Filomat 39:5 (2025), 1551–1571
https://doi.org/10.2298/FIL2505551L

Published by Faculty of Sciences and Mathematics,
University of Niš, Serbia
Available at: http://www.pmf.ni.ac.rs/filomat

# The matrix equation $aX^m + bY^n = cI_2$ over $M_2(\mathbb{Z})$

**Hongjian Li**[a], **Pingzhi Yuan**[b,*]

[a] *School of Mathematics and Statistics, Guangdong University of Foreign Studies, Guangzhou 510006, Guangdong, P. R. China*
[b] *School of Mathematical Sciences, South China Normal University, Guangzhou 510631, Guangdong, P. R. China*

**Abstract.** Let $\mathbb{N}$ be the set of all positive integers, and let $a, b, c$ be nonzero integers such that $\gcd(a, b, c) = 1$. We prove the following three results. Firstly, we show that the solvability of the matrix equation $aX^m + bY^n = cI_2$, $m, n \in \mathbb{N}$ in $M_2(\mathbb{Z})$ can be reduced to the solvability of a corresponding Diophantine equation when the matrices $X$ and $Y$ do not commute, i.e., $XY \neq YX$. Alternatively, when $X$ and $Y$ commute, i.e., $XY = YX$, the solvability of this matrix equation can be reduced to the solvability of the equation $ax^m + by^n = c$, $m, n \in \mathbb{N}$ in quadratic fields. Secondly, we determine all solutions of the matrix equation $X^n + Y^n = c^n I_2$, $n \in \mathbb{N}$, $n \geq 3$ in $M_2(\mathbb{Z})$ when $X$ and $Y$ do not commute. Moreover, when $X$ and $Y$ commute, we show that the solvability of this matrix equation can be reduced to the solvability of the equation $x^n + y^n = c^n$, $n \in \mathbb{N}$, $n \geq 3$ in quadratic fields. Finally, we determine all solutions of the matrix equation $aX^2 + bY^2 = cI_2$ in $M_2(\mathbb{Z})$.

## 1. Introduction

In [12], Vaserstein suggested solving some classical number theory problems in matrices. He considered a few classical problems of number theory with the ring $\mathbb{Z}$ substituted by the ring $M_2(\mathbb{Z})$ of $2 \times 2$ integral matrices, that is $2 \times 2$-matrices over $\mathbb{Z}$. Some classical Diophantine equations, such as Fermat's equation, Catalan's equation and Pell's equation, to matrix equations were studied by number of authors such as [2–9, 11].

Let us recall that the Pell's equation is a Diophantine equation of the form

$$x^2 - dy^2 = 1,$$

where $d$ is a positive integer which is not a perfect square. It is well-known that the Pell's equation has infinitely many solutions in positive integers $x$ and $y$. Recently, A. Grytczuk and I. Kurzydło [5] considered the solvability of the matrix negative Pell's equation

$$X^2 - dY^2 = -I_2,\ X,\ Y \in M_2(\mathbb{Z}),$$

2020 *Mathematics Subject Classification*. Primary 15A20; Secondary 15A24, 15B36, 11D09, 11D41.
*Keywords*. matrix equations; Jordan canonical form; quadratic fields
Received: 02 August 2024; Accepted: 23 December 2024
Communicated by Dijana Mosić
Research supported by the National Natural Science Foundation of China (Grant No. 12171163), the Basic and Applied Basic Research Foundation of Guangdong Province (Grant No. 2024A1515010589) and the Project of Guangdong University of Foreign Studies (Grant No. 2024RC063).
* Corresponding author: Pingzhi Yuan
*Email addresses:* lhj@gdufs.edu.cn (Hongjian Li), yuanpz@scnu.edu.cn (Pingzhi Yuan)
ORCID iDs: https://orcid.org/0000-0002-4842-4692 (Hongjian Li), https://orcid.org/0000-0001-6398-0614 (Pingzhi Yuan)

where $d$ is a positive integer. They gave a necessary and sufficient condition for the solvability of this matrix equation for nonsingular matrices $X, Y \in M_2(\mathbb{Z})$. In [3], B. Cohen considered the solvability of the generalized matrix Pell's equation

$$X^2 - dY^2 = cI_2,\ X,\ Y \in M_2(\mathbb{Z}), \tag{1}$$

where $d$ is a square-free integer and $c$ is an arbitrary integer. He determined all solutions of equation (1) for $c = \pm 1$, as well as all non-commutative solutions for an arbitrary integer $c$. Moreover, he proposed an open problem: how about the commutative solutions of equation (1) for an arbitrary integer $c$ ? In this paper, we give complete answers to this open problem.

The rest of this paper is organized as follows. In Section 2, we mainly study the solvability of the matrix equation

$$aX^m + bY^n = cI_2,\ X,\ Y \in M_2(\mathbb{Z}),\ m,\ n \in \mathbb{N}, \tag{2}$$

where $a, b, c$ are nonzero integers such that $\gcd(a, b, c) = 1$. Let $\lambda$ be a nonzero integer and let $n \geq 3$ be a positive integer. Let $a = b = 1$, $c = \lambda^n$ and $m = n$. Then equation (2) becomes the matrix equation

$$X^n + Y^n = \lambda^n I_2,\ X,\ Y \in M_2(\mathbb{Z}),\ n \in \mathbb{N},\ n \geq 3. \tag{3}$$

In Section 3, we mainly study the solvability of the matrix equation (3). Let $m = n = 2$. Then equation (2) becomes the matrix equation

$$aX^2 + bY^2 = cI_2,\ X,\ Y \in M_2(\mathbb{Z}). \tag{4}$$

In Section 4, we mainly study the solvability of the matrix equation (4), and we determine all solutions of this matrix equation.

## 2. The solvability of $aX^m + bY^n = cI_2,\ X,\ Y \in M_2(\mathbb{Z})$

In this section, we will study separately commutative and non-commutative solutions of equation (2), i.e., solutions satisfying $XY = YX$ or $XY \neq YX$, respectively. We first study the non-commutative solutions of equation (2).

**Lemma 2.1.** ([10, Theorem 1]) *Let $A = \begin{pmatrix} e & f \\ g & h \end{pmatrix}$ be an arbitrary $2 \times 2$-matrix and let $T = e + h$ denote its trace and $D = eh - fg$ its determinant. Let $y_n = \sum_{i=0}^{\lfloor n/2 \rfloor} \binom{n-i}{i} T^{n-2i}(-D)^i$. Then, for $n \geq 1$,*

$$A^n = \begin{pmatrix} y_n - hy_{n-1} & fy_{n-1} \\ gy_{n-1} & y_n - ey_{n-1} \end{pmatrix}.$$

**Theorem 2.2.** *Let $a, b, c$ be nonzero integers such that $\gcd(a, b, c) = 1$ and let $m, n$ be positive integers. If there are two matrices $X, Y \in M_2(\mathbb{Z})$ such that*

$$aX^m + bY^n = cI_2,\ XY \neq YX,$$

*then $X^m$ and $Y^n$ are scalar matrices.*

*Proof.* Note that $X^m$ is a scalar matrix if and only if $Y^n$ is a scalar matrix. So we only need to show that $Y^n$ is a scalar matrix. Let $J$ be the Jordan canonical form of $X$. Then there is a nonsingular matrix $P \in M_2(\mathbb{C})$ such that $P^{-1}XP = J$. The assumption $aX^m + bY^n = cI_2$ implies that $a\left(P^{-1}XP\right)^m + b\left(P^{-1}YP\right)^n = cI_2$, i.e.,

$$aJ^m + b\left(P^{-1}YP\right)^n = cI_2. \tag{5}$$

Let $P^{-1}YP = \begin{pmatrix} e & f \\ g & h \end{pmatrix}$. By Lemma 2.1, we have

$$\left(P^{-1}YP\right)^n = \begin{pmatrix} y_n - hy_{n-1} & fy_{n-1} \\ gy_{n-1} & y_n - ey_{n-1} \end{pmatrix},$$

where $y_n = \sum_{i=0}^{\lfloor n/2 \rfloor} \binom{n-i}{i} (tr(Y))^{n-2i} (-\det(Y))^i$. From (5), it follows that

$$aJ^m + b\begin{pmatrix} y_n - hy_{n-1} & fy_{n-1} \\ gy_{n-1} & y_n - ey_{n-1} \end{pmatrix} = cI_2. \tag{6}$$

**Case 1:** $J = \begin{pmatrix} x_1 & 0 \\ 0 & x_2 \end{pmatrix}$, where $x_1$ and $x_2$ are the eigenvalues of $X$.

By (6), we have

$$a\begin{pmatrix} x_1^m & 0 \\ 0 & x_2^m \end{pmatrix} + b\begin{pmatrix} y_n - hy_{n-1} & fy_{n-1} \\ gy_{n-1} & y_n - ey_{n-1} \end{pmatrix} = \begin{pmatrix} c & 0 \\ 0 & c \end{pmatrix}.$$

Comparing both sides, we have $fy_{n-1} = gy_{n-1} = 0$. If $y_{n-1} \neq 0$, then $f = g = 0$, which implies that $P^{-1}YP = \begin{pmatrix} e & 0 \\ 0 & h \end{pmatrix}$. Since $P^{-1}XP = J = \begin{pmatrix} x_1 & 0 \\ 0 & x_2 \end{pmatrix}$, we obtain $XY = YX$, a contradiction. Therefore, $y_{n-1} = 0$. Then $\left(P^{-1}YP\right)^n = y_nI_2$. This implies that $Y^n = y_nI_2$.

**Case 2:** $J = \begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix}$, where $\lambda$ is the eigenvalue of $X$.

By (6), we obtain

$$a\begin{pmatrix} \lambda^m & * \\ 0 & \lambda^m \end{pmatrix} + b\begin{pmatrix} y_n - hy_{n-1} & fy_{n-1} \\ gy_{n-1} & y_n - ey_{n-1} \end{pmatrix} = \begin{pmatrix} c & 0 \\ 0 & c \end{pmatrix}.$$

Comparing both sides, we have $gy_{n-1} = (e-h)y_{n-1} = 0$. If $y_{n-1} \neq 0$, then $g = 0$ and $e = h$, which imply that $P^{-1}YP = \begin{pmatrix} e & f \\ 0 & e \end{pmatrix}$. Since $P^{-1}XP = J = \begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix}$, we obtain $XY = YX$, a contradiction. Therefore, $y_{n-1} = 0$. Then $\left(P^{-1}YP\right)^n = y_nI_2$. This implies that $Y^n = y_nI_2$. □

If we replace the $cI_2$ by $\begin{pmatrix} c_1 & 0 \\ 0 & c_2 \end{pmatrix}$ in Theorem 2.2 and let $XY = YX$, then we have the following proposition.

**Proposition 2.3.** *Let $a$, $b$ be nonzero integers and let $m$, $n$ be positive integers. Let $c_1$ and $c_2$ be integers such that $c_1 \neq c_2$. Let $X$ and $Y$ be $2 \times 2$-matrices over $\mathbb{Z}$. Then*

$$aX^m + bY^n = \begin{pmatrix} c_1 & 0 \\ 0 & c_2 \end{pmatrix}, \; XY = YX \tag{7}$$

*if and only if*

$$X = \begin{pmatrix} x_1 & 0 \\ 0 & x_2 \end{pmatrix}, \; Y = \begin{pmatrix} y_1 & 0 \\ 0 & y_2 \end{pmatrix},$$

*where $x_1$, $x_2$, $y_1$, $y_2 \in \mathbb{Z}$ satisfy $ax_i^m + by_i^n = c_i$, $i = 1, 2$.*

*Proof.* The sufficiency is clear. We next prove necessity.

**Case 1:** $X$ and $Y$ are diagonalizable.

From $XY = YX$, it follows that they are simultaneously diagonalizable. Then there is a nonsingular matrix $P = \begin{pmatrix} p_{11} & p_{12} \\ p_{21} & p_{22} \end{pmatrix} \in M_2(\mathbb{C})$ such that

$$P^{-1}XP = \begin{pmatrix} x_1 & 0 \\ 0 & x_2 \end{pmatrix}, \; P^{-1}YP = \begin{pmatrix} y_1 & 0 \\ 0 & y_2 \end{pmatrix},$$

where $x_i$, $y_i$, $i = 1, 2$ are the eigenvalues of $X$ and $Y$, respectively. The assumption $aX^m + bY^n = \begin{pmatrix} c_1 & 0 \\ 0 & c_2 \end{pmatrix}$ implies that $a\left(P^{-1}XP\right)^m + b\left(P^{-1}YP\right)^n = P^{-1}\begin{pmatrix} c_1 & 0 \\ 0 & c_2 \end{pmatrix}P$. Then

$$a\begin{pmatrix} x_1^m & 0 \\ 0 & x_2^m \end{pmatrix} + b\begin{pmatrix} y_1^n & 0 \\ 0 & y_2^n \end{pmatrix} = \frac{1}{p_{11}p_{22} - p_{12}p_{21}}\begin{pmatrix} p_{11}p_{22}c_1 - p_{12}p_{21}c_2 & p_{12}p_{22}\left(c_1 - c_2\right) \\ p_{11}p_{21}\left(c_2 - c_1\right) & p_{11}p_{22}c_2 - p_{12}p_{21}c_1 \end{pmatrix}.$$

Comparing both sides, we have $p_{12}p_{22} = p_{11}p_{21} = 0$.

If $p_{12} = 0$, then $\det(P) = p_{11}p_{22} - p_{12}p_{21} = p_{11}p_{22}$. Since $\det(P) \neq 0$ and $p_{11}p_{21} = 0$, we have $p_{21} = 0$. Then

$$X = P\begin{pmatrix} x_1 & 0 \\ 0 & x_2 \end{pmatrix}P^{-1} = \begin{pmatrix} p_{11} & 0 \\ 0 & p_{22} \end{pmatrix}\begin{pmatrix} x_1 & 0 \\ 0 & x_2 \end{pmatrix}\begin{pmatrix} p_{11} & 0 \\ 0 & p_{22} \end{pmatrix}^{-1} = \begin{pmatrix} x_1 & 0 \\ 0 & x_2 \end{pmatrix}.$$

Likewise, $Y = \begin{pmatrix} y_1 & 0 \\ 0 & y_2 \end{pmatrix}$. Since $X, Y \in M_2(\mathbb{Z})$, we have $x_1, x_2, y_1, y_2 \in \mathbb{Z}$. The assumption $aX^m + bY^n = \begin{pmatrix} c_1 & 0 \\ 0 & c_2 \end{pmatrix}$ implies that $ax_i^m + by_i^n = c_i$, $i = 1, 2$.

If $p_{22} = 0$, then $\det(P) = p_{11}p_{22} - p_{12}p_{21} = -p_{12}p_{21}$. Since $\det(P) \neq 0$ and $p_{11}p_{21} = 0$, we have $p_{11} = 0$. Then

$$X = P\begin{pmatrix} x_1 & 0 \\ 0 & x_2 \end{pmatrix}P^{-1} = \begin{pmatrix} 0 & p_{12} \\ p_{21} & 0 \end{pmatrix}\begin{pmatrix} x_1 & 0 \\ 0 & x_2 \end{pmatrix}\begin{pmatrix} 0 & p_{12} \\ p_{21} & 0 \end{pmatrix}^{-1} = \begin{pmatrix} x_2 & 0 \\ 0 & x_1 \end{pmatrix}.$$

Likewise, $Y = \begin{pmatrix} y_2 & 0 \\ 0 & y_1 \end{pmatrix}$. Since $X, Y \in M_2(\mathbb{Z})$, we have $x_1, x_2, y_1, y_2 \in \mathbb{Z}$. The assumption $aX^m + bY^n = \begin{pmatrix} c_1 & 0 \\ 0 & c_2 \end{pmatrix}$ implies that $ax_2^m + by_2^n = c_1$ and $ax_1^m + by_1^n = c_2$.

**Case 2:** $X$ and $Y$ are not both diagonalizable.

Without loss of generality, we can assume that $X$ is not diagonalizable. Let $J$ be the Jordan canonical form of $X$. Then $J = \begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix}$, where $\lambda$ is the eigenvalue of $X$. Moreover, there is a nonsingular matrix $P = \begin{pmatrix} p_{11} & p_{12} \\ p_{21} & p_{22} \end{pmatrix} \in M_2(\mathbb{C})$ such that $P^{-1}XP = J = \begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix}$. Since $XY = YX$, we have $\left(P^{-1}XP\right) \cdot \left(P^{-1}YP\right) = \left(P^{-1}YP\right) \cdot \left(P^{-1}XP\right)$, i.e., $J \cdot \left(P^{-1}YP\right) = \left(P^{-1}YP\right) \cdot J$. This implies that $P^{-1}YP = \begin{pmatrix} y_1 & y_2 \\ 0 & y_1 \end{pmatrix}$, where $y_1, y_2 \in \mathbb{C}$. The assumption $aX^m + bY^n = \begin{pmatrix} c_1 & 0 \\ 0 & c_2 \end{pmatrix}$ implies that $a\left(P^{-1}XP\right)^m + b\left(P^{-1}YP\right)^n = P^{-1}\begin{pmatrix} c_1 & 0 \\ 0 & c_2 \end{pmatrix}P$. Then

$$a\begin{pmatrix} \lambda^m & * \\ 0 & \lambda^m \end{pmatrix} + b\begin{pmatrix} y_1^n & * \\ 0 & y_1^n \end{pmatrix} = \frac{1}{p_{11}p_{22} - p_{12}p_{21}}\begin{pmatrix} p_{11}p_{22}c_1 - p_{12}p_{21}c_2 & p_{12}p_{22}\left(c_1 - c_2\right) \\ p_{11}p_{21}\left(c_2 - c_1\right) & p_{11}p_{22}c_2 - p_{12}p_{21}c_1 \end{pmatrix}.$$

Comparing both sides, we have $p_{11}p_{21} = p_{11}p_{22} + p_{12}p_{21} = 0$. This implies that $\det(P) = p_{11}p_{22} - p_{12}p_{21} = 0$, a contradiction. □

**Remark 2.4.** All commutative solutions of equation (7) are given by Proposition 2.3. How about the non-commutative solutions of equation (7)? This is an interesting problem that lies out of the scope of this paper.

About scalar matrices, we have the following lemma and proposition.

**Lemma 2.5.** ([13]) *Let $X$ be a $2 \times 2$-matrix over $\mathbb{Z}$ such that $X^n$ is a scalar matrix for some $n \in \mathbb{N}$, and let $k$ be the smallest positive integer with such property. Then the following statements hold.*

1) $k \in \{1, 2, 3, 4, 6\}$;
2)
   (i) $k = 1$ *if and only if* $X = aI_2$, $a \in \mathbb{Z}$;
   (ii) $k = 2$ *if and only if* $X = \begin{pmatrix} a & b \\ c & -a \end{pmatrix}$, *where* $a, b, c \in \mathbb{Z}$ *satisfy* $a^2 + b^2 + c^2 \neq 0$. *Moreover,* $X^2 = \left(a^2 + bc\right) I_2$;
   (iii) $k = 3$ *if and only if* $X = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, *where* $a, b, c, d \in \mathbb{Z}$ *satisfy* $(a+d)^2 = ad - bc$ *and* $a + d \neq 0$. *Moreover,* $X^3 = -(a+d)^3 I_2$;
   (iv) $k = 4$ *if and only if* $X = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, *where* $a, b, c, d \in \mathbb{Z}$ *satisfy* $(a+d)^2 = 2(ad - bc)$ *and* $a + d \neq 0$. *Moreover,* $X^4 = -4\left(\frac{a+d}{2}\right)^4 I_2 = -(ad - bc)^2 I_2$;
   (v) $k = 6$ *if and only if* $X = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, *where* $a, b, c, d \in \mathbb{Z}$ *satisfy* $(a+d)^2 = 3(ad - bc)$ *and* $a + d \neq 0$. *Moreover,* $X^6 = -(ad - bc)^3 I_2$.

**Proposition 2.6.** *Let* $X \in M_2(\mathbb{Z})$ *be a nonsingular matrix such that* $X^n$ *is a scalar matrix for some* $n \in \mathbb{N}$, *and let* $k$ *be the smallest positive integer with such property. Then for* $m \in \mathbb{N}$, $X^m$ *is a scalar matrix if and only if* $k \mid m$.

*Proof.* The sufficiency is clear. We next prove necessity. Since $X^m$ and $X^k$ are scalar matrices, we have $X^m = \lambda I_2$ and $X^k = \mu I_2$ for some $\lambda, \mu \in \mathbb{Z}\backslash\{0\}$. Let $m = kq + r$, where $q, r \in \mathbb{Z}$ and $0 \leq r < k$. Then

$$X^r = X^{m-kq} = X^m \cdot \left(X^k\right)^{-q} = \lambda I_2 \cdot (\mu I_2)^{-q} = \frac{\lambda}{\mu^q} I_2.$$

If $r \neq 0$, then we obtain a contradiction to the minimality of $k$. Thus, $r = 0$. This means that $k \mid m$. □

About commutative $2 \times 2$ integral matrices, we have the following lemma.

**Lemma 2.7.** *Let* $X = \begin{pmatrix} t_1 & t_2 \\ t_3 & t_4 \end{pmatrix}$ *and* $Y = \begin{pmatrix} s_1 & s_2 \\ s_3 & s_4 \end{pmatrix}$ *be* $2 \times 2$*-matrices over* $\mathbb{Z}$. *Then* $XY = YX$ *if and only if the vectors* $\overrightarrow{t} = (t_1 - t_4, t_2, t_3)$ *and* $\overrightarrow{s} = (s_1 - s_4, s_2, s_3)$ *are linearly dependent over* $\mathbb{Q}$.

*Proof.* By a direct computation, we have

$$XY - YX = \begin{pmatrix} t_2 s_3 - s_2 t_3 & (t_1 - t_4)s_2 - (s_1 - s_4)t_2 \\ (s_1 - s_4)t_3 - (t_1 - t_4)s_3 & s_2 t_3 - t_2 s_3 \end{pmatrix}$$
$$= \begin{pmatrix} \begin{vmatrix} t_2 & t_3 \\ s_2 & s_3 \end{vmatrix} & \begin{vmatrix} t_1 - t_4 & t_2 \\ s_1 - s_4 & s_2 \end{vmatrix} \\ -\begin{vmatrix} t_1 - t_4 & t_3 \\ s_1 - s_4 & s_3 \end{vmatrix} & -\begin{vmatrix} t_2 & t_3 \\ s_2 & s_3 \end{vmatrix} \end{pmatrix}.$$

Let $\overrightarrow{i} = (1, 0, 0)$, $\overrightarrow{j} = (0, 1, 0)$ and $\overrightarrow{k} = (0, 0, 1)$. Then $XY = YX$ if and only if

$$\begin{vmatrix} t_2 & t_3 \\ s_2 & s_3 \end{vmatrix} = \begin{vmatrix} t_1 - t_4 & t_2 \\ s_1 - s_4 & s_2 \end{vmatrix} = \begin{vmatrix} t_1 - t_4 & t_3 \\ s_1 - s_4 & s_3 \end{vmatrix} = 0$$

if and only if

$$\overrightarrow{t} \times \overrightarrow{s} = \begin{vmatrix} \overrightarrow{i} & \overrightarrow{j} & \overrightarrow{k} \\ t_1 - t_4 & t_2 & t_3 \\ s_1 - s_4 & s_2 & s_3 \end{vmatrix} = \begin{vmatrix} t_2 & t_3 \\ s_2 & s_3 \end{vmatrix} \overrightarrow{i} - \begin{vmatrix} t_1 - t_4 & t_3 \\ s_1 - s_4 & s_3 \end{vmatrix} \overrightarrow{j} + \begin{vmatrix} t_1 - t_4 & t_2 \\ s_1 - s_4 & s_2 \end{vmatrix} \overrightarrow{k} = \overrightarrow{0}$$

if and only if the vectors $\overrightarrow{t}$ and $\overrightarrow{s}$ are linearly dependent over $\mathbb{Q}$. □

From Theorem 2.2, Lemmas 2.5, 2.7 and Proposition 2.6, we conclude that finding the non-commutative solutions of equation (2) can be reduced to finding the solutions of the corresponding Diophantine equation. Next, we give an example to illustrate it, i.e., Proposition 2.8.

**Proposition 2.8.** *Let $a$, $b$, $c$ be nonzero integers such that* $\gcd(a, b, c) = 1$. *Let $X$ and $Y$ be $2 \times 2$-matrices over $\mathbb{Z}$. Then the following statements hold.*

1)
$$aX^2 + bY^2 = cI_2,\ XY \neq YX$$

*if and only if*
$$X = \begin{pmatrix} t_1 & t_2 \\ t_3 & -t_1 \end{pmatrix},\ Y = \begin{pmatrix} s_1 & s_2 \\ s_3 & -s_1 \end{pmatrix},$$

*where $t_1, t_2, t_3, s_1, s_2, s_3 \in \mathbb{Z}$ satisfy $a\left(t_1^2 + t_2t_3\right) + b\left(s_1^2 + s_2s_3\right) = c$ and the vectors $\overrightarrow{t} = (t_1, t_2, t_3)$ and $\overrightarrow{s} = (s_1, s_2, s_3)$ are linearly independent over $\mathbb{Q}$;*

2)
$$X^4 + Y^4 = c^4I_2,\ XY \neq YX$$

*if and only if*
$$X = \begin{pmatrix} t_1 & t_2 \\ t_3 & -t_1 \end{pmatrix},\ Y = \begin{pmatrix} s_1 & s_2 \\ s_3 & -s_1 \end{pmatrix},$$

*where $t_1, t_2, t_3, s_1, s_2, s_3 \in \mathbb{Z}$ satisfy $\left(t_1^2 + t_2t_3\right)^2 + \left(s_1^2 + s_2s_3\right)^2 = c^4$ and the vectors $\overrightarrow{t} = (t_1, t_2, t_3)$ and $\overrightarrow{s} = (s_1, s_2, s_3)$ are linearly independent over $\mathbb{Q}$.*

*Proof.* 1) Sufficiency follows from Lemma 2.5 2) (ii) and Lemma 2.7. We next prove necessity. From Theorem 2.2, it follows that $X^2$ and $Y^2$ are scalar matrices. Since $XY \neq YX$, $X$ and $Y$ are not scalar matrices. By Lemma 2.5 2) (ii), we have
$$X = \begin{pmatrix} t_1 & t_2 \\ t_3 & -t_1 \end{pmatrix},\ Y = \begin{pmatrix} s_1 & s_2 \\ s_3 & -s_1 \end{pmatrix},$$

where $t_1, t_2, t_3, s_1, s_2, s_3$ are integers. Moreover, $X^2 = \left(t_1^2 + t_2t_3\right)I_2$ and $Y^2 = \left(s_1^2 + s_2s_3\right)I_2$. The assumption $aX^2 + bY^2 = cI_2$ implies that $a\left(t_1^2 + t_2t_3\right) + b\left(s_1^2 + s_2s_3\right) = c$. Let $\overrightarrow{t} = (t_1, t_2, t_3)$ and $\overrightarrow{s} = (s_1, s_2, s_3)$. Then it follows from Lemma 2.7 that $\overrightarrow{t}$ and $\overrightarrow{s}$ are linearly independent over $\mathbb{Q}$.

2) Sufficiency follows from Lemma 2.5 2) (ii) and Lemma 2.7. We next prove necessity. From Theorem 2.2, it follows that $X^4$ and $Y^4$ are scalar matrices. Let $k$ and $l$ be the smallest positive integers such that $X^k$ and $Y^l$ are scalar matrices, respectively. Since $XY \neq YX$, we have $k, l \neq 1$. By Lemma 2.5 and Proposition 2.6, we have $k, l \in \{2, 4\}$.

**Case 1:** $k = l = 2$.

By Lemma 2.5, we have
$$X = \begin{pmatrix} t_1 & t_2 \\ t_3 & -t_1 \end{pmatrix},\ Y = \begin{pmatrix} s_1 & s_2 \\ s_3 & -s_1 \end{pmatrix},$$

where $t_1, t_2, t_3, s_1, s_2, s_3$ are integers. Moreover, $X^2 = \left(t_1^2 + t_2t_3\right)I_2$ and $Y^2 = \left(s_1^2 + s_2s_3\right)I_2$. The assumption $X^4 + Y^4 = c^4I_2$ implies that $\left(t_1^2 + t_2t_3\right)^2 + \left(s_1^2 + s_2s_3\right)^2 = c^4$. Let $\overrightarrow{t} = (t_1, t_2, t_3)$ and $\overrightarrow{s} = (s_1, s_2, s_3)$. Then it follows from Lemma 2.7 that $\overrightarrow{t}$ and $\overrightarrow{s}$ are linearly independent over $\mathbb{Q}$.

**Case 2:** $k = 2$, $l = 4$.

By Lemma 2.5, we have $X^2 = uI_2$ and $Y^4 = -4v^4I_2$ for some $u \in \mathbb{Z}$ and $v \in \mathbb{Z}\backslash\{0\}$. The assumption $X^4 + Y^4 = c^4I_2$ implies that $c^4 + 4v^4 = u^2$, which is impossible.

**Case 3:** $k = 4$, $l = 2$.

This case is also impossible, where the reason is similar to Case 2.

**Case 4:** $k = l = 4$.

By Lemma 2.5, we have $X^4 = -4u^4 I_2$ and $Y^4 = -4v^4 I_2$ for some $u, v \in \mathbb{Z}\backslash\{0\}$. The assumption $X^4+Y^4 = c^4 I_2$ implies that $-4u^4 - 4v^4 = c^4$, which is impossible. □

We now study the commutative solutions of equation (2).

**Proposition 2.9.** *If* $(X, Y)$ *is a solution of equation* (2), *then*

$$ax_i^m + by_i^n = c, \ i = 1, 2, \tag{8}$$

*where* $x_i$, $y_i$, $i = 1, 2$ *are the eigenvalues of* $X$ *and* $Y$, *respectively.*

*Proof.* Suppose that $\begin{pmatrix} x_1 & * \\ 0 & x_2 \end{pmatrix}$ is the Jordan canonical form of $X$. Then there is a nonsingular matrix $P \in M_2(\mathbb{C})$ such that $P^{-1}XP = \begin{pmatrix} x_1 & * \\ 0 & x_2 \end{pmatrix}$. The assumption $aX^m + bY^n = cI_2$ implies that $a\left(P^{-1}XP\right)^m + b\left(P^{-1}YP\right)^n = cI_2$. Then we obtain $\begin{pmatrix} ax_1^m & * \\ 0 & ax_2^m \end{pmatrix} + b\left(P^{-1}YP\right)^n = cI_2$, which implies that

$$bY^n = P\begin{pmatrix} c - ax_1^m & * \\ 0 & c - ax_2^m \end{pmatrix}P^{-1}. \tag{9}$$

Comparing the eigenvalues of both sides of (9), we have $ax_i^m + by_i^n = c$, $i = 1, 2$. □

If the eigenvalues of $X$ and $Y$ are integers, then equation (8) becomes the Diophantine equation $ax^m+by^n = c$, $x, y \in \mathbb{Z}$. So we can assume that the eigenvalues of $X$ or $Y$ are not integers. Let $A = \begin{pmatrix} e & f \\ g & 0 \end{pmatrix} \in M_2(\mathbb{Z})$ be a given matrix such that $fg \neq 0$ and $\gcd(e, f, g) = 1$, and let $C(A) = \{B \in M_2(\mathbb{Z}) : AB = BA\}$. In [9], we showed that the solvability of the matrix equation

$$aX^m + bY^n = cI_2, \ XY = YX, \ m, n \in \mathbb{N} \tag{10}$$

in $M_2(\mathbb{Z})$ can be reduced to the solvability of the matrix equation

$$aX^m + bY^n = cI_2, \ m, n \in \mathbb{N} \tag{11}$$

in $C(A)$, and finally to the solvability of the equation

$$ax^m + by^n = c, \ m, n \in \mathbb{N} \tag{12}$$

in quadratic fields. As a corollary of [9, Theorem 3.1], we have the following theorem.

**Theorem 2.10.** *Let* $A = \begin{pmatrix} e & f \\ g & 0 \end{pmatrix} \in M_2(\mathbb{Z})$ *be a given matrix such that* $fg \neq 0$ *and* $\gcd(e, f, g) = 1$. *Let* $K = \mathbb{Q}\left(\sqrt{e^2 + 4fg}\right)$ *and let* $O_K$ *be its ring of integers. Then the following statements hold.*

1) *If* $e^2 + 4fg$ *is a square, then equation* (11) *has a non-trivial solution in* $C(A)$ *if and only if equation* (12) *has a non-trivial solution in* $\mathbb{Z}$;
2) *If* $e^2 + 4fg$ *is not a square and* $D$ *is the unique square-free integer such that* $e^2 + 4fg = k^2 D$ *for some* $k \in \mathbb{N}$, *then equation* (11) *has a non-trivial solution in* $C(A)$ *if and only if equation* (12) *has a non-trivial solution* $(x, y)$ *in* $O_K$ *such that* $x, y$ *can be written in the form*

$$\frac{s + t\sqrt{D}}{2}, \quad s, t \in \mathbb{Z}, \ k \mid t.$$

From Theorem 2.10, we conclude that the solvability of equation (10) in $M_2(\mathbb{Z})$ can be reduced to the solvability of equation (12) in quadratic fields. However, the solvability of equation (12) in quadratic fields is unsolved.

## 3. The solvability of $X^n + Y^n = \lambda^n I_2$, $X, Y \in M_2(\mathbb{Z})$

In this section, we mainly consider the non-trivial solutions of equation (3), i.e., solutions satisfying $\det(XY) \neq 0$. Indeed, suppose that $(X, Y)$ is a solution of equation (3) such that $\det(XY) = 0$. Without loss of generality, we can assume that $\det(X) = 0$. If the eigenvalues of $X$ are both equal to zero, then $X^2 = O$. In this case, equation (3) becomes the matrix equation

$$Y^n = \lambda^n I_2,\ Y \in M_2(\mathbb{Z}),\ n \in \mathbb{N},\ n \geq 3.$$

However, all solutions of this matrix equation can be given by Lemma 2.5. So we only need to consider the non-trivial solutions of equation (3). In [8], we showed that equation (3) has no non-trivial solutions if the eigenvalues of $X$ or $Y$ are integers. Moreover, we gave all non-trivial solutions of equation (3) for $\lambda = \pm 1$. In this section, we will study separately commutative and non-commutative solutions of equation (3) for an arbitrary nonzero integer $\lambda$. We first study the non-commutative solutions of equation (3).

**Theorem 3.1.** *Equation* (3) *has no non-commutative non-trivial solutions for* $n \neq 4$.

*Proof.* Suppose that $(X, Y)$ is a non-commutative non-trivial solution of equation (3) for $n \neq 4$. Then we have $X^n + Y^n = \lambda^n I_2$, $XY \neq YX$ and $\det(XY) \neq 0$. From Theorem 2.2, it follows that $X^n$ and $Y^n$ are scalar matrices. Let $k$ and $l$ be the smallest positive integers such that $X^k$ and $Y^l$ are scalar matrices, respectively. Since $XY \neq YX$, we have $k, l \neq 1$. By Lemma 2.5, we have $k, l \in \{2, 3, 4, 6\}$. From Proposition 2.6, it follows that $k \mid n$ and $l \mid n$. Let $q$ be the least common multiple of $k$ and $l$. Then $q \mid n$. Since $k, l \in \{2, 3, 4, 6\}$, we have $q \in \{2, 3, 4, 6, 12\}$. If $\gcd(n, 6) = 1$, then $q \nmid n$, a contradiction.

**Case 1:** $n \equiv 0 \pmod 6$. Then $n = 6m$ for some positive integer $m$.

**Subcase 1.1:** $2 \mid m$.

Then $m = 2t$ for some positive integer $t$, which implies that $n = 12t$. By Lemma 2.5, we have $X^{12} = a^3 I_2$ and $Y^{12} = b^3 I_2$ for some $a, b \in \mathbb{Z}\backslash\{0\}$. The assumption $X^n + Y^n = \lambda^n I_2$ implies that $a^{3t} I_2 + b^{3t} I_2 = \lambda^{12t} I_2$. Then $(a^t)^3 + (b^t)^3 = \left(\lambda^{4t}\right)^3$, which is impossible by Fermat's last theorem.

**Subcase 1.2:** $2 \nmid m$.

By Proposition 2.6, we have $k, l \in \{2, 3, 6\}$. By Lemma 2.5, we obtain $X^6 = a^3 I_2$ and $Y^6 = b^3 I_2$ for some $a, b \in \mathbb{Z}\backslash\{0\}$. The assumption $X^n + Y^n = \lambda^n I_2$ implies that $a^{3m} I_2 + b^{3m} I_2 = \lambda^{6m} I_2$. Then $(a^m)^3 + (b^m)^3 = \left(\lambda^{2m}\right)^3$, which is impossible by Fermat's last theorem.

**Case 2:** $n \equiv 2 \pmod 6$. Then $n = 2 + 6m$ for some positive integer $m$.

**Subcase 2.1:** $2 \mid m$.

Then $m = 2t$ for some positive integer $t$, which implies that $n = 2 + 12t$. By Proposition 2.6, we have $k = l = 2$. By Lemma 2.5, we have $X^2 = aI_2$ and $Y^2 = bI_2$ for some $a, b \in \mathbb{Z}\backslash\{0\}$. The assumption $X^n + Y^n = \lambda^n I_2$ implies that $a^{1+6t} I_2 + b^{1+6t} I_2 = \lambda^{2+12t} I_2$. Then $a^{1+6t} + b^{1+6t} = \left(\lambda^2\right)^{1+6t}$, which is impossible by Fermat's last theorem.

**Subcase 2.2:** $2 \nmid m$.

Then $1 + 3m = 2t$ for some positive integer $t \geq 2$. Moreover, $3 \nmid t$. We obtain $n = 2 + 6m = 2(1 + 3m) = 4t$. By Proposition 2.6, we have $k, l \in \{2, 4\}$. By Lemma 2.5, we obtain $X^4 = \pm a^2 I_2$ and $Y^4 = \pm b^2 I_2$ for some $a, b \in \mathbb{Z}\backslash\{0\}$. The assumption $X^n + Y^n = \lambda^n I_2$ implies that $\left(\pm a^2\right)^t I_2 + \left(\pm b^2\right)^t I_2 = \left(\lambda^4\right)^t I_2$. Then $\left(\pm a^2\right)^t + \left(\pm b^2\right)^t = \left(\lambda^4\right)^t$, which is impossible by Fermat's last theorem.

**Case 3:** $n \equiv 3 \pmod 6$.

Then $n = 3 + 6m$ for some non-negative integer $m$. By Proposition 2.6, we have $k = l = 3$. By Lemma 2.5, we have $X^3 = a^3 I_2$ and $Y^3 = b^3 I_2$ for some $a, b \in \mathbb{Z}\backslash\{0\}$. The assumption $X^n + Y^n = \lambda^n I_2$ implies that $a^n I_2 + b^n I_2 = \lambda^n I_2$. Then $a^n + b^n = \lambda^n$, which is impossible by Fermat's last theorem.

**Case 4:** $n \equiv 4 \pmod 6$. Since $n \neq 4$, we have $n = 4 + 6m$ for some positive integer $m$.

**Subcase 4.1:** $2 \nmid m$.

By Proposition 2.6, we have $k = l = 2$. By Lemma 2.5, we obtain $X^2 = aI_2$ and $Y^2 = bI_2$ for some $a, b \in \mathbb{Z}\backslash\{0\}$. The assumption $X^n + Y^n = \lambda^n I_2$ implies that $a^{2+3m}I_2 + b^{2+3m}I_2 = \left(\lambda^2\right)^{2+3m} I_2$. Then $a^{2+3m} + b^{2+3m} = \left(\lambda^2\right)^{2+3m}$, which is impossible by Fermat's last theorem.

**Subcase 4.2:** $2 \mid m$.

Then $m = 2t$ for some positive integer $t$, which implies that $n = 4 + 12t$. By Proposition 2.6, we have $k, l \in \{2, 4\}$. By Lemma 2.5, we have $X^4 = aI_2$ and $Y^4 = bI_2$ for some $a, b \in \mathbb{Z}\backslash\{0\}$. The assumption $X^n + Y^n = \lambda^n I_2$ implies that $a^{1+3t}I_2 + b^{1+3t}I_2 = \lambda^{4+12t}I_2$. Then $a^{1+3t} + b^{1+3t} = \left(\lambda^4\right)^{1+3t}$, which is impossible by Fermat's last theorem. □

**Remark 3.2.** All non-commutative solutions of equation (3) are given by Proposition 2.8 2) for $n = 4$.

We now study the commutative solutions of equation (3). If the eigenvalues of $X$ and $Y$ are integers, then it follows from Proposition 2.9 that

$$x_i^n + y_i^n = \lambda^n,\ i = 1, 2,\ n \in \mathbb{N},\ n \geq 3,$$

where $x_i, y_i \in \mathbb{Z}\backslash\{0\}$, $i = 1, 2$ are the eigenvalues of $X$ and $Y$, respectively. We know that this is impossible by Fermat's last theorem. Thus, we can assume that the eigenvalues of $X$ or $Y$ are not integers. Let $A = \begin{pmatrix} e & f \\ g & 0 \end{pmatrix} \in M_2(\mathbb{Z})$ be a given matrix such that $fg \neq 0$ and $\gcd(e, f, g) = 1$, and let $C(A) = \{B \in M_2(\mathbb{Z}) : AB = BA\}$. In [9], we showed that the solvability of the matrix equation

$$X^n + Y^n = \lambda^n I_2,\ XY = YX,\ n \in \mathbb{N},\ n \geq 3 \tag{13}$$

in $M_2(\mathbb{Z})$ can be reduced to the solvability of the matrix equation

$$X^n + Y^n = \lambda^n I_2,\ n \in \mathbb{N},\ n \geq 3 \tag{14}$$

in $C(A)$, and finally to the solvability of the equation

$$x^n + y^n = \lambda^n,\ n \in \mathbb{N},\ n \geq 3 \tag{15}$$

in quadratic fields. As a corollary of [9, Theorem 3.1], we have the following theorem.

**Theorem 3.3.** *Let $A = \begin{pmatrix} e & f \\ g & 0 \end{pmatrix} \in M_2(\mathbb{Z})$ be a given matrix such that $fg \neq 0$ and $\gcd(e, f, g) = 1$. Let $K = \mathbb{Q}\left(\sqrt{e^2 + 4fg}\right)$ and let $O_K$ be its ring of integers. Then the following statements hold.*

1) *If $e^2 + 4fg$ is a square, then equation (14) has no non-trivial solutions in $C(A)$;*
2) *If $e^2 + 4fg$ is not a square and $D$ is the unique square-free integer such that $e^2 + 4fg = k^2D$ for some $k \in \mathbb{N}$, then equation (14) has a non-trivial solution in $C(A)$ if and only if equation (15) has a non-trivial solution $(x, y)$ in $O_K$ such that $x, y$ can be written in the form*

$$\frac{s + t\sqrt{D}}{2},\quad s, t \in \mathbb{Z},\ k \mid t.$$

From Theorem 3.3, we conclude that the solvability of equation (13) in $M_2(\mathbb{Z})$ can be reduced to the solvability of equation (15) in quadratic fields. However, the solvability of equation (15) in quadratic fields is unsolved. We next list a known result about the solvability of the Fermat's equation in quadratic fields.

**Lemma 3.4.** ([1]) *The Fermat's equation*

$$x^n + y^n = z^n,\ n \in \mathbb{N},\ n \geq 3$$

*has no non-trivial solutions in quadratic fields for $n = 6, 9$.*

By Theorems 3.1, 3.3 and Lemma 3.4, we have the following proposition.

**Proposition 3.5.** *Equation* (3) *has no non-trivial solutions in* $M_2(\mathbb{Z})$ *for* $n = 6, 9$.

*Proof.* Directly from Theorems 3.1, 3.3 and Lemma 3.4. □

**Corollary 3.6.** *Let* $\lambda$ *be a nonzero integer and let* $i, j, k$ *be positive integers such that* $6 \mid \gcd(i, j, k)$ *or* $9 \mid \gcd(i, j, k)$. *Then the matrix equation*

$$X^i + Y^j = \lambda^k I_2$$

*has no non-trivial solutions in* $M_2(\mathbb{Z})$.

*Proof.* Directly from Proposition 3.5. □

## 4. All solutions of $aX^2 + bY^2 = cI_2$, $X, Y \in M_2(\mathbb{Z})$

Note that all non-commutative solutions of equation (4) are given by Proposition 2.8 1). Thus, in this section, we only need to study the commutative solutions of equation (4).

**Theorem 4.1.** *Let* $a, b, c$ *be nonzero integers such that* $-ab$ *is not a square and* $\gcd(a, b, c) = 1$. *Let* $X$ *and* $Y$ *be* $2 \times 2$*-matrices over* $\mathbb{Z}$. *Then*

$$aX^2 + bY^2 = cI_2,\ XY = YX$$

*if and only if one of the following statements holds.*

(i) $X = t_1 I_2$ *and* $Y = t_2 I_2$, *where* $t_1, t_2 \in \mathbb{Z}$ *satisfy* $at_1^2 + bt_2^2 = c$;

(ii) $X = t_1 I_2$ *and* $Y = \begin{pmatrix} t_4 & t_2 \\ t_3 & -t_4 \end{pmatrix}$, *where* $t_1, t_2, t_3, t_4 \in \mathbb{Z}$ *satisfy* $at_1^2 + b\left(t_4^2 + t_2 t_3\right) = c$;

(iii) $X = t_1 I_2 + \frac{u-c}{g}\begin{pmatrix} 0 & t_2 \\ t_3 & -k \end{pmatrix}$ *and* $Y = t_4 I_2 + \frac{va}{g}\begin{pmatrix} 0 & t_2 \\ t_3 & -k \end{pmatrix}$, *where* $t_1, t_2, t_3, t_4, u, v, k \in \mathbb{Z}$, $u \neq c$, $g = \gcd(va, u - c)$ *and the following relations hold:*

$$u^2 + v^2 ab = c^2,\ at_1^2 + bt_4^2 + \frac{2act_2t_3}{g^2}(c - u) = c,\ (gt_1 + ck)(u - c) + vbgt_4 = 0.$$

*Proof.* We now prove sufficiency. We need to verify the following three cases.

First, suppose that $X = t_1 I_2$ and $Y = t_2 I_2$, where $t_1, t_2 \in \mathbb{Z}$ satisfy $at_1^2 + bt_2^2 = c$. Then $XY = YX$ and $aX^2 + bY^2 = at_1^2 I_2 + bt_2^2 I_2 = cI_2$.

Then, suppose that $X = t_1 I_2$ and $Y = \begin{pmatrix} t_4 & t_2 \\ t_3 & -t_4 \end{pmatrix}$, where $t_1, t_2, t_3, t_4 \in \mathbb{Z}$ satisfy $at_1^2 + b\left(t_4^2 + t_2t_3\right) = c$. Then $XY = YX$ and $Y^2 = \left(t_4^2 + t_2t_3\right) I_2$. Moreover,

$$aX^2 + bY^2 = at_1^2 I_2 + b\left(t_4^2 + t_2t_3\right) I_2 = \left(at_1^2 + b\left(t_4^2 + t_2t_3\right)\right) I_2 = cI_2.$$

Finally, suppose that $X = t_1 I_2 + \frac{u-c}{g}\begin{pmatrix} 0 & t_2 \\ t_3 & -k \end{pmatrix}$ and $Y = t_4 I_2 + \frac{va}{g}\begin{pmatrix} 0 & t_2 \\ t_3 & -k \end{pmatrix}$, where $t_1, t_2, t_3, t_4, u, v, k \in \mathbb{Z}$ satisfy the above conditions. Then $XY = YX$. Moreover,

$$\begin{aligned} aX^2 + bY^2 &= \left(at_1^2 + bt_4^2 + \frac{2act_2t_3}{g^2}(c - u)\right) I_2 + \frac{2a}{g^2}\left[(gt_1 + ck)(u - c) + vbgt_4\right]\begin{pmatrix} 0 & t_2 \\ t_3 & -k \end{pmatrix} \\ &= \left(at_1^2 + bt_4^2 + \frac{2act_2t_3}{g^2}(c - u)\right) I_2 = cI_2. \end{aligned}$$

We next prove necessity. Let $X = \begin{pmatrix} x_1 & x_2 \\ x_3 & x_4 \end{pmatrix}$ and $Y = \begin{pmatrix} y_1 & y_2 \\ y_3 & y_4 \end{pmatrix}$. Then the assumption $aX^2 + bY^2 = cI_2$ implies that $a^2X^2 + abY^2 = acI_2$. Since $XY = YX$, we have

$$\left(aX + \sqrt{-ab}Y\right)\left(aX - \sqrt{-ab}Y\right) = acI_2. \tag{16}$$

Note that

$$aX + \sqrt{-ab}Y = \begin{pmatrix} ax_1 + y_1\sqrt{-ab} & ax_2 + y_2\sqrt{-ab} \\ ax_3 + y_3\sqrt{-ab} & ax_4 + y_4\sqrt{-ab} \end{pmatrix}$$

and

$$aX - \sqrt{-ab}Y = \begin{pmatrix} ax_1 - y_1\sqrt{-ab} & ax_2 - y_2\sqrt{-ab} \\ ax_3 - y_3\sqrt{-ab} & ax_4 - y_4\sqrt{-ab} \end{pmatrix}.$$

By a direct computation, we have

$$\det\left(aX + \sqrt{-ab}Y\right) = a\left(u + v\sqrt{-ab}\right) \text{ and } \det\left(aX - \sqrt{-ab}Y\right) = a\left(u - v\sqrt{-ab}\right),$$

where $u = a(x_1x_4 - x_2x_3) - b(y_1y_4 - y_2y_3)$ and $v = x_1y_4 + x_4y_1 - x_2y_3 - x_3y_2$. By computing the determinants of both sides of (16), we have $u^2 + v^2ab = c^2$. From (16), it follows that

$$\left(aX + \sqrt{-ab}Y\right)^{-1} = \frac{1}{ac}\left(aX - \sqrt{-ab}Y\right) = \frac{1}{ac}\begin{pmatrix} ax_1 - y_1\sqrt{-ab} & ax_2 - y_2\sqrt{-ab} \\ ax_3 - y_3\sqrt{-ab} & ax_4 - y_4\sqrt{-ab} \end{pmatrix}. \tag{17}$$

Moreover,

$$\begin{aligned} \left(aX + \sqrt{-ab}Y\right)^{-1} &= \frac{1}{\det\left(aX + \sqrt{-ab}Y\right)}\operatorname{adj}\left(aX + \sqrt{-ab}Y\right) \\ &= \frac{1}{a\left(u + v\sqrt{-ab}\right)}\begin{pmatrix} ax_4 + y_4\sqrt{-ab} & -\left(ax_2 + y_2\sqrt{-ab}\right) \\ -\left(ax_3 + y_3\sqrt{-ab}\right) & ax_1 + y_1\sqrt{-ab} \end{pmatrix}, \end{aligned} \tag{18}$$

where $\operatorname{adj}\left(aX + \sqrt{-ab}Y\right)$ is the adjugate of $aX + \sqrt{-ab}Y$. Comparing (17) and (18), we have

$$\begin{cases} acx_1 + (-y_1c)\sqrt{-ab} = (aux_4 + vaby_4) + (uy_4 - avx_4)\sqrt{-ab}, & \text{(19a)} \\ (-acx_2) + y_2c\sqrt{-ab} = (aux_2 + vaby_2) + (uy_2 - avx_2)\sqrt{-ab}, & \text{(19b)} \\ (-acx_3) + y_3c\sqrt{-ab} = (aux_3 + vaby_3) + (uy_3 - avx_3)\sqrt{-ab}, & \text{(19c)} \\ acx_4 + (-y_4c)\sqrt{-ab} = (aux_1 + vaby_1) + (uy_1 - avx_1)\sqrt{-ab}. & \text{(19d)} \end{cases}$$

**Case 1:** $u \neq \pm c$.
Then $v \neq 0$. By (19b) and (19c), we have $y_2c = uy_2 - avx_2$ and $y_3c = uy_3 - avx_3$. Then

$$y_2 = \frac{av}{u - c}x_2 \text{ and } y_3 = \frac{av}{u - c}x_3. \tag{20}$$

From (19a) and (19d), it follows that $-y_1c = uy_4 - avx_4$ and $-y_4c = uy_1 - avx_1$, i.e.,

$$\begin{pmatrix} c & u \\ u & c \end{pmatrix}\begin{pmatrix} y_1 \\ y_4 \end{pmatrix} = \begin{pmatrix} avx_4 \\ avx_1 \end{pmatrix}.$$

Then we have

$$y_1 = \frac{av}{c^2 - u^2}(cx_4 - ux_1) \text{ and } y_4 = \frac{av}{c^2 - u^2}(cx_1 - ux_4). \tag{21}$$

Therefore, from (20), (21) and $u^2 + v^2ab = c^2$, it follows that

$$Y = \frac{av}{c^2 - u^2}\begin{pmatrix} cx_4 - ux_1 & -(u+c)x_2 \\ -(u+c)x_3 & cx_1 - ux_4 \end{pmatrix} = \frac{1}{vb}\begin{pmatrix} cx_4 - ux_1 & -(u+c)x_2 \\ -(u+c)x_3 & cx_1 - ux_4 \end{pmatrix}. \tag{22}$$

Since $Y \in M_2(\mathbb{Z})$, we have $y_i \in \mathbb{Z}$, $i = 1, 2, 3, 4$. Then

$$\begin{cases} vb \mid (cx_4 - ux_1), & \text{(23a)} \\ vb \mid (-(u+c)x_2), & \text{(23b)} \\ vb \mid (-(u+c)x_3), & \text{(23c)} \\ vb \mid (cx_1 - ux_4). & \text{(23d)} \end{cases}$$

From (23a) and (23d), we obtain $vb \mid (-(u+c)(x_1 - x_4))$. Then there is an integer $s$ such that $-(u+c)(x_1 - x_4) = vbs$. Since $u^2 + v^2ab = c^2$, we have

$$x_1 - x_4 = \frac{-vbs}{u+c} = \frac{vbs(u-c)}{c^2 - u^2} = \frac{s(u-c)}{va}.$$

Since $x_1 - x_4 \in \mathbb{Z}$, we obtain $va \mid (s(u-c))$. Let $g = \gcd(va, u-c)$. Then $\frac{va}{g} \mid s$. So there is an integer $k$ such that $s = \frac{va}{g}k$. Thus,

$$x_1 - x_4 = \frac{s(u-c)}{va} = \frac{va}{g}k \cdot \frac{(u-c)}{va} = \frac{u-c}{g}k. \tag{24}$$

Likewise, there are integers $t_2$ and $t_3$ such that

$$x_2 = \frac{u-c}{g}t_2 \text{ and } x_3 = \frac{u-c}{g}t_3. \tag{25}$$

From (24) and (25), we conclude that

$$X = x_1 I_2 + \frac{u-c}{g}\begin{pmatrix} 0 & t_2 \\ t_3 & -k \end{pmatrix}. \tag{26}$$

From $-(u+c)(x_1 - x_4) = vbs$, $s = \frac{va}{g}k$ and (22), it follows that

$$\frac{va}{g}k = s = \frac{-(u+c)(x_1 - x_4)}{vb} = \frac{cx_4 - ux_1 - (cx_1 - ux_4)}{vb} = y_1 - y_4. \tag{27}$$

From $x_2 = \frac{u-c}{g}t_2$, $u^2 + v^2ab = c^2$ and (22), it follows that

$$y_2 = \frac{-(u+c)x_2}{vb} = \frac{\left(c^2 - u^2\right)x_2}{vb(u-c)} = \frac{va}{u-c}x_2 = \frac{va}{u-c} \cdot \frac{u-c}{g}t_2 = \frac{va}{g}t_2. \tag{28}$$

Similarly, we obtain

$$y_3 = \frac{va}{g}t_3. \tag{29}$$

From (27), (28) and (29), we conclude that

$$Y = y_1 I_2 + \frac{va}{g}\begin{pmatrix} 0 & t_2 \\ t_3 & -k \end{pmatrix}. \tag{30}$$

By (26) and (30), we have

$$aX^2 + bY^2 = tI_2 + \frac{2a}{g^2} r \begin{pmatrix} 0 & t_2 \\ t_3 & -k \end{pmatrix},$$

where $t = ax_1^2 + by_1^2 + \frac{2act_2t_3}{g^2}(c-u)$ and $r = (gx_1 + ck)(u-c) + vbgy_1$. From the assumption $aX^2 + bY^2 = cI_2$, it follows that $t = c$ and $rk = rt_2 = rt_3 = 0$. If $k = t_2 = t_3 = 0$, then $X = x_1I_2$ and $Y = y_1I_2$, where $ax_1^2 + by_1^2 = c$. If $k$, $t_2$, $t_3$ are not all equal to zero, then $r = 0$ and $t = c$.

**Case 2:** $u = -c$.

Then $v = 0$. From (19a), (19b) and (19c), it follows that $x_1 = -x_4$, $y_1 = y_4$ and $y_2 = y_3 = 0$. Then $X = \begin{pmatrix} x_1 & x_2 \\ x_3 & -x_1 \end{pmatrix}$ and $Y = y_1I_2$. The assumption $aX^2 + bY^2 = cI_2$ implies that $a\left(x_1^2 + x_2x_3\right) + by_1^2 = c$. Note that the matrices and the condition which we obtain in this case can be obtained by taking $u = -c$ in Case 1. Indeed, let $u = -c$ in Case 1. Then $v = 0$ and $g = \gcd(va, u-c) = 2|c|$. By Case 1, we obtain

$$X = \begin{pmatrix} t_1 & -\frac{c}{|c|}t_2 \\ -\frac{c}{|c|}t_3 & -t_1 \end{pmatrix} \text{ and } Y = t_4I_2,$$

where $t_1, t_2, t_3, t_4 \in \mathbb{Z}$ satisfy $a\left(t_1^2 + t_2t_3\right) + bt_4^2 = c$. If $c > 0$, then let $t_1 = x_1$, $t_2 = -x_2$, $t_3 = -x_3$ and $t_4 = y_1$. Otherwise, let $t_1 = x_1$, $t_2 = x_2$, $t_3 = x_3$ and $t_4 = y_1$. Then we can obtain $X = \begin{pmatrix} x_1 & x_2 \\ x_3 & -x_1 \end{pmatrix}$ and $Y = y_1I_2$, where $a\left(x_1^2 + x_2x_3\right) + by_1^2 = c$.

**Case 3:** $u = c$.

Then $v = 0$. From (19a), (19b) and (19c), it follows that $x_1 = x_4$, $y_1 = -y_4$ and $x_2 = x_3 = 0$. Then $X = x_1I_2$ and $Y = \begin{pmatrix} y_1 & y_2 \\ y_3 & -y_1 \end{pmatrix}$. The assumption $aX^2 + bY^2 = cI_2$ implies that $ax_1^2 + b\left(y_1^2 + y_2y_3\right) = c$. □

About Theorem 4.1, we have the following equivalent statement.

**Theorem 4.2.** *Let $a$, $b$, $c$ be nonzero integers such that $-ab$ is not a square and $\gcd(a, b, c) = 1$. Let $X$ and $Y$ be $2 \times 2$-matrices over $\mathbb{Z}$. Then*

$$aX^2 + bY^2 = cI_2, \; XY = YX$$

*if and only if one of the following statements holds.*

(i) $X = t_1I_2$ *and* $Y = t_2I_2$, *where* $t_1, t_2 \in \mathbb{Z}$ *satisfy* $at_1^2 + bt_2^2 = c$;

(ii) $X = t_1I_2$ *and* $Y = \begin{pmatrix} t_4 & t_2 \\ t_3 & -t_4 \end{pmatrix}$, *where* $t_1, t_2, t_3, t_4 \in \mathbb{Z}$ *satisfy* $at_1^2 + b\left(t_4^2 + t_2t_3\right) = c$;

(iii) $X = \begin{pmatrix} t_1 & \frac{u-c}{g}t_2 \\ \frac{u-c}{g}t_3 & \frac{ut_1+vbt_4}{c} \end{pmatrix}$ *and* $Y = \begin{pmatrix} t_4 & \frac{va}{g}t_2 \\ \frac{va}{g}t_3 & \frac{vat_1-ut_4}{c} \end{pmatrix}$, *where* $t_1, t_2, t_3, t_4, u, v \in \mathbb{Z}$, $u \neq c$, $g = \gcd(va, u-c)$ *and the following relations hold:*

$$u^2 + v^2ab = c^2, \; at_1^2 + bt_4^2 + \frac{2act_2t_3}{g^2}(c-u) = c, \; c \mid (ut_1 + vbt_4), \; c \mid (vat_1 - ut_4).$$

*Proof.* We only need to show that (iii) is equivalent to Theorem 4.1 (iii).

We now prove sufficiency. By Theorem 4.1 (iii), we have $k = \frac{g}{c(c-u)}[(u-c)t_1 + vbt_4]$. Then

$$X = t_1I_2 + \frac{u-c}{g}\begin{pmatrix} 0 & t_2 \\ t_3 & -k \end{pmatrix} = \begin{pmatrix} t_1 & \frac{u-c}{g}t_2 \\ \frac{u-c}{g}t_3 & \frac{ut_1+vbt_4}{c} \end{pmatrix}$$

and

$$Y = t_4I_2 + \frac{va}{g}\begin{pmatrix} 0 & t_2 \\ t_3 & -k \end{pmatrix} = \begin{pmatrix} t_4 & \frac{va}{g}t_2 \\ \frac{va}{g}t_3 & \frac{vat_1-ut_4}{c} \end{pmatrix}.$$

Since $k \in \mathbb{Z}$, we have $c \mid (ut_1 + vbt_4)$ and $c \mid (vat_1 - ut_4)$.

We next prove necessity. By (iii), we have

$$X = \begin{pmatrix} t_1 & \frac{u-c}{g} t_2 \\ \frac{u-c}{g} t_3 & \frac{ut_1+vbt_4}{c} \end{pmatrix} = t_1 I_2 + \frac{u-c}{g} \begin{pmatrix} 0 & t_2 \\ t_3 & -k \end{pmatrix}$$

and

$$Y = \begin{pmatrix} t_4 & \frac{va}{g} t_2 \\ \frac{va}{g} t_3 & \frac{vat_1-ut_4}{c} \end{pmatrix} = t_4 I_2 + \frac{va}{g} \begin{pmatrix} 0 & t_2 \\ t_3 & -k \end{pmatrix},$$

where $k = \frac{g}{c(c-u)} [(u-c)\, t_1 + vbt_4]$. To complete the proof we need to show that $k \in \mathbb{Z}$ and $(gt_1 + ck)(u-c) + vbgt_4 = 0$. Since $c \mid (ut_1 + vbt_4)$ and $c \mid (vat_1 - ut_4)$, we have $\frac{u-c}{g}k,\ \frac{va}{g}k \in \mathbb{Z}$. Then $c \mid ((u-c)\, t_1 + vbt_4)$ and $\frac{c-u}{g} \mid \left(\frac{va}{g} \cdot \frac{(u-c)t_1+vbt_4}{c}\right)$. Since $\gcd\left(\frac{va}{g}, \frac{c-u}{g}\right) = 1$, we obtain $\frac{c-u}{g} \mid \frac{(u-c)t_1+vbt_4}{c}$. Hence, $k \in \mathbb{Z}$. Moreover, by a direct computation, we have $(gt_1 + ck)(u-c) + vbgt_4 = 0$. $\square$

By Theorem 4.2, we can get all solutions of some matrix equations for given nonzero integers $a$, $b$, $c$.

**Proposition 4.3.** *Let $p$ be a prime such that $p \equiv 3 \pmod 4$. Then all solutions of the matrix equations*

$$X^2 + Y^2 = \pm p I_2,\ X, Y \in M_2(\mathbb{Z}) \tag{31}$$

*are given by the following five parts.*

(i) $X = \begin{pmatrix} t_1 & t_2 \\ t_3 & -t_1 \end{pmatrix}$ *and* $Y = \begin{pmatrix} s_1 & s_2 \\ s_3 & -s_1 \end{pmatrix}$, *where* $t_1, t_2, t_3, s_1, s_2, s_3 \in \mathbb{Z}$ *satisfy* $t_1^2 + t_2t_3 + s_1^2 + s_2s_3 = \pm p$;

(ii) $X = t_1 I_2$ *and* $Y = \begin{pmatrix} t_4 & t_2 \\ t_3 & -t_4 \end{pmatrix}$, *where* $t_1, t_2, t_3, t_4 \in \mathbb{Z}$ *satisfy* $t_1^2 + t_4^2 + t_2t_3 = \pm p$;

(iii) $X = \begin{pmatrix} t_1 & t_2 \\ t_3 & -t_1 \end{pmatrix}$ *and* $Y = t_4 I_2$, *where* $t_1, t_2, t_3, t_4 \in \mathbb{Z}$ *satisfy* $t_1^2 + t_4^2 + t_2t_3 = \pm p$;

(iv) $X = \begin{pmatrix} t_1 & t_2 \\ t_3 & t_4 \end{pmatrix}$ *and* $Y = \begin{pmatrix} t_4 & -t_2 \\ -t_3 & t_1 \end{pmatrix}$, *where* $t_1, t_2, t_3, t_4 \in \mathbb{Z}$ *satisfy* $t_1^2 + t_4^2 + 2t_2t_3 = \pm p$;

(v) $X = \begin{pmatrix} t_1 & t_2 \\ t_3 & -t_4 \end{pmatrix}$ *and* $Y = \begin{pmatrix} t_4 & t_2 \\ t_3 & -t_1 \end{pmatrix}$, *where* $t_1, t_2, t_3, t_4 \in \mathbb{Z}$ *satisfy* $t_1^2 + t_4^2 + 2t_2t_3 = \pm p$.

*Proof.* We can prove this proposition simultaneously for the equations $X^2 + Y^2 = pI_2$ and $X^2 + Y^2 = -pI_2$, where the upper signs refer to the first equation and the lower signs refer to the second equation. From Proposition 2.8 1), it follows that all non-commutative solutions of equations (31) are given by (i). We next find commutative solutions of equations (31). By Theorem 4.2, we only need to consider the following three cases.

**Case 1:** $X = t_1 I_2$ and $Y = t_2 I_2$, where $t_1, t_2 \in \mathbb{Z}$ satisfy $t_1^2 + t_2^2 = \pm p$.

Obviously, $t_1^2 + t_2^2 = -p$ is impossible. Since $p$ is a prime such that $p \equiv 3 \pmod 4$, it follows that $p$ cannot be represented as a sum of two squares. This means that $t_1^2 + t_2^2 = p$ is impossible. Therefore, this case is impossible.

**Case 2:** $X = t_1 I_2$ and $Y = \begin{pmatrix} t_4 & t_2 \\ t_3 & -t_4 \end{pmatrix}$, where $t_1, t_2, t_3, t_4 \in \mathbb{Z}$ satisfy $t_1^2 + t_4^2 + t_2t_3 = \pm p$.

Then we can get the solutions (ii) in this case.

**Case 3:** $X = \begin{pmatrix} t_1 & \frac{u \mp p}{g} t_2 \\ \frac{u \mp p}{g} t_3 & \frac{ut_1 + vt_4}{\pm p} \end{pmatrix}$ and $Y = \begin{pmatrix} t_4 & \frac{v}{g} t_2 \\ \frac{v}{g} t_3 & \frac{vt_1 - ut_4}{\pm p} \end{pmatrix}$, where $t_1, t_2, t_3, t_4, u, v \in \mathbb{Z}$, $u \neq \pm p$, $g = \gcd(v, u \mp p)$ and the following relations hold:

$$u^2 + v^2 = p^2,\ t_1^2 + t_4^2 + \frac{2pt_2t_3}{g^2}(p \mp u) = \pm p,\ p \mid (ut_1 + vt_4),\ p \mid (vt_1 - ut_4).$$

In this case, we need to solve the Diophantine equation $u^2 + v^2 = p^2$ in integers $u, v$. Note that $p$ is a prime such that $p \equiv 3 \pmod 4$. Then it follows from $u^2 + v^2 = p^2$ that $p \mid u$ and $p \mid v$. Thus, we obtain $(u, v) \in \{(\mp p, 0), (0, p), (0, -p)\}$.

We now consider the matrix equation $X^2 + Y^2 = pI_2$. Then we have

$$(u, v) \in \{(-p, 0), (0, p), (0, -p)\}.$$

For $(u, v) = (-p, 0)$, we have $X = \begin{pmatrix} t_1 & t_2 \\ t_3 & -t_1 \end{pmatrix}$ and $Y = t_4 I_2$, where $t_1, t_2, t_3, t_4 \in \mathbb{Z}$ satisfy $t_1^2 + t_4^2 + t_2 t_3 = p$. For $(u, v) = (0, p)$, we have $X = \begin{pmatrix} t_1 & t_2 \\ t_3 & t_4 \end{pmatrix}$ and $Y = \begin{pmatrix} t_4 & -t_2 \\ -t_3 & t_1 \end{pmatrix}$, where $t_1, t_2, t_3, t_4 \in \mathbb{Z}$ satisfy $t_1^2 + t_4^2 + 2t_2 t_3 = p$. For $(u, v) = (0, -p)$, we have $X = \begin{pmatrix} t_1 & t_2 \\ t_3 & -t_4 \end{pmatrix}$ and $Y = \begin{pmatrix} t_4 & t_2 \\ t_3 & -t_1 \end{pmatrix}$, where $t_1, t_2, t_3, t_4 \in \mathbb{Z}$ satisfy $t_1^2 + t_4^2 + 2t_2 t_3 = p$.

We next consider the matrix equation $X^2 + Y^2 = -pI_2$. Then we obtain

$$(u, v) \in \{(p, 0), (0, -p), (0, p)\}.$$

For $(u, v) = (p, 0)$, we have $X = \begin{pmatrix} t_1 & t_2 \\ t_3 & -t_1 \end{pmatrix}$ and $Y = t_4 I_2$, where $t_1, t_2, t_3, t_4 \in \mathbb{Z}$ satisfy $t_1^2 + t_4^2 + t_2 t_3 = -p$. For $(u, v) = (0, -p)$, we have $X = \begin{pmatrix} t_1 & t_2 \\ t_3 & t_4 \end{pmatrix}$ and $Y = \begin{pmatrix} t_4 & -t_2 \\ -t_3 & t_1 \end{pmatrix}$, where $t_1, t_2, t_3, t_4 \in \mathbb{Z}$ satisfy $t_1^2 + t_4^2 + 2t_2 t_3 = -p$. For $(u, v) = (0, p)$, we have $X = \begin{pmatrix} t_1 & t_2 \\ t_3 & -t_4 \end{pmatrix}$ and $Y = \begin{pmatrix} t_4 & t_2 \\ t_3 & -t_1 \end{pmatrix}$, where $t_1, t_2, t_3, t_4 \in \mathbb{Z}$ satisfy $t_1^2 + t_4^2 + 2t_2 t_3 = -p$. □

**Proposition 4.4.** *Let $p$ be a prime such that $p \equiv 5 \text{ or } 7 \pmod 8$. Then all solutions of the matrix equations*

$$X^2 + 2Y^2 = \pm pI_2,\ X, Y \in M_2(\mathbb{Z}) \tag{32}$$

*are given by the following three parts.*

(i) $X = \begin{pmatrix} t_1 & t_2 \\ t_3 & -t_1 \end{pmatrix}$ *and* $Y = \begin{pmatrix} s_1 & s_2 \\ s_3 & -s_1 \end{pmatrix}$*, where $t_1, t_2, t_3, s_1, s_2, s_3 \in \mathbb{Z}$ satisfy $t_1^2 + t_2 t_3 + 2\left(s_1^2 + s_2 s_3\right) = \pm p$;*

(ii) $X = t_1 I_2$ *and* $Y = \begin{pmatrix} t_4 & t_2 \\ t_3 & -t_4 \end{pmatrix}$*, where $t_1, t_2, t_3, t_4 \in \mathbb{Z}$ satisfy $t_1^2 + 2\left(t_4^2 + t_2 t_3\right) = \pm p$;*

(iii) $X = \begin{pmatrix} t_1 & t_2 \\ t_3 & -t_1 \end{pmatrix}$ *and $Y = t_4 I_2$, where $t_1, t_2, t_3, t_4 \in \mathbb{Z}$ satisfy $t_1^2 + t_2 t_3 + 2t_4^2 = \pm p$.*

*Proof.* We can prove this proposition simultaneously for the equations $X^2 + 2Y^2 = pI_2$ and $X^2 + 2Y^2 = -pI_2$, where the upper signs refer to the first equation and the lower signs refer to the second equation. From Proposition 2.8 1), it follows that all non-commutative solutions of equations (32) are given by (i). We next find commutative solutions of equations (32). By Theorem 4.2, we only need to consider the following three cases.

**Case 1:** $X = t_1 I_2$ and $Y = t_2 I_2$, where $t_1, t_2 \in \mathbb{Z}$ satisfy $t_1^2 + 2t_2^2 = \pm p$.

Obviously, $t_1^2 + 2t_2^2 = -p$ is impossible. We claim that $t_1^2 + 2t_2^2 = p$ is also impossible. Indeed, if $t_1^2 + 2t_2^2 = p$, then $\gcd(p, t_1 t_2) = 1$. Otherwise, we have $p \mid t_1$ and $p \mid t_2$. This is impossible by $t_1^2 + 2t_2^2 = p$. So $\gcd(p, t_1 t_2) = 1$. Then there is an integer $t_2'$ such that $t_2 t_2' \equiv 1 \pmod p$. From $t_1^2 + 2t_2^2 = p$, it follows that $\left(t_1 t_2'\right)^2 + 2\left(t_2 t_2'\right)^2 = p\left(t_2'\right)^2$. Then $\left(t_1 t_2'\right)^2 \equiv -2 \pmod p$. This means that $\left(\frac{-2}{p}\right) = 1$, where $\left(\frac{\cdot}{p}\right)$ is the Legendre symbol. However, for $p \equiv 5 \text{ or } 7 \pmod 8$, we have $\left(\frac{-2}{p}\right) = -1$, a contradiction.

**Case 2:** $X = t_1 I_2$ and $Y = \begin{pmatrix} t_4 & t_2 \\ t_3 & -t_4 \end{pmatrix}$, where $t_1, t_2, t_3, t_4 \in \mathbb{Z}$ satisfy $t_1^2 + 2\left(t_4^2 + t_2 t_3\right) = \pm p$.

Then we can get the solutions (ii) in this case.

**Case 3:** $X = \begin{pmatrix} t_1 & \frac{u\mp p}{g}t_2 \\ \frac{u\mp p}{g}t_3 & \frac{ut_1+2vt_4}{\pm p} \end{pmatrix}$ and $Y = \begin{pmatrix} t_4 & \frac{v}{g}t_2 \\ \frac{v}{g}t_3 & \frac{vt_1-ut_4}{\pm p} \end{pmatrix}$, where $t_1, t_2, t_3, t_4, u, v \in \mathbb{Z}$, $u \neq \pm p$, $g = \gcd(v, u \mp p)$ and the following relations hold:

$$u^2 + 2v^2 = p^2,\ t_1^2 + 2t_4^2 + \frac{2pt_2t_3}{g^2}(p \mp u) = \pm p,\ p \mid (ut_1 + 2vt_4),\ p \mid (vt_1 - ut_4).$$

In this case, we need to solve the Diophantine equation $u^2 + 2v^2 = p^2$ in integers $u, v$. From $u^2 + 2v^2 = p^2$, it follows that $2 \mid (p-u)(p+u)$. Then $p$ and $u$ have the same parity. Moreover, $2 \mid v$. By $u^2 + 2v^2 = p^2$, we have

$$2\left(\frac{v}{2}\right)^2 = \frac{p-u}{2} \cdot \frac{p+u}{2}. \tag{33}$$

If $v = 0$, then we obtain $(u, v) = (\mp p, 0)$. Let us now assume that $v \neq 0$. Let $g = \gcd\left(\frac{p-u}{2}, \frac{p+u}{2}\right)$. Then $g \mid p$. If $g = 1$, then it follows from (33) that there are integers $y_1$ and $y_2$ such that

$$\frac{p-u}{2} = 2y_1^2,\ \frac{p+u}{2} = y_2^2 \text{ or } \frac{p-u}{2} = y_1^2,\ \frac{p+u}{2} = 2y_2^2.$$

Then we have $p = 2y_1^2 + y_2^2$ or $p = y_1^2 + 2y_2^2$, which is impossible by the argument of Case 1. Therefore, $g = p$. Then $p \mid u$, so $p \mid v$. From $u^2 + 2v^2 = p^2$, it follows that $(u, v) = (\mp p, 0)$. Then we have $X = \begin{pmatrix} t_1 & t_2 \\ t_3 & -t_1 \end{pmatrix}$ and $Y = t_4 I_2$, where $t_1, t_2, t_3, t_4 \in \mathbb{Z}$ satisfy $t_1^2 + t_2t_3 + 2t_4^2 = \pm p$. □

Let $c = \pm 1$ in Theorem 4.2. Then we have the following corollary.

**Corollary 4.5.** *Let $a, b$ be nonzero integers such that $-ab$ is not a square and let $X, Y \in M_2(\mathbb{Z})$. Then*

$$aX^2 + bY^2 = \pm I_2,\ XY = YX$$

*if and only if one of the following statements holds.*

(i) $X = t_1 I_2$ *and* $Y = t_2 I_2$, *where* $t_1, t_2 \in \mathbb{Z}$ *satisfy* $at_1^2 + bt_2^2 = \pm 1$;

(ii) $X = t_1 I_2$ *and* $Y = \begin{pmatrix} t_4 & t_2 \\ t_3 & -t_4 \end{pmatrix}$, *where* $t_1, t_2, t_3, t_4 \in \mathbb{Z}$ *satisfy* $at_1^2 + b\left(t_4^2 + t_2t_3\right) = \pm 1$;

(iii) $X = \begin{pmatrix} t_1 & \frac{u\mp 1}{g}t_2 \\ \frac{u\mp 1}{g}t_3 & \pm(ut_1 + vbt_4) \end{pmatrix}$ *and* $Y = \begin{pmatrix} t_4 & \frac{va}{g}t_2 \\ \frac{va}{g}t_3 & \pm(vat_1 - ut_4) \end{pmatrix}$, *where* $t_1, t_2, t_3, t_4, u, v \in \mathbb{Z}$, $u \neq \pm 1$, $g = \gcd(va, u \mp 1)$ *and the following relations hold:*

$$u^2 + v^2ab = 1,\ at_1^2 + bt_4^2 + \frac{2at_2t_3}{g^2}(1 \mp u) = \pm 1.$$

**Remark 4.6.** Let $d$ be a square-free integer and let $a = 1$, $b = -d$. Then Corollary 4.5 becomes [3, Theorem 2.1].

By Corollary 4.5, we have the following proposition.

**Proposition 4.7.** *Let $b$ be a nonzero integer such that $-b$ is not a square. Suppose that $b$ has a prime divisor of the form $4k + 3$. Then all solutions of the matrix equation*

$$X^2 + bY^2 = -I_2,\ X, Y \in M_2(\mathbb{Z}) \tag{34}$$

*are given by the following two parts.*

(i) $X = \begin{pmatrix} t_1 & t_2 \\ t_3 & -t_1 \end{pmatrix}$ *and* $Y = \begin{pmatrix} s_1 & s_2 \\ s_3 & -s_1 \end{pmatrix}$, *where* $t_1, t_2, t_3, s_1, s_2, s_3 \in \mathbb{Z}$ *satisfy* $t_1^2 + t_2t_3 + b\left(s_1^2 + s_2s_3\right) = -1$;

(ii) *For* $b > 0$, *let* $X = \begin{pmatrix} t_1 & t_2 \\ t_3 & -t_1 \end{pmatrix}$ *and* $Y = t_4I_2$, *where* $t_1, t_2, t_3, t_4 \in \mathbb{Z}$ *satisfy* $t_1^2+t_2t_3+bt_4^2 = -1$. *Otherwise, let* $X = \begin{pmatrix} t_1 & \frac{u+1}{g}t_2 \\ \frac{u+1}{g}t_3 & -(ut_1 + vbt_4) \end{pmatrix}$ *and* $Y = \begin{pmatrix} t_4 & \frac{v}{g}t_2 \\ \frac{v}{g}t_3 & ut_4 - vt_1 \end{pmatrix}$, *where* $t_1, t_2, t_3, t_4, u, v \in \mathbb{Z}$, $u \neq -1$, $g = \gcd(v, u + 1)$ *and the following relations hold:*

$$u^2 + v^2b = 1,\ t_1^2 + bt_4^2 + \frac{2t_2t_3}{g^2}(1 + u) = -1.$$

*Proof.* From Proposition 2.8 1), it follows that all non-commutative solutions of equation (34) are given by (i). We next find commutative solutions of equation (34). Suppose that $p \equiv 3 \pmod 4$ is the prime divisor of $b$. Then $\left(\frac{-1}{p}\right) = -1$, where $\left(\frac{\cdot}{p}\right)$ is the Legendre symbol. By Corollary 4.5, we only need to consider the following three cases.

**Case 1:** $X = t_1I_2$ and $Y = t_2I_2$, where $t_1, t_2 \in \mathbb{Z}$ satisfy $t_1^2 + bt_2^2 = -1$.

We claim that $t_1^2 + bt_2^2 = -1$ is impossible. Indeed, if $t_1^2 + bt_2^2 = -1$, then $t_1^2 \equiv -1 \pmod p$. This means that $\left(\frac{-1}{p}\right) = 1$, a contradiction.

**Case 2:** $X = t_1I_2$ and $Y = \begin{pmatrix} t_4 & t_2 \\ t_3 & -t_4 \end{pmatrix}$, where $t_1, t_2, t_3, t_4 \in \mathbb{Z}$ satisfy $t_1^2 + b\left(t_4^2 + t_2t_3\right) = -1$.

However, this case is also impossible, where the reason is similar to Case 1.

**Case 3:** $X = \begin{pmatrix} t_1 & \frac{u+1}{g}t_2 \\ \frac{u+1}{g}t_3 & -(ut_1 + vbt_4) \end{pmatrix}$ and $Y = \begin{pmatrix} t_4 & \frac{v}{g}t_2 \\ \frac{v}{g}t_3 & ut_4 - vt_1 \end{pmatrix}$, where $t_1, t_2, t_3, t_4, u, v \in \mathbb{Z}$, $u \neq -1$, $g = \gcd(v, u + 1)$ and the following relations hold:

$$u^2 + v^2b = 1,\ t_1^2 + bt_4^2 + \frac{2t_2t_3}{g^2}(1 + u) = -1.$$

If $b > 0$, then it follows from $u^2 + v^2b = 1$ that $u = 1$ and $v = 0$. Then we have $X = \begin{pmatrix} t_1 & t_2 \\ t_3 & -t_1 \end{pmatrix}$ and $Y = t_4I_2$, where $t_1, t_2, t_3, t_4 \in \mathbb{Z}$ satisfy $t_1^2 + t_2t_3 + bt_4^2 = -1$. If $b < 0$, then $u^2 + v^2b = 1$ is the Pell's equation. We know that it has infinitely many solutions in integers $u$ and $v$. □

**Example 4.8.** Let $b = -3$ in Proposition 4.7. Then all solutions of the matrix equation

$$X^2 - 3Y^2 = -I_2,\ X, Y \in M_2(\mathbb{Z}) \tag{35}$$

are given by the following two parts.

(i) $X = \begin{pmatrix} t_1 & t_2 \\ t_3 & -t_1 \end{pmatrix}$ and $Y = \begin{pmatrix} s_1 & s_2 \\ s_3 & -s_1 \end{pmatrix}$, where $t_1, t_2, t_3, s_1, s_2, s_3 \in \mathbb{Z}$ satisfy $t_1^2 + t_2t_3 - 3\left(s_1^2 + s_2s_3\right) = -1$;

(ii) $X = \begin{pmatrix} t_1 & \frac{u+1}{g}t_2 \\ \frac{u+1}{g}t_3 & 3vt_4 - ut_1 \end{pmatrix}$ and $Y = \begin{pmatrix} t_4 & \frac{v}{g}t_2 \\ \frac{v}{g}t_3 & ut_4 - vt_1 \end{pmatrix}$, where $t_1, t_2, t_3, t_4, u, v \in \mathbb{Z}$, $u \neq -1$, $g = \gcd(v, u + 1)$ and the following relations hold:

$$u^2 - 3v^2 = 1,\ t_1^2 - 3t_4^2 + \frac{2t_2t_3}{g^2}(1 + u) = -1.$$

For example, let $u = 7$ and $v = 4$ in (ii). Then we can get a family of solutions to equation (35):

$$\begin{pmatrix} t_1 & 2t_2 \\ 2t_3 & 12t_4 - 7t_1 \end{pmatrix}^2 - 3\begin{pmatrix} t_4 & t_2 \\ t_3 & 7t_4 - 4t_1 \end{pmatrix}^2 = -I_2,$$

where $t_1, t_2, t_3, t_4 \in \mathbb{Z}$ satisfy $t_1^2 - 3t_4^2 + t_2t_3 = -1$.

Let $c = \pm 2$ in Theorem 4.2. Then we have the following corollary.

**Corollary 4.9.** *Let $a$, $b$ be nonzero integers such that $-ab$ is not a square and let $X, Y \in M_2(\mathbb{Z})$. Then*

$$aX^2 + bY^2 = \pm 2I_2,\ XY = YX$$

*if and only if one of the following statements holds.*

(i) $X = t_1 I_2$ *and* $Y = t_2 I_2$, *where* $t_1, t_2 \in \mathbb{Z}$ *satisfy* $at_1^2 + bt_2^2 = \pm 2$;

(ii) $X = t_1 I_2$ *and* $Y = \begin{pmatrix} t_4 & t_2 \\ t_3 & -t_4 \end{pmatrix}$, *where* $t_1, t_2, t_3, t_4 \in \mathbb{Z}$ *satisfy* $at_1^2 + b\left(t_4^2 + t_2 t_3\right) = \pm 2$;

(iii) $X = \begin{pmatrix} t_1 & \frac{u\mp 2}{g} t_2 \\ \frac{u\mp 2}{g} t_3 & \frac{ut_1 + vbt_4}{\pm 2} \end{pmatrix}$ *and* $Y = \begin{pmatrix} t_4 & \frac{va}{g} t_2 \\ \frac{va}{g} t_3 & \frac{vat_1 - ut_4}{\pm 2} \end{pmatrix}$, *where* $t_1, t_2, t_3, t_4, u, v \in \mathbb{Z}$, $u \neq \pm 2$, $g = \gcd(va, u \mp 2)$ *and the following relations hold:*

$$u^2 + v^2 ab = 4,\ at_1^2 + bt_4^2 + \frac{4at_2t_3}{g^2}(2 \mp u) = \pm 2.$$

*Proof.* By Theorem 4.2, we only need to show that $2 \mid (ut_1 + vbt_4)$ and $2 \mid (vat_1 - ut_4)$ in (iii). To see that $g = \gcd(va, u \mp 2)$, the proof is divided into the following two cases, depending on whether $g$ is even or not.

**Case 1:** $2 \mid g$.

Then $2 \mid va$ and $2 \mid u$. Therefore, $2 \mid (vat_1 - ut_4)$. If $2 \mid v$, then $2 \mid (ut_1 + vbt_4)$. Otherwise, by $u^2 + v^2 ab = 4$, we have $4 \mid ab$. If $2 \mid b$, then $2 \mid (ut_1 + vbt_4)$. If $2 \nmid b$, then $2 \mid a$. From $at_1^2 + bt_4^2 + \frac{4at_2t_3}{g^2}(2 \mp u) = \pm 2$, it follows that $vat_1^2 + vbt_4^2 + \frac{4vat_2t_3}{g^2}(2 \mp u) = \pm 2v$. Then $2 \mid t_4$, so $2 \mid (ut_1 + vbt_4)$.

**Case 2:** $2 \nmid g$.

From $t_1, t_2, t_3, t_4, u, v \in \mathbb{Z}$ and $at_1^2 + bt_4^2 + \frac{4at_2t_3}{g^2}(2 \mp u) = \pm 2$, it follows that $g^2 \mid 4at_2t_3(2 \mp u)$. Since $2 \nmid g$, we obtain $g^2 \mid at_2t_3(2 \mp u)$. Then from $u^2 + v^2ab = 4$ and $at_1^2 + bt_4^2 + \frac{4at_2t_3}{g^2}(2 \mp u) = \pm 2$, it follows that

$$u^2 + v^2 ab \equiv 0 \pmod 4 \text{ and } at_1^2 + bt_4^2 \equiv 0 \pmod 2. \tag{36}$$

If $2 \mid u$, then it follows from (36) and $2 \nmid g$ that $2 \nmid va$, $2 \mid b$ and $2 \mid t_1$. In this case, we have $2 \mid (ut_1 + vbt_4)$ and $2 \mid (vat_1 - ut_4)$. If $2 \nmid u$, then it follows from (36) that $2 \nmid v$ and $2 \nmid ab$. Then $t_1$ and $t_4$ have the same parity. Therefore, in this case, we have

$$ut_1 + vbt_4 \equiv t_1 + t_4 \equiv 0 \pmod 2 \text{ and } vat_1 - ut_4 \equiv t_1 + t_4 \equiv 0 \pmod 2.$$

□

By Corollary 4.9, we have the following two propositions.

**Proposition 4.10.** *Let $b \neq 3$ be a nonzero integer such that $-b$ is not a square. Suppose that $b$ has a prime divisor of the form $8k + 3$ or $8k + 5$. Then all solutions of the matrix equation*

$$X^2 + bY^2 = 2I_2,\ X, Y \in M_2(\mathbb{Z}) \tag{37}$$

*are given by the following two parts.*

(i) $X = \begin{pmatrix} t_1 & t_2 \\ t_3 & -t_1 \end{pmatrix}$ *and* $Y = \begin{pmatrix} s_1 & s_2 \\ s_3 & -s_1 \end{pmatrix}$, *where* $t_1, t_2, t_3, s_1, s_2, s_3 \in \mathbb{Z}$ *satisfy* $t_1^2 + t_2t_3 + b\left(s_1^2 + s_2s_3\right) = 2$;

(ii) *For* $b>0$, *let* $X=\begin{pmatrix} t_1 & t_2 \\ t_3 & -t_1 \end{pmatrix}$ *and* $Y=t_4I_2$, *where* $t_1, t_2, t_3, t_4\in\mathbb{Z}$ *satisfy* $t_1^2+t_2t_3+bt_4^2=2$. *Otherwise, let* $X=\begin{pmatrix} t_1 & \frac{u-2}{g}t_2 \\ \frac{u-2}{g}t_3 & \frac{ut_1+vbt_4}{2} \end{pmatrix}$ *and* $Y=\begin{pmatrix} t_4 & \frac{v}{g}t_2 \\ \frac{v}{g}t_3 & \frac{vt_1-ut_4}{2} \end{pmatrix}$, *where* $t_1, t_2, t_3, t_4, u, v\in\mathbb{Z}$, $u\neq 2$, $g=\gcd(v, u-2)$ *and the following relations hold:*

$$u^2+v^2b=4,\ t_1^2+bt_4^2+\frac{4t_2t_3}{g^2}(2-u)=2.$$

*Proof.* From Proposition 2.8 1), it follows that all non-commutative solutions of equation (37) are given by (i). We next find commutative solutions of equation (37). Suppose that $p\equiv 3\,\text{or}\,5 \pmod 8$ is the prime divisor of $b$. Then $\left(\frac{2}{p}\right)=-1$, where $\left(\frac{\cdot}{p}\right)$ is the Legendre symbol. By Corollary 4.9, we only need to consider the following three cases.

**Case 1:** $X=t_1I_2$ and $Y=t_2I_2$, where $t_1, t_2\in\mathbb{Z}$ satisfy $t_1^2+bt_2^2=2$.

We claim that $t_1^2+bt_2^2=2$ is impossible. Indeed, if $t_1^2+bt_2^2=2$, then $t_1^2\equiv 2 \pmod p$. This means that $\left(\frac{2}{p}\right)=1$, a contradiction.

**Case 2:** $X=t_1I_2$ and $Y=\begin{pmatrix} t_4 & t_2 \\ t_3 & -t_4 \end{pmatrix}$, where $t_1, t_2, t_3, t_4\in\mathbb{Z}$ satisfy $t_1^2+b\left(t_4^2+t_2t_3\right)=2$.

However, this case is also impossible, where the reason is similar to Case 1.

**Case 3:** $X=\begin{pmatrix} t_1 & \frac{u-2}{g}t_2 \\ \frac{u-2}{g}t_3 & \frac{ut_1+vbt_4}{2} \end{pmatrix}$ and $Y=\begin{pmatrix} t_4 & \frac{v}{g}t_2 \\ \frac{v}{g}t_3 & \frac{vt_1-ut_4}{2} \end{pmatrix}$, where $t_1, t_2, t_3, t_4, u, v\in\mathbb{Z}$, $u\neq 2$, $g=\gcd(v, u-2)$ and the following relations hold:

$$u^2+v^2b=4,\ t_1^2+bt_4^2+\frac{4t_2t_3}{g^2}(2-u)=2.$$

If $b>0$, then it follows from $u^2+v^2b=4$ that $u=-2$ and $v=0$. Then we have $X=\begin{pmatrix} t_1 & t_2 \\ t_3 & -t_1 \end{pmatrix}$ and $Y=t_4I_2$, where $t_1, t_2, t_3, t_4\in\mathbb{Z}$ satisfy $t_1^2+t_2t_3+bt_4^2=2$. If $b<0$, then $u^2+v^2b=4$ is the Pell's equation. We know that it has infinitely many solutions in integers $u$ and $v$. □

**Example 4.11.** Let $b=-5$ in Proposition 4.10. Then all solutions of the matrix equation

$$X^2-5Y^2=2I_2,\ X, Y\in M_2(\mathbb{Z}) \tag{38}$$

are given by the following two parts.

(i) $X=\begin{pmatrix} t_1 & t_2 \\ t_3 & -t_1 \end{pmatrix}$ and $Y=\begin{pmatrix} s_1 & s_2 \\ s_3 & -s_1 \end{pmatrix}$, where $t_1, t_2, t_3, s_1, s_2, s_3\in\mathbb{Z}$ satisfy $t_1^2+t_2t_3-5\left(s_1^2+s_2s_3\right)=2$;

(ii) $X=\begin{pmatrix} t_1 & \frac{u-2}{g}t_2 \\ \frac{u-2}{g}t_3 & \frac{ut_1-5vt_4}{2} \end{pmatrix}$ and $Y=\begin{pmatrix} t_4 & \frac{v}{g}t_2 \\ \frac{v}{g}t_3 & \frac{vt_1-ut_4}{2} \end{pmatrix}$, where $t_1, t_2, t_3, t_4, u, v\in\mathbb{Z}$, $u\neq 2$, $g=\gcd(v, u-2)$ and the following relations hold:

$$u^2-5v^2=4,\ t_1^2-5t_4^2+\frac{4t_2t_3}{g^2}(2-u)=2.$$

For example, let $u=18$ and $v=8$ in (ii). Then we can get a family of solutions to equation (38):

$$\begin{pmatrix} t_1 & 2t_2 \\ 2t_3 & 9t_1-20t_4 \end{pmatrix}^2-5\begin{pmatrix} t_4 & t_2 \\ t_3 & 4t_1-9t_4 \end{pmatrix}^2=2I_2,$$

where $t_1, t_2, t_3, t_4\in\mathbb{Z}$ satisfy $t_1^2-5t_4^2-t_2t_3=2$.

**Proposition 4.12.** *Let $b$ be a nonzero integer such that $-b$ is not a square. Suppose that $b$ has a prime divisor of the form $8k+5$ or $8k+7$. Then all solutions of the matrix equation*

$$X^2 + bY^2 = -2I_2,\ X,\ Y \in M_2(\mathbb{Z}) \tag{39}$$

*are given by the following two parts.*

(i) $X = \begin{pmatrix} t_1 & t_2 \\ t_3 & -t_1 \end{pmatrix}$ *and* $Y = \begin{pmatrix} s_1 & s_2 \\ s_3 & -s_1 \end{pmatrix}$, *where* $t_1, t_2, t_3, s_1, s_2, s_3 \in \mathbb{Z}$ *satisfy* $t_1^2 + t_2t_3 + b\left(s_1^2 + s_2s_3\right) = -2$;

(ii) *For* $b > 0$, *let* $X = \begin{pmatrix} t_1 & t_2 \\ t_3 & -t_1 \end{pmatrix}$ *and* $Y = t_4I_2$, *where* $t_1, t_2, t_3, t_4 \in \mathbb{Z}$ *satisfy* $t_1^2 + t_2t_3 + bt_4^2 = -2$. *Otherwise, let* $X = \begin{pmatrix} t_1 & \frac{u+2}{g}t_2 \\ \frac{u+2}{g}t_3 & \frac{ut_1+vbt_4}{-2} \end{pmatrix}$ *and* $Y = \begin{pmatrix} t_4 & \frac{v}{g}t_2 \\ \frac{v}{g}t_3 & \frac{vt_1-ut_4}{-2} \end{pmatrix}$, *where* $t_1, t_2, t_3, t_4, u, v \in \mathbb{Z}$, $u \neq -2$, $g = \gcd(v, u+2)$ *and the following relations hold:*

$$u^2 + v^2b = 4,\ t_1^2 + bt_4^2 + \frac{4t_2t_3}{g^2}(2+u) = -2.$$

*Proof.* From Proposition 2.8 1), it follows that all non-commutative solutions of equation (39) are given by (i). We next find commutative solutions of equation (39). Suppose that $p \equiv 5 \text{ or } 7 \pmod 8$ is the prime divisor of $b$. Then $\left(\frac{-2}{p}\right) = -1$, where $\left(\frac{\cdot}{p}\right)$ is the Legendre symbol. By Corollary 4.9, we only need to consider the following three cases.

**Case 1:** $X = t_1I_2$ and $Y = t_2I_2$, where $t_1, t_2 \in \mathbb{Z}$ satisfy $t_1^2 + bt_2^2 = -2$.

We claim that $t_1^2 + bt_2^2 = -2$ is impossible. Indeed, if $t_1^2 + bt_2^2 = -2$, then $t_1^2 \equiv -2 \pmod p$. This means that $\left(\frac{-2}{p}\right) = 1$, a contradiction.

**Case 2:** $X = t_1I_2$ and $Y = \begin{pmatrix} t_4 & t_2 \\ t_3 & -t_4 \end{pmatrix}$, where $t_1, t_2, t_3, t_4 \in \mathbb{Z}$ satisfy $t_1^2 + b\left(t_4^2 + t_2t_3\right) = -2$.

However, this case is also impossible, where the reason is similar to Case 1.

**Case 3:** $X = \begin{pmatrix} t_1 & \frac{u+2}{g}t_2 \\ \frac{u+2}{g}t_3 & \frac{ut_1+vbt_4}{-2} \end{pmatrix}$ and $Y = \begin{pmatrix} t_4 & \frac{v}{g}t_2 \\ \frac{v}{g}t_3 & \frac{vt_1-ut_4}{-2} \end{pmatrix}$, where $t_1, t_2, t_3, t_4, u, v \in \mathbb{Z}$, $u \neq -2$, $g = \gcd(v, u+2)$ and the following relations hold:

$$u^2 + v^2b = 4,\ t_1^2 + bt_4^2 + \frac{4t_2t_3}{g^2}(2+u) = -2.$$

If $b > 0$, then it follows from $u^2 + v^2b = 4$ that $u = 2$ and $v = 0$. Then we have $X = \begin{pmatrix} t_1 & t_2 \\ t_3 & -t_1 \end{pmatrix}$ and $Y = t_4I_2$, where $t_1, t_2, t_3, t_4 \in \mathbb{Z}$ satisfy $t_1^2 + t_2t_3 + bt_4^2 = -2$. If $b < 0$, then $u^2 + v^2b = 4$ is the Pell's equation. We know that it has infinitely many solutions in integers $u$ and $v$. □

**Example 4.13.** Let $b = -5$ in Proposition 4.12. Then all solutions of the matrix equation

$$X^2 - 5Y^2 = -2I_2,\ X,\ Y \in M_2(\mathbb{Z}) \tag{40}$$

are given by the following two parts.

(i) $X = \begin{pmatrix} t_1 & t_2 \\ t_3 & -t_1 \end{pmatrix}$ and $Y = \begin{pmatrix} s_1 & s_2 \\ s_3 & -s_1 \end{pmatrix}$, where $t_1, t_2, t_3, s_1, s_2, s_3 \in \mathbb{Z}$ satisfy $t_1^2 + t_2t_3 - 5\left(s_1^2 + s_2s_3\right) = -2$;

(ii) $X = \begin{pmatrix} t_1 & \frac{u+2}{g}t_2 \\ \frac{u+2}{g}t_3 & \frac{5vt_4-ut_1}{2} \end{pmatrix}$ and $Y = \begin{pmatrix} t_4 & \frac{v}{g}t_2 \\ \frac{v}{g}t_3 & \frac{vt_1-ut_4}{-2} \end{pmatrix}$, where $t_1, t_2, t_3, t_4, u, v \in \mathbb{Z}$, $u \neq -2$, $g = \gcd(v, u+2)$ and the following relations hold:

$$u^2 - 5v^2 = 4,\ t_1^2 - 5t_4^2 + \frac{4t_2t_3}{g^2}(2+u) = -2.$$

For example, let $u = -18$ and $v = 8$ in (ii). Then we can get a family of solutions to equation (40):

$$\begin{pmatrix} t_1 & -2t_2 \\ -2t_3 & 20t_4 + 9t_1 \end{pmatrix}^2 - 5\begin{pmatrix} t_4 & t_2 \\ t_3 & -(4t_1 + 9t_4) \end{pmatrix}^2 = -2I_2,$$

where $t_1,\ t_2,\ t_3,\ t_4 \in \mathbb{Z}$ satisfy $t_1^2 - 5t_4^2 - t_2t_3 = -2$.

## References


[1] A. Aigner, *Die Unmöglichkeit von $x^6 + y^6 = z^6$ und $x^9 + y^9 = z^9$ in quadratischen Körpern*, Monatsh. Math. **61** (1957), 147–150.

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

[3] B. Cohen, *Generalized Pell equations for $2 \times 2$ matrices*, Discuss. Math. Gen. Algebra Appl. **37** (2017), 13–30.

[4] A. Grytczuk, *On Fermat's equation in the set of integral $2 \times 2$ matrices*, Period. Math. Hung. **30** (1995), 67–72.

[5] A. Grytczuk, I. Kurzydło, *On the matrix negative Pell equation*, Discuss. Math. Gen. Algebra Appl. **29** (2009), 35–45.

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

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

[8] H. Li, R. Liu, P. Yuan, *Solutions to a class of integer matrix equation $X^n + Y^n = \lambda^n I$ ($n \in \mathbb{N}$, $\lambda \in \mathbb{Z}$, $\lambda \neq 0$) (in Chinese)*, Acta Math. Sinica (Chinese Ser.) **65** (2022), 89–114.

[9] H. Li, P. Yuan, *Fermat's and Catalan's equations over $M_2(\mathbb{Z})$*, AIMS Math. **8** (2023), 977–996.

[10] J. Mc Laughlin, *Combinatorial identities deriving from the n-th power of a $2 \times 2$ matrix*, Integers **4** (2004), A19.

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

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

[13] X. Zhong, *The solution of $2 \times 2$ matrices equations $A^n = kE$ with integer entries (in Chinese)*, Coll. Math. **22** (2006), 71–74.