Mathematics and Systems Science 2024, 2(2), 2624.
https://doi.org/10.54517/mss.v2i2.2624

Article

On matrix strong Diophantine 27-Tuples and matrix elliptic curves

Joachim Moussounda Mouanda[1,*], Kouakou Kouassi Vincent[2]

[1] Mathematics Department, Blessington Christian University, Nkayi KIVIDI, Republic of Congo
[2] Applied Fondamentale Sciences Department, Nangui Abrogoua University, Abidjan 02 BP 801, Cote d'Ivoire
*** Corresponding author:** Joachim Moussounda Mouanda, mmoussounda@yahoo.fr

CITATION

Mouanda JM, Vincent KK. On matrix strong Diophantine 27-Tuples and matrix elliptic curves. Mathematics and Systems Science. 2024; 2(2): 2624. https://doi.org/10.54517/mss.v2i2.2624

ARTICLE INFO

Received: 14 March 2024
Accepted: 20 May 2024
Available online: 30 July 2024

Abstract: We introduce an algorithm which allows us to prove that there exists an infinite number of matrix strong Diophantine 27-tuples. We show that Diophantine quadruples generate matrix elliptic (or hyperelliptic) curves which have each 54 matrix points.

Keywords: Matrices of integers; Diophantine m-tuples; elliptic curves
Mathematics Subject Classification (2010): 15B36; 11D09; 11G05

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: $\{a, b, a+b+2r, 4r(r+a)(r+b)\}$, where $ab+1=r^2, a, b \in N$. In other words, every Diophantine pair can be extended to Diophantine quadruples. He was able to add the fifth positive rational $\frac{777480}{8288641}$ to Fermat's set [2]. In 1969, Baker and Davenport proved that it not possible to add a fifth positive integer to the Fermat's set [3]. The Fibonacci sequence $(F_k)_{k\geq 0}$ has several strong connections with the Diophantine quadruples. In 1977, Hoggatt and Bergum conjectured that the set $\{F_{2k}, F_{2k+2}, F_{2k+4}, 4F_{2k+1}F_{2k+2}F_{2k+3}\}$ is a Diophantine quadruple [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 $\{2; 4; 12\}$ to a Diophantine quadruple [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 1998, it was proved that the sets $\{k-1, k+1, 4k\}$ can be extended respectively to a Diophantine quadruple [8]. In 1998, Dujella and Petho proved that the pair $\{1,3\}$ cannot be extended to a Diophantine quintuple [9]. 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 [10]. In 2008, Fujita proved that for $k \geq 2$, the Diophantine pair $\{k-1, k+1\}$ cannot be extended to a Diophantine quintuple [11]. 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 [12]. In 2019, He, Togbé and Ziegle proved that Diophantine quintuples do not exist [13]. A set of m nonzero positive rational numbers $\{a_1, a_2, \dots, a_m\}$ is called a strong Diophantine m-tuple if $a_i a_j + 1$ is a perfect square for all $i, j = 1,2, \dots, m$. It is quiet clear that there does not exist a strong Diophantine pair consisting of integers. However, in 2008, Dujella and Petričcević proved that there exist infinitely many strong Diophantine triples of positive rational numbers and it is not known whether there exist any strong Diophantine quadruples [14].

In this paper, from Diophantine quadruples, we construct matrix strong Diophantine 27-tuples.

Theorem 1. *There exists an infinite number of matrix strong Diophantine* 27*-tuples.*

We show that Diophantine quadruples generate matrix elliptic (or hyperelliptic) curves which have each 54 matrix points.

2. Preliminaries

Let

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

be the set of n-by-n complex matrices.

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

Definition 2. *A set of* m *positive rational numbers* $\{a_1, a_2, \dots, a_m\}$ *is called a rational Diophantine* m*-tuple if* $a_i a_j + 1$ *is a rational square for all* $1 \le i < j \le m$.

Let us introduce the matrix version of the above definitions.

Definition 3. *A set of* m *matrices with positive integers as entries* $\{A_1, A_2, \dots, A_m\}$, $A_i \in M_n(N)$, *is called a matrix Diophantine* m*-tuple if* $A_i A_j + I_n$ *are matrix squares, with positive integers as entries, for all* $i \neq j$.

Definition 4. *A set of* m *matrices with positive rational numbers as entries* $\{A_1, A_2, \dots, A_m\}$, $A_i \in M_n(Q)$, *is called a rational matrix Diophantine mtuple* $A_i A_j + I_n$ *are rational matrix squares, with positive rational numbers as entries, for all* $i \neq j$. *Let* $S = \{a_1, a_2, \dots, a_m\}$ *be a Diophantine tuple. Consider the elliptic curve* $y^2 = (a_1 x + 1)(a_2 x + 1)(a_3 x + 1)$.

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

Theorem 2. *The number of integers points on the elliptic curve* $y^2 = x^3 + ax + b$ *is finite [15].*

This result allows us to claim that the number of elements of the set S is finite. In 2019, He et al. [13] proved the following conjecture.

Conjecture 1. *There does not exist a Diophantine quintuple.*

This conjecture is not true at all for Diophantine m-tuples over the set of matrices $M_n(N)$.

Definition 5. *A set of m positive integers $\{a_4, a_5, \dots, a_m\}$ is called a strong Diophantine m-tuple if $a_i a_j + 1$ is a perfect square for all $1 \le i < j \le m$. This definition includes the case $a_i^2 + 1$ is a perfect square for all i.*

Definition 6. *A set of m positive rational numbers $\{a_4, a_5, \dots, a_m\}$is called a rational strong Diophantine m-tuple if $a_i a_j + 1$ is a rational squares for all $1 \le i < j \le m$.*

3. Proof of the main result

In this section, we show that Diophantine quadruples generate matrix strong Diophantine 27-tuples. Let us introduce the matrix version of the definition of a strong Diophantine m-tuple.

Definition 7. *A set of m matrices with positive integers as entries*

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

is called a matrix strong Diophantine m-tuple if $A_i A_j + I_n$ are matrix squares, with positive integers as entries, for all i and j.

Definition 8. *A set of m matrices with positive rational numbers as entries*

$$\{A_1, A_2, \dots, A_m\} \subset M_n(Q),$$

is called a rational matrix strong Diophantine m-tuple if $A_i A_j + I_n$ are rational matrix squares, with positive rational numbers as entries, for all i and j.

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

First of all, let us observe that the set $S = \{a_4, a_5, \dots, a_m\}$ is a strong Diophantine m tuple if the set S is a Diophantine mtuple and $a_i^2 + 1$ is a perfect square for all $1 \le i \le m$. Finding strong Diophantine mtuples is equivalent of solving the equation

$$x^2 + 1 = y^2, x, y \in N. \quad (1)$$

The structures of Pythagorean triples allow us to claim that this Equation (1) does not have any solution in N at all. Therefore, there does not exist any strong Diophantine pair of positive integers. This means that there does not exist any diagonal matrix strong Diophantine pair. In other words, if $A \in M_n(N)$, is a diagonal matrix with positive integers cœfficients, then the matrix $A^2 + I_n$ cannot be written as a matrix square with positive integers as entries. Therefore, matrix strong Diophantine m-tuples cannot be made of diagonal matrices. We can now prove our main result.

Proof of Theorem 1. Let $S = \{a, b, c, d\}$ be a Diophantine quadruple such that $ab + 1 = r_1^2, ac + 1 = r_2^2, ad + 1 = r_3^2$. Suppose that

$$A_\alpha(x, y, z) = \begin{pmatrix} 0 & 0 & 0 & z & 0 & 0 \\ 0 & 0 & x & 0 & 0 & 0 \\ 0 & a & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & y \\ 0 & 0 & 0 & 0 & a & 0 \end{pmatrix}$$

Let $Q_a(b, c, d) = \{b, c, d\} \times \{b, c, d\} \times \{3,8,120\}$ be the set of triples of positive integers. The set $Q_a(b, c, d)$ has exactly 27 elements. Let $G_a(S)$ be the set of matrices defined by $G_a(S) = \{A_\alpha(x, y, z): (x, y, z) \in Q_a(b, c, d)\}$.

The set $G_a(S)$ has exactly 27 matrices. A simple calculation shows that

$$A_a(x,y,z)A_a(x',y',z') + I_6 = \begin{pmatrix} z'+1 & 0 & 0 & 0 & 0 & 0 \\ 0 & ax'+1 & 0 & 0 & 0 & 0 \\ 0 & 0 & ax'+1 & 0 & 0 & 0 \\ 0 & 0 & 0 & z'+1 & 0 & 0 \\ 0 & 0 & 0 & 0 & ay'+1 & 0 \\ 0 & 0 & 0 & 0 & 0 & ay'+1 \end{pmatrix}$$

$$A_a(x',y',z')A_a(x,y,z) + I_6 = \begin{pmatrix} z+1 & 0 & 0 & 0 & 0 & 0 \\ 0 & ax+1 & 0 & 0 & 0 & 0 \\ 0 & 0 & ax+1 & 0 & 0 & 0 \\ 0 & 0 & 0 & z+1 & 0 & 0 \\ 0 & 0 & 0 & 0 & ay+1 & 0 \\ 0 & 0 & 0 & 0 & 0 & ay+1 \end{pmatrix}$$

and

$$A_a(x,y,z)^2 + I_6 = \begin{pmatrix} z+1 & 0 & 0 & 0 & 0 & 0 \\ 0 & ax+1 & 0 & 0 & 0 & 0 \\ 0 & 0 & ax+1 & 0 & 0 & 0 \\ 0 & 0 & 0 & z+1 & 0 & 0 \\ 0 & 0 & 0 & 0 & ay+1 & 0 \\ 0 & 0 & 0 & 0 & 0 & ay+1 \end{pmatrix}$$

for all $(x,y,z),(x',y',z') \in Q_a(b,c,d)$.

We can say that the matrices $A_a(x,y,z)A_a(x',y',z') + I_6$ are matrix squares for all $(x,y,z),(x',y',z') \in Q_a(b,c,d)$, since $ab+1 = r_1^2, ac+1 = r_2^2, ad+1 = r_3^2$.

Therefore, the set $G_a(S) = \{A_\alpha(x,y,z): (x,y,z) \in Q_a(b,c,d)\}$, is a matrix strong Diophantine 27-tuple. Finally, there exists an infinite number of matrix strong Diophantine 27-tuples. □

Every Diophantine pair generates a matrix strong Diophantine 27-tuple. Indeed, let $\{a,b\}$ be two positive integers such $ab+1 = r^2, r \in N$. Euler's result allows us to claim that the set $S(a,b) = \{a,b,a+b+2r,4r(r+a)(r+b)\}$ is a Diophantine quadruple [2]. Our main result allows us to claim that the associated set $G_a(S) = \{A_\alpha(x,y,z): (x,y,z) \in Q_a(b,c,d)\}$, is a matrix strong Diophantine 27-tuple.

4. Construction of matrix elliptic curves

It is well know that elliptic curves can be constructed from Diophantine quadruples [10]. Let $S = \{a,b,c,d\}$ be a Diophantine quadruple. It is possible to construct a matrix elliptic curve from the elements of the set $G_a(S) = \{A_\alpha(x,y,z): (x,y,z) \in Q_a(b,c,d)\}$.

Let $A_1(S), A_2(S), A_3(S)$be elements of the set $G_a(S)$. Let us consider the matrix elliptic curve:

$$E: Y^2 = (A_1(S) + I_6)(A_2(S)X + I_6)(A_3(S)X + I_6), X \in G_a(S) \quad (2)$$

Every matrix of the set $G_a(S)$ allows the construction of a solution of the Equation (2). Therefore, the matrix elliptic curve E has 54 matrix points in $M_6(N) \times M_6(N)$. Finally, there exists an infinite number of matrix elliptic curves which have 54 matrix points in $M_6(N) \times M_6(N)$. To every matrix A of $G_a(S)$, we associate the matrix elliptic curve $E_A: Y^2 = (X^2 + I_6)(AX + I_6)$.

The matrix elliptic curve E_A has 54 matrix points in $M_6(N) \times M_6(N), X \in G_a(S)$.

5. Construction of matrix hyperelliptic curves

Let $S = \{a, b, c, d\}$ be a Diophantine quadruple. It is possible to construct a matrix hyperelliptic curve from the elements of the set $G_a(S)$. Let us consider the matrix hyperelliptic curve

$$E_1: Y^2 = (X^2 + I_6)(A_1(S)X + I_6)(A_2(S)X + I_6)(A_3(S)X + I_6), X \in G_a(S) \quad (3)$$

of genus $g = 2$. This equation has exactly 54 solutions $X, A_i \in G_a(S)$.

Therefore, the matrix hyperelliptic curve E_1 has 54 matrix points in $M_6(N) \times M_6(N)$.

Author contributions: Conceptualization, JMM and KKV; methodology, JMM; software, JMM; validation, JMM, KKV; formal analysis, JMM; investigation, JMM; resources, JMM; data curation, JMM; writing—original draft preparation, JMM; writing—review and editing, JMM; visualization, JMM; supervision, JMM; project administration, JMM; funding acquisition, JMM, KKV. All authors have read and agreed to the published version of the manuscript.

Conflict of interest: The authors declare no conflict of interest.

References

1. Bashmakova IG. Diophantus of Alexandria, Arithmetics and the Book of Polygonal Numbers. Moscow: Nauka; 1974.
2. Euler L. Theorematum quorundam arithmeticorum demonstrationes. Novi Commentarii academiae scientiarum Petropolitanae. 1738; 10: 125-146.
3. Baker A, Davenport H. The equations $3x^2 - 2 = y^2$ and $8x^2 - 7 = z^2$. The Quarterly Journal of Mathematics. 1969; 20(1): 129-137. doi: 10.1093/qmath/20.1.129
4. Hoggatt VE, Bergum GE. A problem of Fermat and the Fibonacci sequence, Fibonacci Quart. Available online: https://www.mathstat.dal.ca/FQ/Scanned/15-4/hoggatt1.pdf (accessed on 7 March 2024).
5. Joseph A, Jr Hoggatt VE, Straus EG. On Euler's solution of a problem of Diophantus. Fibonacci Quarterly. 1979; 17(4): 333339.
6. Veluppillai M. A Collection of Manuscripts Related to the Fibonacci sequence, The Fibonacci Association. Santa Clara; 1980. pp. 71-75.
7. Kedlaya K. Solving constrained Pell equations. Mathematics of Computation. 1998; 67(222): 833-842. doi: 10.1090/s0025-5718-98-00918-1
8. Dujella A. The problem of the extension of a parametric family of Diophantine triples. Publicationes Mathematicae Debrecen. 1997; 51(3-4): 311-322. doi: 10.5486/pmd.1997.1886
9. Dujella A, Petho A. A Generalization of a Theorem of Baker and Davenport. The Quarterly Journal of Mathematics. 1998; 49(3): 291-306. doi: 10.1093/qmathj/49.3.291
10. Dujella A. A proof of the Hoggatt-Bergum conjecture. Proceedings of the American Mathematical Society. 1999; 127(7): 1999-2005. doi: 10.1090/s0002-9939-99-04875-3
11. Fujita Y. The extensibility of Diophantine pairs{k−1,k+1}. Journal of Number Theory. 2008; 128(2): 322-353. doi: 10.1016/j.jnt.2007.03.013
12. Dujella A. There are only finitely many Diophantine quintuples. Journal für die reine und angewandte Mathematik (Crelles Journal). 2004; 2004(566). doi: 10.1515/crll.2004.003
13. He B, Togbé A, Ziegler V. There is no Diophantine Quintuple.Transactions of the American Mathematical Society. arXiv. 2019; arXiv:1610.04020.
14. Dujella A, Petričcević V. Strong Diophantine Triples. Experimental Mathematics. 2008; 17(1): 83-89. doi: 10.1080/10586458.2008.10129020
15. Siegel CL. The integer solutions of the equation $y^2 = ax^n + bx^{n-1} + \cdots + k$. Journal of the London Mathematical Society. 1926.