Provided for non-commercial research and educational use.
Not for reproduction, distribution or commercial use.

Serdica
Mathematical Journal
Сердика
Математическо списание

The attached copy is furnished for non-commercial research and education use only.
Authors are permitted to post this version of the article to their personal websites or institutional repositories and to share with other researchers in the form of electronic reprints.
Other uses, including reproduction and distribution, or selling or licensing copies, or posting to third party websites are prohibited.

For further information on
Serdica Mathematical Journal
which is the new series of
Serdica Bulgaricae Mathematicae Publicationes
visit the website of the journal http://serdica.math.bas.bg
or contact: Editorial Office
Serdica Mathematical Journal
Institute of Mathematics and Informatics
Bulgarian Academy of Sciences
Telephone: (+359-2)9792818, FAX:(+359-2)971-36-49
e-mail: serdica@math.bas.bg

Serdica Math. J. **51** (2025), 189–196

Serdica
Mathematical Journal

Bulgarian Academy of Sciences
Institute of Mathematics and Informatics

A RECIPE ON THE CONSTRUCTION OF MATRICES SATISFYING $X^k + Y^k = Z^k$ OVER $M_n(\mathbb{Z})$

Kuldeep Sarma

Communicated by V. Drensky

Abstract. In this note, we provide a recipe for the construction of matrices satisfying Fermat's matrix equation over $M_n(\mathbb{Z})$.

1. Introduction. Pierre de Fermat in 1637, mentioned that for any integer k greater than 2, there exists no positive integers x, y, z satisfying the equation

$$x^k + y^k = z^k. \tag{1}$$

Since then, Fermat's last theorem had become a conjecture. Andrew Wiles first [15] confirmed that the conjecture is indeed true. Currently, Fermat's last theorem has been extended over some number fields [6]. In contrast to the classical Fermat's last theorem in integers, one can define the Fermat's matrix equation as $X^k + Y^k = Z^k$ where $X, Y, Z \in M_n(\mathbb{Z})$ and $k(\geq 2) \in \mathbb{N}$. Many researchers have studied the Fermat's matrix equation. For example, the Fermat's matrix equation has been well investigated in rational matrices [9], some classes of 2×2

https://doi.org/10.55630/serdica.2025.51.189-196

2020 *Mathematics Subject Classification:* 15B33, 15A24, 11D41.
Key words: matrix equation, Fermat equation.

matrices [4], general linear group $GL_2(\mathbb{Z})$ of integral 2×2 matrices with det $= \pm 1$ [14] and special linear group $SL_2(\mathbb{Z})$ of integral 2×2 matrices with det $= 1$ [10]. In [5], the author discussed the Fermat's matrix equation for $k = 4$ in the set of 2×2 integer matrices. In [3], Brenner and Jacobson considered the Fermat's matrix equation for arbitrary k in the set of 2×2 integer matrices. Till now, a significant amount of work related to solvability of Fermat's equation in matrices has been done by the researchers up to 2×2 matrices. In [2], the author studied the Fermat's matrix equation for $k = 2n$ (for even indices) in the set of arbitrary $n \times n$ integer matrices. Author proved that there exists nonsingular matrices $A, B, C \in M_n(\mathbb{Z})$ such that $A^{2n} + B^{2n} = C^{2n}$. In the same article, author remarks that he suspects that no solution exist when $k = 3$ and $n = 2$. In [7], the author showed that solutions do exist in this case too and more generally solutions exist if k is any positive odd integer and either $n \geq k$ or n is even. Till now, a significant amount of work related to solvability of Fermat's matrix equation has been done by the researchers, see in [4, 8, 9, 10, 11, 13] and the references therein. But a complete characterization of matrices satisfying Fermat's matrix equation is still open and indeed a challenging one. Therefore, instead of seeking a complete characterization of such matrices, we put an another question: *Can one provide a recipe on the construction of matrices satisfying Fermat's matrix equation over $M_n(\mathbb{Z})$?* We answer this in Theorem 3 of our article.

Before we proceed further, first we explain few notations.

Let s, t be two given noncommuting variables. Then any finite formal product of nonnegative powers of s and t given by

$$\omega(s,t) = s^{m_1}t^{n_1}s^{m_2}t^{n_2}\dots s^{m_k}t^{n_k}, \quad m_1, n_1, \dots, m_k, n_k \geq 0$$

is called a *word* in s and t. The *length* of the word $\omega(s,t)$ is the nonnegative integer $m_1 + n_1 + m_2 + n_2 + \cdots + m_k + n_k$, that is, the sum of all the exponents in the word. Let $p(s,t)$ be a polynomial in two noncommuting variables, that is, any linear combination of words in two noncommuting variables. For example, if s, t are two given noncommuting variables as discussed above, then $p(s,t) = s^3 + s^2t + t^2s + t^3 + sts + st^2 + ts^2 + tst$ is a polynomial in the noncommuting variables s and t where $s^3, s^2t, t^2s, \dots, tst$ are the respective words (of length 3) of the polynomial.

Note that for any square matrices U and V, the following identity holds.

$$(U+V)^k = U^k + V^k + p(U,V), \tag{2}$$

where $p(U,V)$ is a matrix polynomial in the noncommuting variables U and V and $k(\geq 2) \in \mathbb{N}$. For example if $k = 3$, one can see that $p(U,V) = UVU + VU^2 + V^2U + U^2V + UV^2 + VUV$.

2. Main result. The following lemma is crucial for further development. By $\mathbb{Z}^n$, we mean the cartesian product $\mathbb{Z} \times \mathbb{Z} \times \cdots \times \mathbb{Z}$ of n copies of $\mathbb{Z}$.

Lemma 1. *Let $x, y, u, v \in \mathbb{Z}^n$ be any four column vectors. Then there exists a nonzero matrix $A \in M_n(\mathbb{Q})$ such that $Ax = u$ and $A^\top y = v$ if and only if* $\operatorname{rank}(\mathbf{A}) = \operatorname{rank}(\mathbf{A} \mid \mathbf{v})$, *where*

$$\mathbf{A} = \begin{pmatrix} e_1 x^\top & e_2 x^\top & \cdots & e_n x^\top \\ y_1 I_n & y_2 I_n & \cdots & y_n I_n \end{pmatrix},$$

$\mathbf{v} = [u, v]^\top$ *and e_i's are standard basis of $\mathbb{R}^n$.*

P r o o f. Let $x = [x_1, x_2, \ldots, x_n]^\top$, $y = [y_1, y_2, \ldots, y_n]^\top$, $u = [u_1, u_2, \ldots, u_n]^\top$ and $v = [v_1, v_2, \ldots, v_n]^\top$ be any four column vectors in $\mathbb{Z}^n$. First assume that there exists a nonzero matrix $A = [a_{ij}] \in M_n(\mathbb{Q})$ such that $Ax = u$ and $A^\top y = v$. Thus we have the following two system of equations.

$$\begin{aligned} &\sum_{i=1}^{n} a_{1i}x_i = u_1 && && \sum_{i=1}^{n} a_{i1}y_i = v_1 \\ &\sum_{i=1}^{n} a_{2i}x_i = u_2 && \text{and} && \sum_{i=1}^{n} a_{i2}y_i = v_2 \\ &\quad\vdots \qquad \vdots && && \quad\vdots \qquad \vdots \\ &\sum_{i=1}^{n} a_{ni}x_i = u_n && && \sum_{i=1}^{n} a_{in}y_i = v_n. \end{aligned}$$

Note that, the above two system is equivalent to the matrix equation

$$\mathbf{A}\mathbf{a_0} = \mathbf{v}, \tag{3}$$

where

$$\mathbf{A} = \begin{pmatrix} e_1 x^\top & e_2 x^\top & \cdots & e_n x^\top \\ y_1 I_n & y_2 I_n & \cdots & y_n I_n \end{pmatrix},$$

$\mathbf{a_0} = [a_{11}, a_{12} \ldots a_{1n}, a_{21}, a_{22} \ldots a_{2n}, \ldots, a_{n1}, a_{n2}, \ldots, a_{nn}]^\top$ and $\mathbf{v} = [u\ v]^\top$.

Hence we have $\operatorname{rank}(\mathbf{A}) = \operatorname{rank}(\mathbf{A} \mid \mathbf{v})$ in equation (3).

Conversely assume that $\operatorname{rank}(\mathbf{A}) = \operatorname{rank}(\mathbf{A} \mid \mathbf{v})$ where $\mathbf{A}$ and $\mathbf{v}$ are defined as above and $\mathbf{A}$ is a $2n \times n^2$ matrix. So there always exists a nonzero vector say, $\mathbf{b_0} = [b_{11}, b_{12}, \ldots b_{1n}, b_{21}, b_{22}, \ldots, b_{2n}, \ldots, b_{n1}, , b_{n2}, \ldots, b_{nn}]^\top \in \mathbb{Q}^{n^2}$ such that

$$\mathbf{A}\mathbf{b_0} = \mathbf{v}. \tag{4}$$

Now using $\mathbf{b_0}$, we construct $A = \begin{pmatrix} b_{11} & b_{12} & \cdots & b_{1n} \\ b_{21} & b_{22} & \cdots & b_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ b_{n1} & b_{n2} & \cdots & b_{nn} \end{pmatrix}$. Note that $A \in M_n(\mathbb{Q})$ and is nonzero. Then from equation (4), it follows that $Ax = u$ and $A^\top y = v$. □

The following corollary is an immediate consequence of Lemma 1.

Corollary 2. *Let $x, y \in \mathbb{Z}^n$ be two column vectors. Then there always exists a nonzero matrix $A \in M_n(\mathbb{Z})$ such that $Ax = 0$ and $y^\top A = 0$. Here* $\operatorname{rank}(A) \in \{1, 2, \ldots, n-1\}$.

We now present our main result of this article which provides a recipe for constructing three matrices satisfying Fermat's matrix equation over $M_n(\mathbb{Z})$ for any index $k \geq 2$.

Theorem 3. *For any two column vectors in $\mathbb{Z}^n$, there exist matrices $U, V \in M_n(\mathbb{Z})$ such that $(U+V)^k = U^k + V^k$ for all $k(\geq 2) \in \mathbb{N}$. In particular, $(U, V, U+V)$ forms a solution to the Fermat's matrix equation $X^k + Y^k = Z^k$.*

Proof. Let $x, y \in \mathbb{Z}^n$ be two given column vectors. By Corollary 2, there exists a nonzero matrix $U \in M_n(\mathbb{Z})$ such that $Ux = 0$ and $y^\top U = 0$. Let $V = xy^\top$. Note that $V \in M_n(\mathbb{Z})$. Using V in Equation 2, we get

$$(U+V)^k - U^k - V^k = p(U, xy^\top). \tag{5}$$

Observe that $p(U, V)$ is a linear combination of words of the form

$$\omega(U, V) = U^{m_1} V^{n_1} U^{m_2} V^{n_2} \cdots U^{m_k} V^{n_k}.$$

Now for $V = xy^\top$, consider the following

$$\omega(U, xy^\top) = U^{m_1} (xy^\top)^{n_1} U^{m_2} (xy^\top)^{n_2} \cdots U^{m_k} (xy^\top)^{n_k}.$$

Since $Ux = 0$ and $y^\top U = 0$, it follows that $\omega(U, xy^\top) = 0$. This implies that $p(U, V) = p(U, xy^\top) = 0$. Then from Equation 5, we have

$$(U+V)^k = U^k + V^k.$$

Thus one can choose $X = U, Y = V$ and $Z = U + V$ so that $X^k + Y^k = Z^k$. The proof is complete. □

Remark 1. Choosing the two column vectors suitably in Theorem 3 and using Corollary 2, one can construct X and Z in such a way that $\operatorname{rank}(X) = n-1$ and $\operatorname{rank}(Z) = n$. So starting with a rank one matrix, our recipe provides a way to construct one non singular matrix of rank n and one singular matrix with rank $n-1$.

Below we illustrate Theorem 3 with an example for 3×3 matrices with $k = 3$.

Example 4. Choose any two column vector in $\mathbb{Z}^3$, say $x = (1, 1, -1)^\top$ and $y = (1, 2, -1)^\top$. By Corollary 2, there exists a nonzero matrix $U \in M_3(\mathbb{Z})$ such that $Ux = 0$ and $y^\top U = 0$. For example, one can choose $U = \begin{pmatrix} 7 & -3 & 4 \\ -3 & 2 & -1 \\ 1 & 1 & 2 \end{pmatrix}$. Then $V = xy^\top = \begin{pmatrix} 1 & 2 & -1 \\ 1 & 2 & -1 \\ -1 & -2 & 1 \end{pmatrix}$ and $U + V = \begin{pmatrix} 8 & -1 & 3 \\ -2 & 4 & -2 \\ 0 & -1 & 3 \end{pmatrix}$. Note that $\operatorname{rank}(U) = 2, \operatorname{rank}(V) = 1$ and $\operatorname{rank}(U + V) = 3$.

Now choosing $X = U, Y = V$ and $Z = U + V$, we see that $X^3 + Y^3 = Z^3$.

3. Some application. In this section, we discuss various application of Theorem 3. We give a parametric solution of certain well-known matrix Diophantine equation whose corresponding scalar Diophantine equation has only trivial solution in some sense. We consider the following well-known scalar Diophantine equations in our article.

1. [1] As a direct consequence of Theorem 3, for $k = 2$, we get a parametric solution of the well known matrix Pythagorean equation $X^2 + Y^2 = Z^2$. Note that the solutions obtained via our parametric form are different from one obtained by Arnold and Eydelzon. Thus for $k = 2$, Theorem 3 provides us a new class of matrix Pythagorean triple.

2. [12, Chapter 4, Theorem 1] The scalar equation $x^4 + y^4 = z^2$ has no integer solutions with $xy \neq 0$ (and so no rational solutions with $xy \neq 0$).

   We now consider the corresponding matrix Diophantine equation $X^4 + Y^4 = Z^2$ where $X, Y, Z \in M_n(\mathbb{Z})$. Consider $k = 4$ in Theorem 3. We have $(U + V)^4 = U^4 + V^4$. Now choose $X = U, Y = V$ and $Z = (U + V)^2$. We see that $X^4 + Y^4 = Z^2$. Thus the corresponding matrix analogue of the scalar equation $x^4 + y^4 = z^2$ has infinitely many solution.

3. [12, Chapter 4, Theorem 2] The scalar equation $x^4 - y^4 = z^2$, $(x, y) = 1$ has no integer solutions except $x^2 = y^2 = 1$ and $x^2 = 1, y = 0$.

   Now choose $k = 4$ in Theorem 3. We have $(U + V)^4 = U^4 + V^4$. Finally, taking $X = U + V, Y = U$ and $Z = V^2$, we see that $X^4 - Y^4 = Z^2$. Thus the corresponding matrix Diophantine equation has infinitely many solution.

4. [12, Chapter 4, Corollary 6] The only integer solutions of $x^4+6x^2y^2+y^4 = z^2$ where $(x, y) = 1$ are given by $x^2 = 1, y = 0$ and $x = 0, y^2 = 1$.

   Choose $k = 4$ in Theorem (3). We have $(U+V)^4 = U^4+V^4$. Now choosing $X = U, Y = V$ and $Z = (U + V)^2$ and using Remark 1, it follows that the corresponding matrix Diophantine equation $X^4 + 6X^2Y^2 + Y^4 = Z^2$ has infinitely many solutions. This same parametrization also works for the matrix Diophantine equation $X^4 - 6X^2Y^2 + Y^4 = Z^2$ whose corresponding scalar equation $x^4 - 6x^2y^2 + y^4 = z^2$ where $(x, y) = 1$ has only integer solution $x = 0$ or $y = 0$.

5. [12, Chapter 10, Example 1] The scalar equation $x^3 + y^3 + z^3 - xyz = 0$ has only solution $x + y = 0, z = 0$.

   Choose $k = 3$ in Theorem 3. Then we have $(U + V)^3 = U^3 + V^3$. Now choosing $X = U, Y = V$ and $Z = -(U + V)$ and using Remark 1, we see that $X^3 + Y^3 + Z^3 - XYZ = 0$ which proves that the corresponding matrix Diophantine equation has infinitely many solution. Using this same parametrization, we can show that although the scalar equation $x^3 + y^3 + z^3 = 0$ has no integer solution except those given by $xyz = 0$, it's matrix analogue has infinitely many solution.

6. [12, Chapter 4, Equation 7′] The only integer solutions of $x^4+x^2y^2+y^4 = z^2$ where $(x, y) = 1$ are given by $x^2 = 1, y = 0$ and $x = 0, y^2 = 1$.

   Choose $k = 4$ in Theorem 3. We have $(U + V)^4 = U^4 + V^4$. Now using Remark 1 and choosing $X = U, Y = V$ and $Z = (U + V)^2$ in the corresponding matrix Diophantine equation $X^4+6X^2Y^2+Y^4 = Z^2$, we see that it has infinitely many solutions. This same parametrization also works for the matrix Diophantine equation $X^4 - X^2Y^2 + Y^4 = Z^2$ whose corresponding scalar equation $x^4 - x^2y^2 + y^4 = z^2$ where $(x, y) = 1$ has only integer solutions namely $x^2 = 1, y = 0$ and $x = 0, y^2 = 1$ and $x^2 = y^2 = 1$.

   The following three results are not directly related to Theorem 3 but we discuss them in our present context.

7. [12, Chapter 4, Corollary 3] The scalar equation $y^2 = x^4 + 1$ has only the rational solutions $x = 0, y = \pm 1$.

   We show that the corresponding matrix Diophantine equation $Y^2 = X^4+I$ has infinitely many solution. We have $XX^3 = X^4 = Y^2-I = (Y+I)(Y-I)$. So we would like X to be such that $X = Y+I$ and $X^3 = Y-I$, which gives $(Y + I)^3 = Y - I \implies Y^3 + 3Y^2 + 2Y + 2I = 0$. Therefore we may choose

any matrix Y with minimal polynomial $y^3 + 3y^2 + 2y + 2$ and $X = Y + I$. For $n = 2$, let $Y_2 = \begin{pmatrix} 0 & 1 \\ 2 & 0 \end{pmatrix}$, $X_2 = I_2$. We see that $Y_2^2 = X_2^4 + I_2$ and for $n = 3$, let $Y_3 = \begin{pmatrix} 0 & 0 & -2 \\ 1 & 0 & -2 \\ 0 & 1 & -3 \end{pmatrix}$ and $X_3 = \begin{pmatrix} 1 & 0 & -2 \\ 1 & 1 & -2 \\ 0 & 1 & -2 \end{pmatrix}$ and see that $Y_3^2 = X_3^4 + I_3$. For $n > 3$, we construct two block diagonal matrix X and Y where the main diagonal blocks of X are consists of X_2 and X_3 while main diagonal blocks of Y are consists of Y_2 and Y_3. Now since any matrix similar to Y have same minimal polynomial, it follows that the matrix equation $Y^2 = X^4 + I$ has infinitely many solutions. In particular, one can see that the matrix analogue of Tijdeman's theorem possesses infinitely many solutions. Using this similar technique, one can also show that the matrix analogue of Catalan's conjecture possesses infinitely many solutions too.

8. [12, Chapter 4, Theorem 3] There cannot be four squares in arithmetical progression.

   The above statement is false in matrix theory. That is, there exist matrices $X, Y, Z, W \in M_n(\mathbb{Z})$ such that $X^2 + Z^2 = 2Y^2$ and $Y^2 + W^2 = 2Z^2$. For example, let $X = \begin{pmatrix} 2 & -1 \\ 3 & -2 \end{pmatrix}$, $Y = \begin{pmatrix} 3 & 8 \\ -1 & -3 \end{pmatrix}$, $Z = \begin{pmatrix} -3 & 2 \\ -4 & 3 \end{pmatrix}$ and $W = \begin{pmatrix} -2 & 3 \\ -1 & 2 \end{pmatrix}$. We see that the matrices satisfy $X^2 + Z^2 = 2Y^2$ and $Y^2 + W^2 = 2Z^2$ and we call that X^2, Y^2, Z^2 and W^2 are in arithmetical progression.

REFERENCES

[1] M. Arnold, A. Eydelzon. On matrix Pythagorean triples. *Amer. Math. Monthly* **126**, *2* (2019), 158–160.

[2] E. D. Bolker. Solutions of $A^k + B^k = C^k$ in $n \times n$ integral matrices. *Amer. Math. Monthly* **75** (1968) 759–760.

[3] J. L. Brenner, B. Jacobson. Problems and Solutions: Solutions of Elementary Problems: E2030. *Amer. Math. Monthly* **78**, *5* (1971), 543–544

[4] M.-T. Chien, J. Meng. Fermat's equation over 2-by-2 matrices, *Bull. Korean Math. Soc.* **58**, *3* (2021) 609–616.

[5] R. Z. Domiaty. Solutions of $x^4 + y^4 = z^4$ in 2×2 integral matrices. *Amer. Math. Monthly* **73** (1966), 631.

[6] N. Freitas, S. Siksek. Fermat's last theorem over some small real quadratic fields. *Algebra Number Theory* **9**, *4* (2015), 875–895.

[7] P. M. Gibson. Solutions of $A^K + B^K = C^K$ in nonsingular integral matrices. *Math. Mag.* **43** (1970), 275–276.

[8] A. Grytczuk. On Fermat's equation in the set of integral 2×2 matrices. *Period. Math. Hungar.* **30**, *1* (1995) 67–72.

[9] A. Grytczuk, I. Kurzydlo. Note on the matrix Fermat's equation. *Notes on Number Theory and Discrete Mathematics* **17**, *2* (2011) 4–11, `https://nntdm.net/papers/nntdm-17/NNTDM-17-2-04-11.pdf`.

[10] A. Khazanov. Fermat's equation in matrices. *Serdica Math. J.* **21**, *1* (1995) 19–40.

[11] M. Le, C. Li. On Fermat's equation in integral 2×2 matrices. *Period. Math. Hungar.* **31**, *3* (1995) 219–222.

[12] L. J. Mordell. Diophantine equations. Pure Appl. Math., vol. **30**. London-New York, Academic Press, 1969.

[13] H. Qin. Fermat's problem and Goldbach's problem over $M_n(\mathbb{Z})$. *Linear Algebra Appl.* **236** (1996), 131–135.

[14] L. N. Vaserstein. Noncommutative number theory. *Contemp. Math.* **83** (1989) 445–449.

[15] A. Wiles. Modular elliptic curves and Fermat's last theorem. *Ann. of Math. (2)* **141**, *3* (1995), 443–551.

Department of Applied Sciences
Tezpur University
Napaam, Sonitpur, Assam-784028, India
e-mail: `kuldeep.sarma65@gmail.com`

Received August 25, 2024
Accepted August 8, 2025