 150 years. In 1920, elliptic curves were studied separately by Cauchy, Lucas, Sylvester, Poincare. In 1984, Lenstra used elliptic curves for factoring integers. More details about elliptic curves can be found in [16].

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

In this paper, we construct matrix strong Diophantine 540-tuples by using Diophantine quadruples.

Theorem 1.1. *There exists an infinite number of matrix strong Diophantine 540-tuples.*

We also construct elliptic curves and hyperelliptic curves by using matrix strong Diophantine 540-tuples.

2. Proof of the Main Result

In this section, we construct matrix strong Diophantine 540-tuples with positive integers as entries by using Diophantine quadruples. 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. Assume that

$$A=\left[a_{i,j}\right]_{i,j=1}^{n}=\begin{pmatrix} a_{1,1} & a_{1,2} & a_{1,3} & \ddots & a_{1,n-1} & a_{1,n} \\ a_{2,1} & a_{2,2} & a_{2,3} & a_{2,4} & \ddots & a_{2,n} \\ \ddots & \ddots & \ddots & \ddots & \ddots & \ddots \\ \ddots & \ddots & \ddots & \ddots & \ddots & \ddots \\ a_{n-1,1} & \ddots & \ddots & a_{n-1,n-2} & a_{n-1,n-1} & a_{n-1,n} \\ a_{n,1} & a_{n,2} & \ddots & \ddots & a_{n,n-1} & a_{n,n} \end{pmatrix}\in M_n(\mathbb{N}).$$

Definition 2.1. *A set of* m *positive integers* $\{a_1,a_2,\cdots,a_m\}$ *is called a Diophantine m-tuple if* a_ia_j+1 *is a perfect square for all* $1\le i<j\le m$.

Definition 2.2. *A set of* m *positive rational numbers* $\{a_1,a_2,\cdots,a_m\}$ *is called a rational Diophantine m-tuple if* a_ia_j+1 *is a rational square for all* $1\le i<j\le m$.

Definition 2.3. *A set of* m *matrices with positive integers as entries* $\{A_1,A_2,\cdots,A_m\}$, *is called a matrix Diophantine m-tuple if* $A_iA_j+I_n$ *is a matrix square, with positive integers as entries, for all* $1\le i<j\le m$, $A_i\in M_n(\mathbb{N})$.

Definition 2.4. *A set of* m *matrices with positive rational numbers as entries* $\{A_1,A_2,\cdots,A_m\}$, $A_i\in M_n(\mathbb{Q})$, *is called a rational matrix Diophantine m-tuple if* $A_iA_j+I_n$ *is a rational matrix square, with positive rational numbers as entries, for all* $1\le i<j\le m$.

The Main Question: Are any matrix Diophantine quintuples (sextuples, septuples)? Can there be an infinite Diophantine tuple?

Let $S=\{a_1,a_2,\cdots\}$ be a Diophantine tuple. Consider the elliptic curve

$$y^2=(a_1x+1)(a_2x+1)(a_3x+1).$$

Then, every integer x of the set $\{a_4,a_5,\cdots\}$ generates an integer point on this curve.

Theorem 2.5. (*Siegel*) [17]. *The number of integers points on the elliptic curve* $y^2=x^3+ax+b$ *is finite.*

This result allows us to claim that the number of elements of S is finite. In 2019, He, Togbe and Ziegler [14] proved that there does not exist any Diophantine quintuple. This is not true at all for Diophantine *m*-tuples over the set matrices of $M_n(\mathbb{N})$.

Definition 2.6. *A set of* m *positive integers* $\{a_1, a_2, \cdots, a_m\}$ *is called a strong Diophantine m-tuple if* $a_i a_j + 1$ *is a perfect squares for all* $1 \le i \le j \le m$.

This definition includes the case $a_i^2 + 1$ is a perfect square for all i.

Definition 2.7. *A set of* m *positive rational numbers* $\{a_1, a_2, \cdots, a_m\}$ *is called a rational strong Diophantine m-tuple if* $a_i a_j + 1$ *is a rational squares for all* $1 \le i \le j \le m$.

In the case of matrices, we introduce a new definition.

Definition 2.8. *A set of* m *matrices with positive integers as entries*

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

is called a matrix strong Diophantine *m*-tuple if $A_i A_j + I_n, A_j A_i + I_n$ are matrix squares for all $1 \le i \le j \le m$.

Definition 2.9. *A set of* m *matrices with positive rational numbers as entries* $\{A_1, A_2, \cdots, A_m\}$, $A_i \in M_n(\mathbb{Q})$, *is called a rational matrix strong Diophantine m-tuple if* $A_i A_j + I_n, A_j A_i + I_n$ *are rational matrix squares, with positive rational numbers as entries, for all* $1 \le i \le j \le m$.

The Main Question: Are any matrix strong Diophantine quintuples (sextuples, septuples)? Can there be an infinite matrix strong Diophantine tuple?

First of all, let us observe that the set $S = \{a_1, a_2, \cdots, a_m\}$ is said a strong Diophantine *m*-tuple if the set S is a Diophantine *m*-tuple and $a_i^2 + 1$ is a perfect square for all $1 \le i \le m$. Finding strong Diophantine *m*-tuples is equivalent of solving the equation

$$x^2 + 1 = y^2, x, y \in \mathbb{N}, x \ne 0. \tag{2.1}$$

The structure of Pythagorean triples allows us to claim that equation (2.1) has no positive integer solutions. Indeed, assume that there exist two positive integers such that

$$x^2 + 1 = y^2, x, y \in \mathbb{N}, x \ne 0. \tag{2.2}$$

This equation is equivalent to

$$y^2 - x^2 = 1, x, y \in \mathbb{N}, x \ne 0. \tag{2.3}$$

That is,

$$(y - x)(y + x) = 1, x, y \in \mathbb{N}, x \ne 0. \tag{2.4}$$

This is impossible. Therefore, this equation does not have any solution in $\mathbb{N}$. We can now prove our main result.

Proof of Theorem 1.1

Let $S = \{a, b, c, d\}$ be a Diophantine quadruple such that

$$ab + 1 = r_1^2, ac + 1 = r_2^2, ad + 1 = r_3^2, bc + 1 = r_4^2, bd + 1 = r_5^2, cd + 1 = r_6^2.$$

Let $S_1 = \{a_1, b_1, c_1, d_1\}$ be a Diophantine quadruple. Assume that

$$A_1(S) = \begin{pmatrix} 0 & 0 & 0 & 3 & 0 & 0 \\ 0 & 0 & b & 0 & 0 & 0 \\ 0 & a & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & b \\ 0 & 0 & 0 & 0 & a & 0 \end{pmatrix}, W_k(A_1(S)) = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & k \\ 0 & 0 & 0 & 0 & 3 & 0 & 0 & 0 \\ 0 & 0 & 0 & b & 0 & 0 & 0 & 0 \\ 0 & 0 & a & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & b & 0 \\ 0 & 0 & 0 & 0 & 0 & a & 0 & 0 \\ a_1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix},$$

$$A_2(S) = \begin{pmatrix} 0 & 0 & 0 & 8 & 0 & 0 \\ 0 & 0 & b & 0 & 0 & 0 \\ 0 & a & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & b \\ 0 & 0 & 0 & 0 & a & 0 \end{pmatrix}, W_k(A_2(S)) = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & k \\ 0 & 0 & 0 & 0 & 8 & 0 & 0 & 0 \\ 0 & 0 & 0 & b & 0 & 0 & 0 & 0 \\ 0 & 0 & a & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & b & 0 \\ 0 & 0 & 0 & 0 & 0 & a & 0 & 0 \\ a_1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix},$$

$$A_3(S) = \begin{pmatrix} 0 & 0 & 0 & 120 & 0 & 0 \\ 0 & 0 & b & 0 & 0 & 0 \\ 0 & a & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & b \\ 0 & 0 & 0 & 0 & a & 0 \end{pmatrix}, W_k(A_3(S)) = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & k \\ 0 & 0 & 0 & 0 & 120 & 0 & 0 & 0 \\ 0 & 0 & 0 & b & 0 & 0 & 0 & 0 \\ 0 & 0 & a & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & b & 0 \\ 0 & 0 & 0 & 0 & 0 & a & 0 & 0 \\ a_1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix},$$

$$A_4(S) = \begin{pmatrix} 0 & 0 & 0 & 3 & 0 & 0 \\ 0 & 0 & c & 0 & 0 & 0 \\ 0 & a & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & b \\ 0 & 0 & 0 & 0 & a & 0 \end{pmatrix}, W_k(A_4(S)) = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & k \\ 0 & 0 & 0 & 0 & 3 & 0 & 0 & 0 \\ 0 & 0 & 0 & c & 0 & 0 & 0 & 0 \\ 0 & 0 & a & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & b & 0 \\ 0 & 0 & 0 & 0 & 0 & a & 0 & 0 \\ a_1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix},$$

$$A_5(S) = \begin{pmatrix} 0 & 0 & 0 & 8 & 0 & 0 \\ 0 & 0 & c & 0 & 0 & 0 \\ 0 & a & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & b \\ 0 & 0 & 0 & 0 & a & 0 \end{pmatrix}, W_k(A_5(S)) = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & k \\ 0 & 0 & 0 & 0 & 8 & 0 & 0 & 0 \\ 0 & 0 & 0 & c & 0 & 0 & 0 & 0 \\ 0 & 0 & a & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & b & 0 \\ 0 & 0 & 0 & 0 & 0 & a & 0 & 0 \\ a_1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix},$$

$$A_6(S)=\begin{pmatrix}0&0&0&120&0&0\\0&0&c&0&0&0\\0&a&0&0&0&0\\1&0&0&0&0&0\\0&0&0&0&0&b\\0&0&0&0&a&0\end{pmatrix},W_k\left(A_6(S)\right)=\begin{pmatrix}0&0&0&0&0&0&0&k\\0&0&0&0&120&0&0&0\\0&0&0&c&0&0&0&0\\0&0&a&0&0&0&0&0\\0&1&0&0&0&0&0&0\\0&0&0&0&0&0&b&0\\0&0&0&0&0&a&0&0\\a_1&0&0&0&0&0&0&0\end{pmatrix},$$

$$A_7(S)=\begin{pmatrix}0&0&0&3&0&0\\0&0&c&0&0&0\\0&a&0&0&0&0\\1&0&0&0&0&0\\0&0&0&0&0&c\\0&0&0&0&a&0\end{pmatrix},W_k\left(A_7(S)\right)=\begin{pmatrix}0&0&0&0&0&0&0&k\\0&0&0&0&3&0&0&0\\0&0&0&c&0&0&0&0\\0&0&a&0&0&0&0&0\\0&1&0&0&0&0&0&0\\0&0&0&0&0&0&c&0\\0&0&0&0&0&a&0&0\\a_1&0&0&0&0&0&0&0\end{pmatrix},$$

$$A_8(S)=\begin{pmatrix}0&0&0&8&0&0\\0&0&c&0&0&0\\0&a&0&0&0&0\\1&0&0&0&0&0\\0&0&0&0&0&c\\0&0&0&0&a&0\end{pmatrix},W_k\left(A_8(S)\right)=\begin{pmatrix}0&0&0&0&0&0&0&k\\0&0&0&0&8&0&0&0\\0&0&0&c&0&0&0&0\\0&0&a&0&0&0&0&0\\0&1&0&0&0&0&0&0\\0&0&0&0&0&0&c&0\\0&0&0&0&0&a&0&0\\a_1&0&0&0&0&0&0&0\end{pmatrix},$$

$$A_9(S)=\begin{pmatrix}0&0&0&120&0&0\\0&0&d&0&0&0\\0&a&0&0&0&0\\1&0&0&0&0&0\\0&0&0&0&0&d\\0&0&0&0&a&0\end{pmatrix},W_k\left(A_9(S)\right)=\begin{pmatrix}0&0&0&0&0&0&0&k\\0&0&0&0&120&0&0&0\\0&0&0&d&0&0&0&0\\0&0&a&0&0&0&0&0\\0&1&0&0&0&0&0&0\\0&0&0&0&0&0&d&0\\0&0&0&0&0&a&0&0\\a_1&0&0&0&0&0&0&0\end{pmatrix},$$

$$A_{10}(S)=\begin{pmatrix}0&0&0&3&0&0\\0&0&c&0&0&0\\0&a&0&0&0&0\\1&0&0&0&0&0\\0&0&0&0&0&d\\0&0&0&0&a&0\end{pmatrix},W_k\left(A_{10}(S)\right)=\begin{pmatrix}0&0&0&0&0&0&0&k\\0&0&0&0&3&0&0&0\\0&0&0&c&0&0&0&0\\0&0&a&0&0&0&0&0\\0&1&0&0&0&0&0&0\\0&0&0&0&0&0&d&0\\0&0&0&0&0&a&0&0\\a_1&0&0&0&0&0&0&0\end{pmatrix},$$

$$A_{11}(S)=\begin{pmatrix}0&0&0&8&0&0\\0&0&c&0&0&0\\0&a&0&0&0&0\\1&0&0&0&0&0\\0&0&0&0&0&d\\0&0&0&0&a&0\end{pmatrix},W_k\left(A_{11}(S)\right)=\begin{pmatrix}0&0&0&0&0&0&0&k\\0&0&0&0&8&0&0&0\\0&0&0&c&0&0&0&0\\0&0&a&0&0&0&0&0\\0&1&0&0&0&0&0&0\\0&0&0&0&0&0&d&0\\0&0&0&0&0&a&0&0\\a_1&0&0&0&0&0&0&0\end{pmatrix},$$

$$A_{12}(S)=\begin{pmatrix}0&0&0&120&0&0\\0&0&c&0&0&0\\0&a&0&0&0&0\\1&0&0&0&0&0\\0&0&0&0&0&d\\0&0&0&0&a&0\end{pmatrix},W_k\left(A_{12}(S)\right)=\begin{pmatrix}0&0&0&0&0&0&0&k\\0&0&0&0&120&0&0&0\\0&0&0&c&0&0&0&0\\0&0&a&0&0&0&0&0\\0&1&0&0&0&0&0&0\\0&0&0&0&0&0&d&0\\0&0&0&0&0&a&0&0\\a_1&0&0&0&0&0&0&0\end{pmatrix},$$

$$A_{13}(S)=\begin{pmatrix}0&0&0&3&0&0\\0&0&d&0&0&0\\0&a&0&0&0&0\\1&0&0&0&0&0\\0&0&0&0&0&d\\0&0&0&0&a&0\end{pmatrix},W_k\left(A_{13}(S)\right)=\begin{pmatrix}0&0&0&0&0&0&0&k\\0&0&0&0&3&0&0&0\\0&0&0&d&0&0&0&0\\0&0&a&0&0&0&0&0\\0&1&0&0&0&0&0&0\\0&0&0&0&0&0&d&0\\0&0&0&0&0&a&0&0\\a_1&0&0&0&0&0&0&0\end{pmatrix},$$

$$A_{14}(S)=\begin{pmatrix}0&0&0&8&0&0\\0&0&d&0&0&0\\0&a&0&0&0&0\\1&0&0&0&0&0\\0&0&0&0&0&d\\0&0&0&0&a&0\end{pmatrix},W_k\left(A_{14}(S)\right)=\begin{pmatrix}0&0&0&0&0&0&0&k\\0&0&0&0&8&0&0&0\\0&0&0&d&0&0&0&0\\0&0&a&0&0&0&0&0\\0&1&0&0&0&0&0&0\\0&0&0&0&0&0&d&0\\0&0&0&0&0&a&0&0\\a_1&0&0&0&0&0&0&0\end{pmatrix},$$

$$A_{15}(S)=\begin{pmatrix}0&0&0&8&0&0\\0&0&d&0&0&0\\0&a&0&0&0&0\\1&0&0&0&0&0\\0&0&0&0&0&c\\0&0&0&0&a&0\end{pmatrix},W_k\left(A_{15}(S)\right)=\begin{pmatrix}0&0&0&0&0&0&0&k\\0&0&0&0&8&0&0&0\\0&0&0&d&0&0&0&0\\0&0&a&0&0&0&0&0\\0&1&0&0&0&0&0&0\\0&0&0&0&0&0&c&0\\0&0&0&0&0&a&0&0\\a_1&0&0&0&0&0&0&0\end{pmatrix},$$

$$A_{16}(S)=\begin{pmatrix}0&0&0&120&0&0\\0&0&d&0&0&0\\0&a&0&0&0&0\\1&0&0&0&0&0\\0&0&0&0&0&c\\0&0&0&0&a&0\end{pmatrix},W_k\left(A_{16}(S)\right)=\begin{pmatrix}0&0&0&0&0&0&0&k\\0&0&0&0&120&0&0&0\\0&0&0&d&0&0&0&0\\0&0&a&0&0&0&0&0\\0&1&0&0&0&0&0&0\\0&0&0&0&0&0&c&0\\0&0&0&0&0&a&0&0\\a_1&0&0&0&0&0&0&0\end{pmatrix},$$

$$A_{17}(S)=\begin{pmatrix}0&0&0&3&0&0\\0&0&d&0&0&0\\0&a&0&0&0&0\\1&0&0&0&0&0\\0&0&0&0&0&b\\0&0&0&0&a&0\end{pmatrix},W_k\left(A_{17}(S)\right)=\begin{pmatrix}0&0&0&0&0&0&0&k\\0&0&0&0&3&0&0&0\\0&0&0&d&0&0&0&0\\0&0&a&0&0&0&0&0\\0&1&0&0&0&0&0&0\\0&0&0&0&0&0&b&0\\0&0&0&0&0&a&0&0\\a_1&0&0&0&0&0&0&0\end{pmatrix},$$

$$A_{18}(S)=\begin{pmatrix}0&0&0&8&0&0\\0&0&d&0&0&0\\0&a&0&0&0&0\\1&0&0&0&0&0\\0&0&0&0&0&b\\0&0&0&0&a&0\end{pmatrix},W_k\left(A_{18}(S)\right)=\begin{pmatrix}0&0&0&0&0&0&0&k\\0&0&0&0&8&0&0&0\\0&0&0&d&0&0&0&0\\0&0&a&0&0&0&0&0\\0&1&0&0&0&0&0&0\\0&0&0&0&0&0&b&0\\0&0&0&0&0&a&0&0\\a_1&0&0&0&0&0&0&0\end{pmatrix},$$

$$A_{19}(S)=\begin{pmatrix}0&0&0&120&0&0\\0&0&d&0&0&0\\0&a&0&0&0&0\\1&0&0&0&0&0\\0&0&0&0&0&b\\0&0&0&0&a&0\end{pmatrix},W_k\left(A_{19}(S)\right)=\begin{pmatrix}0&0&0&0&0&0&0&k\\0&0&0&0&120&0&0&0\\0&0&0&d&0&0&0&0\\0&0&a&0&0&0&0&0\\0&1&0&0&0&0&0&0\\0&0&0&0&0&0&b&0\\0&0&0&0&0&a&0&0\\a_1&0&0&0&0&0&0&0\end{pmatrix},$$

$$A_{20}(S)=\begin{pmatrix}0&0&0&120&0&0\\0&0&c&0&0&0\\0&a&0&0&0&0\\1&0&0&0&0&0\\0&0&0&0&0&c\\0&0&0&0&a&0\end{pmatrix},W_k\left(A_{20}(S)\right)=\begin{pmatrix}0&0&0&0&0&0&0&k\\0&0&0&0&120&0&0&0\\0&0&0&c&0&0&0&0\\0&0&a&0&0&0&0&0\\0&1&0&0&0&0&0&0\\0&0&0&0&0&0&c&0\\0&0&0&0&0&a&0&0\\a_1&0&0&0&0&0&0&0\end{pmatrix},$$

with $k\in\{b_1,c_1,d_1\}$. The matrix $A_1(S)$ is embedded in the matrix $W_k\left(A_1(S)\right)$. The matrix $W_k\left(A_1(S)\right)$ is called the embedding of the matrix $A_1(S)$ of order 1. It was shown by Mouanda that the set of matrices G(S) define by

$$G(S)=\{A_1(S),A_2(S),A_3(S),A_4(S),A_5(S),\cdots,A_{20}(S)\}$$

is a matrix strong Diophantine 20-tuple [15]. We can construct matrix strong Diophantine m-tuples with $m\geq 20$. Let us consider the set

$$G(S,S_1)=\{W_k(A_1(S)),\cdots,W_k(A_{19}(S)),W_k(A_{20}(S)):k\in\{b_1,c_1,d_1\}\}.$$

This set has exactly 60 elements. It is straightforward to check that the set $G(S_1,S)$ is a matrix strong Diophantine 60-tuple, since the set $S_1=\{a_1,b_1,c_1,d_1\}$ is a strong Diophantine quadruple. From the structure of the matrices

$$A_1(S)=\begin{pmatrix}0&0&0&3&0&0\\0&0&b&0&0&0\\0&a&0&0&0&0\\1&0&0&0&0&0\\0&0&0&0&0&b\\0&0&0&0&a&0\end{pmatrix},W_k(A_1(S))=\begin{pmatrix}0&0&0&0&0&0&0&k\\0&0&0&0&3&0&0&0\\0&0&0&b&0&0&0&0\\0&0&a&0&0&0&0&0\\0&1&0&0&0&0&0&0\\0&0&0&0&0&0&b&0\\0&0&0&0&0&a&0&0\\a_1&0&0&0&0&0&0&0\end{pmatrix},$$

let us construct a new family of 10 × 10-matrices which is a matrix strong Diophantine 180 tuple. Let

$$S=\{a,b,c,d\},S_0=\{a_0,b_0,c_0,d_0\},S_1=\{a_1,b_1,c_1,d_1\},S_2=\{a_2,b_2,c_2,d_2\}$$

be four Diophantine quadruples. Assume that

$$H_1(S)=\begin{pmatrix}0&0&0&b_0&0&0\\0&0&b&0&0&0\\0&a&0&0&0&0\\a_0&0&0&0&0&0\\0&0&0&0&0&b\\0&0&0&0&a&0\end{pmatrix}$$

and

$$W_{(b_1,b_2)}(H_1(S))=\begin{pmatrix}0&0&0&0&0&0&0&0&0&b_2\\0&0&0&0&0&0&0&0&b_1&0\\0&0&0&0&0&b_0&0&0&0&0\\0&0&0&0&b&0&0&0&0&0\\0&0&0&a&0&0&0&0&0&0\\0&0&a_0&0&0&0&0&0&0&0\\0&0&0&0&0&0&0&b&0&0\\0&0&0&0&0&0&a&0&0&0\\0&a_1&0&0&0&0&0&0&0&0\\a_2&0&0&0&0&0&0&0&0&0\end{pmatrix}.$$

Let us look closely the structure of the matrix $H_1(S)$. We can notice that the entry of the row 1 and column 4 of the matrix $A_1(S)$, which is 3, is replaced by b_0 to get $H_1(S)$. If we replace the entry 8 by c_0 and the entry 120 by d_0 inside the matrices of the set

$$G(S)=\{A_1(S),A_2(S),A_3(S),A_4(S),A_5(S),\cdots,A_{20}(S)\},$$

we get a new set of 20 matrices denoted by

$$H(S)=\{H_1(S),H_2(S),H_3(S),H_4(S),H_5(S),\cdots,H_{20}(S)\}.$$

The set H(S) is a matrix strong Diophantine 20-tuple as well since the set S_0 is a Diophantine quadruple. Let us look the structure of the matrix $W_{(b_1,b_2)}(H_1(S))$. This matrix embeds the matrix $H_1(S)$. The matrix $W_{(b_1,b_2)}(H_1(S))$ is called the embedding of the matrix $H_1(S)$ of order 2. For a fixed pair (b_1,b_2) of the set $\{b_1,c_1,d_1\}\times\{b_2,c_2,d_2\}$, there are 20 embedding of the matrices of the set $H(S)$ which are the elements of the set

$$\{W_{(b_1,b_2)}(H_1(S)),\cdots,W_{(b_1,b_2)}(H_{20}(S))\}.$$

We know that there are exactly 9 pairs (k_1,k_2) of the set $\{b_1,c_1,d_1\}\}\times\{b_2,c_2,d_2\}$. In all, there exist 20 × 9 = 180 embeddings of the elements of H(S). Let us consider the set

$$G(S_0,S_1,S_2)=\{W_{(k_1,k_2)}(H_1(S)),\cdots,W_{(k_1,k_2)}(H_{20}(S)):(k_1,k_2)\in\{b_1,c_1,d_1\}\times\{b_2,c_2,d_2\}\}.$$

This set has exactly 180 elements. It is straightforward to check that the set $G(S_0,S_1,S_2)$ is a matrix strong Diophantine 180-tuple. It is possible to construct matrix strong Diophantine 540-tuples. Indeed, let $S_3=\{a_3,b_3,c_3,d_3\}$ be a Diophantine quadruple. Let us consider the matrix

$$W_{(b_1,b_2)}(H_1(S))=\begin{pmatrix}0&0&0&0&0&0&0&0&0&b_2\\0&0&0&0&0&0&0&0&b_1&0\\0&0&0&0&0&b_0&0&0&0&0\\0&0&0&0&b&0&0&0&0&0\\0&0&0&a&0&0&0&0&0&0\\0&0&a_0&0&0&0&0&0&0&0\\0&0&0&0&0&0&0&b&0&0\\0&0&0&0&0&0&a&0&0&0\\0&a_1&0&0&0&0&0&0&0&0\\a_2&0&0&0&0&0&0&0&0&0\end{pmatrix}.$$

Let (b_1,b_2,b_3) be a triple of the set $\{b_1,c_1,d_1\}\times\{b_2,c_2,d_2\}\times\{b_3,c_3,d_3\}$. The 12 × 12-matrix defined by

$$W_{(b_1,b_2,b_3)}(H_1(S))=\begin{pmatrix}0&0&0&0&0&0&0&0&0&0&0&b_3\\0&0&0&0&0&0&0&0&0&0&b_2&0\\0&0&0&0&0&0&0&0&0&b_1&0&0\\0&0&0&0&0&0&b_0&0&0&0&0&0\\0&0&0&0&0&b&0&0&0&0&0&0\\0&0&0&0&a&0&0&0&0&0&0&0\\0&0&0&a_0&0&0&0&0&0&0&0&0\\0&0&0&0&0&0&0&0&b&0&0&0\\0&0&0&0&0&0&0&a&0&0&0&0\\0&0&a_1&0&0&0&0&0&0&0&0&0\\0&a_2&0&0&0&0&0&0&0&0&0&0\\a_3&0&0&0&0&0&0&0&0&0&0&0\end{pmatrix}$$

is called the embedding of the matrix $W_{(b_1,b_2)}\left(H_1(S)\right)$ of order 1. In other words, the embedding of $H_1(S)$ of order 3. For a fixed triple (b_1,b_2,b_3) of the set $\{b_1,c_1,d_1\}\times\{b_2,c_2,d_2\}\times\{b_3,c_3,d_3\}$, the set $\left\{W_{(b_1,b_2,b_3)}\left(H_1(S)\right),\cdots,W_{(b_1,b_2,b_3)}\left(H_{19}(S)\right),W_{(b_1,b_2,b_3)}\left(H_{20}(S)\right)\right\}$ has exactly 180 matrices. Therefore, the set

$$G(S_0,S_1,S_2,S_3)=\left\{W_{(k_1,k_2,k_3)}\left(H_1(S)\right),\cdots,W_{(k_1,k_2,k_3)}\left(H_{20}(S)\right):(k_1,k_2,k_3)\in Q\right\}$$

with $Q=\{b_1,c_1,d_1\}\times\{b_2,c_2,d_2\}\times\{b_3,c_3,d_3\}$. The set $G(S_0,S_1,S_2,S_3)$ has exactly $20\times3\times3\times3=540$ elements. Due to the fact that the set $G(S_0,S_1,S_2)$ is a matrix strong Diophantine 180-tuple implies that the set $G(S_0,S_1,S_2,S_3)$ is a matrix strong Diophantine 540-tuple. Finally, there exists an infinite number of matrix strong Diophantine 540-tuples. □

The process of constructing $W_{b_1}\left(H_1(S)\right),W_{(b_1,b_2)}\left(H_1(S)\right),W_{(b_1,b_2,b_3)}\left(H_1(S)\right)$ is called the embedding process. The embedding process allows us to construct indefinitely matrix strong Diophantine m-tuples for $m\geq540$.

3. Construction of Matrix Elliptic Curves

It is possible to construct matrix elliptic curves from Diophantine quadruples. Indeed, let us construct a matrix elliptic curve from the elements of the set

$$G(S_0,S_1,S_2,S_3)=\left\{W_{(k_1,k_2,k_3)}\left(H_1(S)\right),\cdots,W_{(k_1,k_2,k_3)}\left(H_{20}(S)\right):(k_1,k_2,k_3)\in Q\right\}$$

with $Q=\{b_1,c_1,d_1\}\times\{b_2,c_2,d_2\}\times\{b_3,c_3,d_3\}$. Let us consider the elliptic curve

$$Y^2=\left(W_{(b_1,b_2,b_3)}\left(H_1(S)\right)X+I_{12}\right)\left(W_{(b_1,b_2,b_3)}\left(H_2(S)\right)X+I_{12}\right)\left(W_{(b_1,b_2,b_3)}\left(H_3(S)\right)X+I_{12}\right). \quad (3.1)$$

Every matrix of the set $G(S_0,S_1,S_2,S_3)$ allows the construction of a solution of the Equation (3.1). Therefore, this elliptic curve has 540 matrix solutions. Finally, there exists an infinite number of elliptic curves which have 540 matrix solutions in $M_{12}(\mathbb{N})$. To every matrix A of $G(S_0,S_1,S_2,S_3)$, we associate the elliptic curve

$$E_A:Y^2=\left(X^2+I_{12}\right)\left(AX+I_{12}\right).$$

This elliptic curve has 540 matrix solutions, $\left(X\in G(S_0,S_1,S_2,S_3)\right)$, in $M_{12}(\mathbb{N})$.

4. Construction of Matrix Hyperelliptic Curves

It is possible to construct a matrix hyperelliptic curve from the elements of the set $G(S_0,S_1,S_2,S_3)$. Let us consider the hyperelliptic curve

$$Y^2=\left(X^2+I_{12}\right)\left(W_\beta\left(H_1(S)\right)X+I_{12}\right)\left(W_\beta\left(H_2(S)\right)X+I_{12}\right)\left(W_\beta\left(H_3(S)\right)X+I_{12}\right), \quad (4.1)$$

$\beta=(b_1,b_2,b_3)$, of genus g = 2. The matrix solutions of this equation are generated from the elements of $G(S_0,S_1,S_2,S_3)$. Therefore, this equation has at least 540 solutions $\left(X\in G(S_0,S_1,S_2,S_3)\right)$ in $M_{12}(\mathbb{N})$.

Conflicts of Interest

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

References

[1] Bashmakova, I.G. (1974) 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] Baker, A. and Davenport, H. (1969) The Equations $3x^2-2=y^2$ and $8x^2-7=z^2$. *The Quarterly Journal of Mathematics*, **20**, 129-137. https://doi.org/10.1093/qmath/20.1.129

[4] 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

[5] 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

[6] 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, 71-75.

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

[8] 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

[9] 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

[10] Dujella, A. (1998) A Generalization of a Theorem of Baker and Davenport. *The Quarterly Journal of Mathematics*, **49**, 291-306. https://doi.org/10.1093/qjmath/49.195.291

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

[12] 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

[13] 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

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

[15] 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

[16] Barsagade, M.W. and Meshram, S. (2014) Overview of History of Elliptic Curves and Its Use in Cryptography. *International Journal of Scientific and Engineering Research*, **5**, 467-471.

[17] Mordell, L. (1926) The Integer Solutions of the Equation $y^2=ax^n+bx^{n-1}+\cdots+k$. *Journal of the London Mathematical Society*, **s1-1**, 66-68.