Discussiones Mathematicae
General Algebra and Applications 37 (2017) 13–30
doi:10.7151/dmgaa.1261

GENERALIZED PELL EQUATIONS FOR 2×2 MATRICES

Boaz Cohen

Department of Pure Mathematics
Tel Aviv University
Ramat Aviv, Tel Aviv 69978, Israel

e-mail: arctanx@gmail.com

Abstract

In this paper we consider the solutions of the generalized matrix Pell equations $\mathrm{X}^2 - d\mathrm{Y}^2 = c\mathrm{I}$, where X and Y are 2×2 matrices over $\mathbb{Z}$, d is a non-zero (positive or negative) square-free integer, c is an arbitrary integer and I is the 2×2 identity matrix. We determine all solutions of such equations for $c = \pm 1$, as well as all non-commutative solutions for an arbitrary c.

Keywords: matrix equations, Pell equation.

2010 Mathematics Subject Classification: 15A24, 15B36, 11D09.

1. Introduction

In [8] 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 $\mathrm{M}_2(\mathbb{Z})$ of 2×2 *integral matrices*, that is 2×2 matrices over $\mathbb{Z}$. Some generalization of the classical Diophantine equations, such as Fermat's equation, to matrix equations were studied by number of authors such as [1, 6] and [9].

The Pell equation is a diophantine equation of the form $x^2 - dy^2 = 1$, where d is an arbitrary integer. In the discussion on classical Pell equation, it is customary to assume that d is positive since negative d yields only trivial solutions. Generally, d is taken to be square-free, since otherwise we can "absorb" the largest square factor of d into y. Given that d is square-free positive integer, it is known that Pell equation has infinitely many solutions, which arise from a special "fundamental solution". This problem is extensively discussed in the literature. See, for instance [5, pp. 137–158] and also [4].

Given a non-zero (positive or negative) square-free integer d we shall be interested in finding the set of all 2×2 integral matrices X and Y which satisfy the matrix equation

$$\mathrm{X}^2 - d\mathrm{Y}^2 = c\mathrm{I}, \tag{1}$$

where c is an arbitrary integer and"I" denotes the 2×2 identity matrix. By analogy to the ordinary Pell equation, this matrix equation will be called "matrix Pell equation". We emphasize that contrary to the classical Pell equation, where d is considered to be positive, in the matrix Pell equation we shall also handle negative d, since in this case we also get non-trivial solutions.

A similar matrix equation was studied by Grytczuk and Kurzydło in [2]. The former authors gave a necessary and sufficient condition for solvability of the *negative* matrix Pell equation, namely, of the equation

$$\mathrm{X}^2 - d\mathrm{Y}^2 = -\mathrm{I}, \tag{2}$$

for *nonsingular* 2×2 matrices X, Y over $\mathbb{Z}$.

In order to solve the matrix Pell equations (1) we investigate separately commuting and non-commuting solutions, that is, solutions satisfying $\mathrm{XY} = \mathrm{YX}$ or $\mathrm{XY} \neq \mathrm{YX}$, respectively. In this paper we determine all (non-commutating and commutating) solutions of matrix Pell equations (1) for $c = \pm 1$, as well as all non-commutating solutions for an arbitrary c. The following theorem demonstrates our main results for $c = 1$, that is, concerning the equation $\mathrm{X}^2 - d\mathrm{Y}^2 = \mathrm{I}$ (see Theorem 2.1 and Theorem 3.2).

Theorem 1.1. *Suppose that* X *and* Y *are* 2×2 *integral matrices and let* d *be a non-zero square-free integer. Then*

(a) $\mathrm{XY} = \mathrm{YX}$ *and* $\mathrm{X}^2 - d\mathrm{Y}^2 = \mathrm{I}$ *iff either*

$$\mathrm{X} = \begin{pmatrix} t_1 & 0 \\ 0 & t_1 \end{pmatrix} \quad ; \quad \mathrm{Y} = \begin{pmatrix} t_4 & t_2 \\ t_3 & -t_4 \end{pmatrix}$$

where $t_1, t_2, t_3, t_4 \in \mathbb{Z}$ *satisfy* $t_1^2 - dt_4^2 - dt_2t_3 = 1$, *or*

$$\mathrm{X} = \begin{pmatrix} t_1 & \frac{a-1}{g}t_2 \\ \frac{a-1}{g}t_3 & at_1 - bdt_4 \end{pmatrix} \quad ; \quad \mathrm{Y} = \begin{pmatrix} t_4 & \frac{b}{g}t_2 \\ \frac{b}{g}t_3 & bt_1 - at_4 \end{pmatrix}$$

where $t_1, t_2, t_3, t_4, a, b \in \mathbb{Z}$, $a \neq 1$, $g = \gcd(a-1, b)$ *and the following relations hold:*

$$t_1^2 - dt_4^2 - \frac{2(a-1)}{g^2}t_2t_3 = 1 \quad \textit{and} \quad a^2 - b^2d = 1.$$

(b) $\mathrm{XY} \neq \mathrm{YX}$ *and* $\mathrm{X}^2 - d\mathrm{Y}^2 = \mathrm{I}$ *iff*

$$\mathrm{X} = \begin{pmatrix} t_1 & t_2 \\ t_3 & -t_1 \end{pmatrix} \quad ; \quad \mathrm{Y} = \begin{pmatrix} s_1 & s_2 \\ s_3 & -s_1 \end{pmatrix}$$

where $t_1, t_2, t_3, s_1, s_2, s_3 \in \mathbb{Z}$ *satisfy* $t_1^2 + t_2 t_3 - d(s_1^2 + s_2 s_3) = 1$ *and the vectors* $\vec{t} = (t_1, t_2, t_3)$ *and* $\vec{s} = (s_1, s_2, s_3)$ *are linearly independent over the field* $\mathbb{Q}$ *of rational numbers.*

We shall denote the trace of a square matrix A by tr(A), its determinant by |A| and its adjugate matrix by adj(A). The linear algebra information may be found, for example, in the book [3].

The author is grateful to the referee for his constructive remarks.

2. Commuting Integral Solutions of the Matrix Pell Equation

The following theorem characterizes all the commuting integral solutions of the matrix Pell equation (1) and for $c = 1$ and $c = -1$.

Theorem 2.1. *Suppose that* X *and* Y *are* 2×2 *integral matrices and let* d *be a non-zero square-free integer. Then* $\mathrm{XY} = \mathrm{YX}$ *and* $\mathrm{X}^2 - d\mathrm{Y}^2 = \pm\mathrm{I}$ *iff either*

$$\mathrm{X} = \begin{pmatrix} t_1 & 0 \\ 0 & t_1 \end{pmatrix} \quad ; \quad \mathrm{Y} = \begin{pmatrix} t_4 & t_2 \\ t_3 & -t_4 \end{pmatrix}$$

where $t_1, t_2, t_3, t_4 \in \mathbb{Z}$ *satisfy* $t_1^2 - dt_4^2 - dt_2 t_3 = \pm 1$*, or*

$$\mathrm{X} = \begin{pmatrix} t_1 & \frac{a \mp 1}{g} t_2 \\ \frac{a \mp 1}{g} t_3 & \pm(at_1 - bdt_4) \end{pmatrix} \quad ; \quad \mathrm{Y} = \begin{pmatrix} t_4 & \frac{b}{g} t_2 \\ \frac{b}{g} t_3 & \pm(bt_1 - at_4) \end{pmatrix}$$

where $t_1, t_2, t_3, t_4, a, b \in \mathbb{Z}$*,* $a \neq \pm 1$*,* $g = \gcd(a \mp 1, b)$ *and the following relations hold:*

$$t_1^2 - dt_4^2 \mp \frac{2(a \mp 1)}{g^2} t_2 t_3 = \pm 1 \quad \textit{and} \quad a^2 - b^2 d = 1.$$

Proof. We shall prove this theorem simultaneously for the equations $\mathrm{X}^2 - d\mathrm{Y}^2 = \mathrm{I}$ and $\mathrm{X}^2 - d\mathrm{Y}^2 = -\mathrm{I}$, where the upper signs refer to the first equation and the lower signs refer to the second case. Note that the condition $a \neq \pm 1$ means that $a \neq 1$ in the first case and $a \neq -1$ in the second case. Thus g is always defined.

We begin by proving that the conditions are sufficient. We have to verify two cases.

First suppose that

$$\mathrm{X} = \begin{pmatrix} t_1 & 0 \\ 0 & t_1 \end{pmatrix} \quad ; \quad \mathrm{Y} = \begin{pmatrix} t_4 & t_2 \\ t_3 & -t_4 \end{pmatrix},$$

where $t_1, t_2, t_3, t_4 \in \mathbb{Z}$ satisfy $t_1^2 - dt_4^2 - dt_2t_3 = \pm 1$. Then X and Y commute and

$$\begin{aligned} \mathrm{X}^2 - d\mathrm{Y}^2 &= \begin{pmatrix} t_1 & 0 \\ 0 & t_1 \end{pmatrix}^2 - d\begin{pmatrix} t_4 & t_2 \\ t_3 & -t_4 \end{pmatrix}^2 \\ &= \begin{pmatrix} t_1^2 - dt_4^2 - dt_2t_3 & 0 \\ 0 & t_1^2 - dt_4^2 - dt_2t_3 \end{pmatrix}. \end{aligned} \tag{3}$$

By our assumption $t_1^2 - dt_4^2 - dt_2t_3 = \pm 1$, so indeed $\mathrm{X}^2 - d\mathrm{Y}^2 = \pm \mathrm{I}$, as required.

Now suppose that

$$\mathrm{X} = \begin{pmatrix} t_1 & \frac{a\mp 1}{g} t_2 \\ \frac{a\mp 1}{g} t_3 & \pm(at_1 - bdt_4) \end{pmatrix} \quad ; \quad \mathrm{Y} = \begin{pmatrix} t_4 & \frac{b}{g} t_2 \\ \frac{b}{g} t_3 & \pm(bt_1 - at_4) \end{pmatrix}$$

where $t_1, t_2, t_3, t_4, a, b \in \mathbb{Z}$, $a \neq \pm 1$, $g = \gcd(a \mp 1, b)$ and the following relations hold: $t_1^2 - dt_4^2 \mp 2(1 \mp a)t_2t_3/g^2 = \pm 1$ and $a^2 - db^2 = 1$. First let us verify that X and Y commute. Indeed, a direct computation yields

$$\mathrm{XY} - \mathrm{YX} = \begin{pmatrix} 0 & \mp\frac{a^2 - b^2d - 1}{g} t_2t_4 \\ \pm\frac{a^2 - b^2d - 1}{g} t_3t_4 & 0 \end{pmatrix}.$$

Since $a^2 - b^2d = 1$, it follows that $\mathrm{XY} = \mathrm{YX}$, as claimed. Next, we have

$$\mathrm{X}^2 - d\mathrm{Y}^2 = \begin{pmatrix} t_1 & \frac{a\mp 1}{g} t_2 \\ \frac{a\mp 1}{g} t_3 & \pm(at_1 - bdt_4) \end{pmatrix}^2 - d\begin{pmatrix} t_4 & \frac{b}{g} t_2 \\ \frac{b}{g} t_3 & \pm(bt_1 - at_4) \end{pmatrix}^2$$

$$= \begin{pmatrix} t_1^2 - dt_4^2 + \frac{a^2 - db^2 + 1 \mp 2a}{g^2} t_2t_3 & \pm\frac{a^2 - db^2 - 1}{g} t_1t_2 \\ \pm\frac{a^2 - b^2d - 1}{g} t_1t_3 & d(b^2d - a^2)t_4^2 + \frac{a^2 - db^2 + 1 \mp 2a}{g^2} t_2t_3 + (a^2 - b^2d)t_1^2 \end{pmatrix}.$$

Since $a^2 - b^2d = 1$, we get

$$\mathrm{X}^2 - d\mathrm{Y}^2 = \begin{pmatrix} t_1^2 - dt_4^2 \mp \frac{2(a\mp 1)}{g^2} t_2t_3 & 0 \\ 0 & t_1^2 - dt_4^2 \mp \frac{2(a\mp 1)}{g^2} t_2t_3 \end{pmatrix}, \tag{4}$$

By our assumption $t_1^2 - dt_4^2 \mp 2(a \mp 1)t_2t_3/g^2 = \pm 1$, so $\mathrm{X}^2 - d\mathrm{Y}^2 = \pm \mathrm{I}$, as required.

Next we prove that the conditions are necessary. Set

$$\mathrm{X} = \begin{pmatrix} x_1 & x_2 \\ x_3 & x_4 \end{pmatrix} \quad ; \quad \mathrm{Y} = \begin{pmatrix} y_1 & y_2 \\ y_3 & y_4 \end{pmatrix},$$

where the x_i's and y_i's are integers and assume that $\mathrm{X}^2 - d\mathrm{Y}^2 = \pm \mathrm{I}$.

Since by our assumption $\mathrm{XY} = \mathrm{YX}$, it follows that over the ring $\mathbb{Z}[\sqrt{d}]$ we get the following decomposition

$$(\mathrm{X} + \sqrt{d}\mathrm{Y})(\mathrm{X} - \sqrt{d}\mathrm{Y}) = \pm \mathrm{I}. \tag{5}$$

Hence $|\mathrm{X} + \sqrt{d}\mathrm{Y}||\mathrm{X} - \sqrt{d}\mathrm{Y}| = 1$. Set

$$|\mathrm{X} + \sqrt{d}\mathrm{Y}| = a + b\sqrt{d},$$

where $a, b \in \mathbb{Z}$. Note that

$$\mathrm{X} \pm \sqrt{d}\mathrm{Y} = \begin{pmatrix} x_1 \pm y_1\sqrt{d} & x_2 \pm y_2\sqrt{d} \\ x_3 \pm y_3\sqrt{d} & x_4 \pm y_4\sqrt{d} \end{pmatrix}.$$

Thus

$$\begin{aligned} |\mathrm{X} \pm \sqrt{d}\mathrm{Y}| &= (x_1 \pm \sqrt{d}y_1)(x_4 \pm \sqrt{d}y_4) - (x_2 \pm \sqrt{d}y_2)(x_3 \pm \sqrt{d}y_3) \\ &= x_1x_4 - x_2x_3 + d(y_1y_4 - y_2y_3) \pm (x_1y_4 + x_4y_1 - x_2y_3 - y_2x_3)\sqrt{d}. \end{aligned}$$

Therefore $|\mathrm{X} - \sqrt{d}\mathrm{Y}| = a - b\sqrt{d}$. By (5) we get $(\mathrm{X} + \sqrt{d}\mathrm{Y})^{-1} = \pm(\mathrm{X} - \sqrt{d}\mathrm{Y})$ and $a^2 - b^2d = 1$. Hence

$$\frac{1}{|\mathrm{X} + \sqrt{d}\mathrm{Y}|}\mathrm{adj}(\mathrm{X} + \sqrt{d}\mathrm{Y}) = \pm(\mathrm{X} - \sqrt{d}\mathrm{Y}),$$

that is

$$(a - b\sqrt{d}) \begin{pmatrix} x_4 + \sqrt{d}y_4 & -x_2 - \sqrt{d}y_2 \\ -x_3 - \sqrt{d}y_3 & x_1 + \sqrt{d}y_1 \end{pmatrix} = \pm \begin{pmatrix} x_1 - \sqrt{d}y_1 & x_2 - \sqrt{d}y_2 \\ x_3 - \sqrt{d}y_3 & x_4 - \sqrt{d}y_4 \end{pmatrix}.$$

Thus

$$(6) \qquad \begin{cases} (ax_4 - bdy_4) + (ay_4 - bx_4)\sqrt{d} = \pm(x_1 - y_1\sqrt{d}) & \text{(i)} \\ (bdy_2 - ax_2) + (bx_2 - ay_2)\sqrt{d} = \pm(x_2 - y_2\sqrt{d}) & \text{(ii)} \\ (bdy_3 - ax_3) + (bx_3 - ay_3)\sqrt{d} = \pm(x_3 - y_3\sqrt{d}) & \text{(iii)} \\ (ax_1 - bdy_1) + (ay_1 - bx_1)\sqrt{d} = \pm(x_4 - y_4\sqrt{d}) & \text{(iv)}. \end{cases}$$

We shall distinguish between two cases.

Case 1. Assume, first, that $a \neq 1$ and $a \neq -1$. Hence $b \neq 0$. Since the x_i's and the y_i's are integers, it follows from (ii) and (iii) of (6) that

$$bx_2 - ay_2 = \mp y_2 \quad \text{and} \quad bx_3 - ay_3 = \mp y_3.$$

Hence

$$y_2 = \frac{b}{a \mp 1}x_2 \quad \text{and} \quad y_3 = \frac{b}{a \mp 1}x_3.$$

Similarly, by equations (i) and (iv) of (6) we get

$$\begin{cases} ay_4 - bx_4 = \mp y_1 \\ ay_1 - bx_1 = \mp y_4, \end{cases}$$

that is

$$\begin{cases} \pm y_1 + a y_4 = b x_4 \\ a y_1 \pm y_4 = b x_1. \end{cases}$$

Since $1 - a^2 \neq 0$ we may use Cramer's Rule to obtain

$$y_1 = \frac{\begin{vmatrix} bx_4 & a \\ bx_1 & \pm 1 \end{vmatrix}}{\begin{vmatrix} \pm 1 & a \\ a & \pm 1 \end{vmatrix}} = \frac{b(\pm x_4 - a x_1)}{1 - a^2} = \frac{b}{a^2 - 1}(a x_1 \mp x_4)$$

and

$$y_4 = \frac{\begin{vmatrix} \pm 1 & bx_4 \\ a & bx_1 \end{vmatrix}}{\begin{vmatrix} \pm 1 & a \\ a & \pm 1 \end{vmatrix}} = \frac{b(\pm x_1 - a x_4)}{1 - a^2} = \frac{b}{a^2 - 1}(a x_4 \mp x_1).$$

Therefore

$$\mathrm{Y} = \frac{b}{a^2 - 1} \begin{pmatrix} a x_1 \mp x_4 & (a \pm 1) x_2 \\ (a \pm 1) x_3 & a x_4 \mp x_1 \end{pmatrix}.$$

Using $a^2 - 1 = b^2 d$ yields

$$\mathrm{Y} = \frac{1}{bd} \begin{pmatrix} a x_1 \mp x_4 & (a \pm 1) x_2 \\ (a \pm 1) x_3 & a x_4 \mp x_1 \end{pmatrix}.$$

Since Y is over $\mathbb{Z}$, it follows in particular that

$$\begin{cases} bd \mid a x_1 \mp x_4 & \text{(i)} \\ bd \mid (a \pm 1) x_2 & \text{(ii)} \\ bd \mid (a \pm 1) x_3 & \text{(iii)}. \end{cases} \tag{7}$$

If we set $x_1 = t_1$, then by (i) of (7) there is $t_4 \in \mathbb{Z}$ such that $bdt_4 = at_1 \mp x_4$, that is $x_4 = \pm(at_1 - bdt_4)$. By (ii) there is $s_2 \in \mathbb{Z}$ such that $bds_2 = (a \pm 1)x_2$, that is $x_2 = \frac{bd}{a \pm 1} s_2$. Since $(a-1)(a+1) = db^2$, we have $x_2 = \frac{a \mp 1}{b} s_2$. Note that since x_2 is an integer, it follows that $b \mid (a \mp 1)s_2$, that is $\frac{b}{g} \mid s_2$, where $g = \gcd(a \mp 1, b)$. Thus there exists $t_2 \in \mathbb{Z}$ such that $s_2 = \frac{b}{g} t_2$. Since $b^2 d = a^2 - 1$, we get $x_2 = \frac{a \mp 1}{g} t_2$. Similarly, by (iii), there is $t_3 \in \mathbb{Z}$ such that $x_3 = \frac{a \mp 1}{g} t_3$. Therefore

$$\mathrm{X} = \begin{pmatrix} t_1 & \frac{a \mp 1}{g} t_2 \\ \frac{a \mp 1}{g} t_3 & \pm(at_1 - bdt_4) \end{pmatrix},$$

where $t_1, t_2, t_3, t_4, a, b \in \mathbb{Z}$, $a^2 - b^2 d = 1$, $a \neq 1$, $a \neq -1$ and $g = \gcd(a \mp 1, b)$. Moreover

$$\mathrm{Y} = \frac{1}{bd}\begin{pmatrix} ax_1 \mp x_4 & (a \pm 1)x_2 \\ (a \pm 1)x_3 & ax_4 \mp x_1 \end{pmatrix} = \begin{pmatrix} t_4 & \frac{a^2-1}{bdg}t_2 \\ \frac{a^2-1}{bdg}t_3 & \pm\left(\frac{a^2-1}{bd}t_1 - at_4\right) \end{pmatrix}$$
$$= \begin{pmatrix} t_4 & \frac{b}{g}t_2 \\ \frac{b}{g}t_3 & \pm(bt_1 - at_4) \end{pmatrix}.$$

To complete the proof we need to show that $t_1^2 - dt_4^2 \mp \frac{2(1\mp a)}{g^2}t_2t_3 = \pm 1$. Indeed, by (4) we have

$$\mathrm{X}^2 - d\mathrm{Y}^2 = \begin{pmatrix} t_1^2 - dt_4^2 \mp \frac{2(a\mp 1)}{g^2}t_2t_3 & 0 \\ 0 & t_1^2 - dt_4^2 \mp \frac{2(a\mp 1)}{g^2}t_2t_3 \end{pmatrix}.$$

Since $\mathrm{X}^2 - d\mathrm{Y}^2 = \pm\mathrm{I}$, the assertion follows.

Case 2. Now, assume that either $a = 1$ or $a = -1$. Hence $b = 0$ and by (6) we get

$$\begin{cases} a(x_4 + y_4\sqrt{d}) = \pm(x_1 - y_1\sqrt{d}) \\ -a(x_2 + y_2\sqrt{d}) = \pm(x_2 - y_2\sqrt{d}) \\ -a(x_3 + y_3\sqrt{d}) = \pm(x_3 - y_3\sqrt{d}) \\ a(x_1 + y_1\sqrt{d}) = \pm(x_4 - y_4\sqrt{d}). \end{cases}$$

Thus

$$(8) \qquad \begin{cases} ax_4 \mp x_1 = 0 \quad \text{and} \quad ay_4 \pm y_1 = 0 & \text{(i)} \\ (a \pm 1)x_2 = 0 \quad \text{and} \quad (a \mp 1)y_2 = 0 & \text{(ii)} \\ (a \pm 1)x_3 = 0 \quad \text{and} \quad (a \mp 1)y_3 = 0 & \text{(iii)} \\ ax_1 \mp x_4 = 0 \quad \text{and} \quad ay_1 \pm y_4 = 0 & \text{(iv)} \end{cases}$$

First let us consider the equation $\mathrm{X}^2 - d\mathrm{Y}^2 = \mathrm{I}$ (so we shall refer in (8) to the upper sign among "$\pm$" and "$\mp$").

If $a = -1$, then (ii), (iii) and (iv) of (8) yield

$$\begin{cases} x_4 = -x_1 \\ y_4 = y_1 \\ y_2 = y_3 = 0. \end{cases}$$

Therefore, there exist $t_1, t_2, t_3, t_4 \in \mathbb{Z}$ such that $x_1 = t_1$, $x_2 = -t_2$, $x_3 = -t_3$, $y_1 = t_4$ and

$$\mathrm{X} = \begin{pmatrix} t_1 & -t_2 \\ -t_3 & -t_1 \end{pmatrix} \quad ; \quad \mathrm{Y} = \begin{pmatrix} t_4 & 0 \\ 0 & t_4 \end{pmatrix}.$$

In addition,

$$\mathrm{X}^2 - d\mathrm{Y}^2 = \begin{pmatrix} t_1^2 - dt_4^2 + t_2t_3 & 0 \\ 0 & t_1^2 - dt_4^2 + t_2t_3 \end{pmatrix}.$$

Since by our assumption $\mathrm{X}^2 - d\mathrm{Y}^2 = \mathrm{I}$, it follows that $t_1^2 - dt_4^2 + t_2t_3 = 1$.

We note that the matrices and the condition which we obtained for $a = -1$ (regarding the equation $\mathrm{X}^2 - d\mathrm{Y}^2 = \mathrm{I}$) are obtained by taking $a = -1$ in Case 1. Indeed, if $a = -1$, then $b = 0$, so $g = \gcd(a-1, b) = \gcd(-2, 0) = 2$. Hence in Case 1 we obtian

$$\mathrm{X} = \begin{pmatrix} t_1 & \frac{a-1}{g}t_2 \\ \frac{a-1}{g}t_3 & at_1 - bdt_4 \end{pmatrix} = \begin{pmatrix} t_1 & \frac{-2}{2}t_2 \\ \frac{-2}{2}t_3 & -t_1 - 0 \end{pmatrix} = \begin{pmatrix} t_1 & -t_2 \\ -t_3 & -t_1 \end{pmatrix}$$

and

$$\mathrm{Y} = \begin{pmatrix} t_4 & \frac{b}{g}t_2 \\ \frac{b}{g}t_3 & bt_1 - at_4 \end{pmatrix} = \begin{pmatrix} t_4 & 0 \\ 0 & t_4 \end{pmatrix}.$$

In addition, for $a = -1$, $b = 0$ and $g = 2$ we get the same condition

$$1 = t_1^2 - dt_4^2 - \frac{2(a-1)}{g^2}t_2t_3 = t_1^2 - dt_4^2 - \frac{2(-2)}{4}t_2t_3 = t_1^2 - dt_4^2 + t_2t_3,$$

as claimed.

If $a = 1$, then (i), (ii) and (iii) of (8) yield

$$\begin{cases} x_1 = x_4 \\ y_4 = -y_1 \\ x_2 = x_3 = 0. \end{cases}$$

Therefore, there exist $t_1, t_2, t_3, t_4 \in \mathbb{Z}$ such that $x_1 = t_1$, $y_2 = t_2$, $y_3 = t_3$ and $y_1 = t_4$, so

$$\mathrm{X} = \begin{pmatrix} t_1 & 0 \\ 0 & t_1 \end{pmatrix} \quad ; \quad \mathrm{Y} = \begin{pmatrix} t_4 & t_2 \\ t_3 & -t_4 \end{pmatrix}.$$

In addition, by (3) we have

$$\mathrm{X}^2 - d\mathrm{Y}^2 = \begin{pmatrix} t_1^2 - dt_4^2 - dt_2t_3 & 0 \\ 0 & t_1^2 - dt_4^2 - dt_2t_3 \end{pmatrix}.$$

Since by our assumption $\mathrm{X}^2 - d\mathrm{Y}^2 = \mathrm{I}$, it follows that $t_1^2 - dt_4^2 - dt_2t_3 = 1$, as required.

Next, let us consider the negative matrix Pell equation $\mathrm{X}^2 - d\mathrm{Y}^2 = -\mathrm{I}$ (so we shall refer in (8) to the lower sign among "$\pm$" and "$\mp$").

If $a = -1$, then (ii), (iii) and (iv) of (8) yield

$$\begin{cases} x_4 = x_1 \\ y_4 = -y_1 \\ x_2 = x_3 = 0. \end{cases}$$

Therefore, there exist $t_1, t_2, t_3, t_4 \in \mathbb{Z}$ such that $x_1 = t_1$, $y_2 = t_2$, $y_3 = t_3$ and $y_1 = t_4$, so

$$\mathrm{X} = \begin{pmatrix} t_1 & 0 \\ 0 & t_1 \end{pmatrix} \quad ; \quad \mathrm{Y} = \begin{pmatrix} t_4 & t_2 \\ t_3 & -t_4 \end{pmatrix}.$$

As in the former case, since $\mathrm{X}^2 - d\mathrm{Y}^2 = -\mathrm{I}$, it follows that $t_1^2 - dt_4^2 - dt_2t_3 = -1$, as required.

If $a = 1$, then (i), (ii) and (iii) of (8) yield

$$\begin{cases} x_4 = -x_1 \\ y_4 = y_1 \\ y_2 = y_3 = 0. \end{cases}$$

Therefore, there exist $t_1, t_2, t_3, t_4 \in \mathbb{Z}$ such that $x_1 = t_1$, $x_2 = t_2$, $x_3 = t_3$, $y_1 = t_4$ and

$$\mathrm{X} = \begin{pmatrix} t_1 & t_2 \\ t_3 & -t_1 \end{pmatrix} \quad ; \quad \mathrm{Y} = \begin{pmatrix} t_4 & 0 \\ 0 & t_4 \end{pmatrix}.$$

Since

$$\mathrm{X}^2 - d\mathrm{Y}^2 = \begin{pmatrix} t_1^2 - dt_4 + t_2t_3 & 0 \\ 0 & t_1^2 - dt_4 + t_2t_3 \end{pmatrix} = -\mathrm{I},$$

it follows that $t_1^2 - dt_4^2 + t_2t_3 = -1$.

As shown in the previous case, it can be verified the matrices and the condition which we obtained for $a = 1$ (regarding the equation $\mathrm{X}^2 - d\mathrm{Y}^2 = -\mathrm{I}$) are obtained by taking $a = 1$ in Case 1. ∎

Example 2.2. Let us construct a set of commutative solutions for the matrix Pell equation $\mathrm{X}^2 - 2\mathrm{Y}^2 = \mathrm{I}$.

First we choose a solution for the ordinary Pell equation $a^2 - 2b^2 = 1$, say $(a, b) = (3, 2)$. Regarding the equation $\mathrm{X}^2 - 2\mathrm{Y}^2 = \mathrm{I}$, set $g = \gcd(a - 1, b) = 2$. By Theorem 2.1, the matrices

$$\mathrm{X} = \begin{pmatrix} t_1 & \frac{a-1}{g}t_2 \\ \frac{a-1}{g}t_3 & at_1 - bdt_4 \end{pmatrix} = \begin{pmatrix} t_1 & t_2 \\ t_3 & 3t_1 - 4t_4 \end{pmatrix}$$

and

$$\mathrm{Y} = \begin{pmatrix} t_4 & \frac{b}{g}t_2 \\ \frac{b}{g}t_3 & bt_1 - at_4 \end{pmatrix} = \begin{pmatrix} t_4 & t_2 \\ t_3 & 2t_1 - 3t_4 \end{pmatrix},$$

where $t_1, t_2, t_3, t_4 \in \mathbb{Z}$ such that $t_1^2 - 2t_4^2 - t_2t_3 = 1$, constitute a set of commutative matrix solutions for $\mathrm{X}^2 - 2\mathrm{Y}^2 = \mathrm{I}$. For example, by choosing $t_1 = 5$, $t_2 = 2$, $t_3 = 3$ and $t_4 = 3$, we get the particular solution

$$\mathrm{X} = \begin{pmatrix} 5 & 2 \\ 3 & 3 \end{pmatrix} \quad ; \quad \mathrm{Y} = \begin{pmatrix} 3 & 2 \\ 3 & 1 \end{pmatrix}.$$

Indeed,

$$\mathrm{X}^2 - 2\mathrm{Y}^2 = \begin{pmatrix} 5 & 2 \\ 3 & 3 \end{pmatrix}^2 - 2\begin{pmatrix} 3 & 2 \\ 3 & 1 \end{pmatrix}^2 = \begin{pmatrix} 31 & 16 \\ 24 & 15 \end{pmatrix} - 2\begin{pmatrix} 15 & 8 \\ 12 & 7 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \mathrm{I}.$$

Example 2.3. Let us describe the set of all commutative solutions for the matrix Pell equation $\mathrm{X}^2 + \mathrm{Y}^2 = \mathrm{I}$.

Theorem 2.1 gives us two sets of solutions. The first set consists of all matrices of the form

$$\mathrm{X} = \begin{pmatrix} t_1 & 0 \\ 0 & t_1 \end{pmatrix} \quad ; \quad \mathrm{Y} = \begin{pmatrix} t_4 & t_2 \\ t_3 & -t_4 \end{pmatrix}$$

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

For the second set, notice that the solutions of the ordinary Pell equation $a^2 + b^2 = 1$ with $a \neq 1$ are $(a, b) \in \{(-1, 0), (0, -1), (0, 1)\}$. For $(a, b) = (-1, 0)$, we have $g = \gcd(a - 1, b) = \gcd(-2, 0) = 2$. The corresponding matrix solutions are therefore

$$\mathrm{X} = \begin{pmatrix} t_1 & \frac{a-1}{g}t_2 \\ \frac{a-1}{g}t_3 & at_1 - bdt_4 \end{pmatrix} = \begin{pmatrix} t_1 & -t_2 \\ -t_3 & -t_1 \end{pmatrix}$$

and

$$\mathrm{Y} = \begin{pmatrix} t_4 & \frac{b}{g}t_2 \\ \frac{b}{g}t_3 & bt_1 - at_4 \end{pmatrix} = \begin{pmatrix} t_4 & 0 \\ 0 & t_4 \end{pmatrix},$$

where $t_1, t_2, t_3, t_4 \in \mathbb{Z}$ satisfy $t_1^2 - dt_4^2 - 2(a-1)t_2t_3/g^2 = 1$, that is $t_1^2 + t_4^2 + t_2t_3 = 1$. For $(a, b) = (0, 1)$, we have that $g = \gcd(a - 1, b) = \gcd(-1, 1) = 1$. The corresponding matrix solutions are therefore

$$\mathrm{X} = \begin{pmatrix} t_1 & \frac{a-1}{g}t_2 \\ \frac{a-1}{g}t_3 & at_1 - bdt_4 \end{pmatrix} = \begin{pmatrix} t_1 & -t_2 \\ -t_3 & t_4 \end{pmatrix}$$

and

$$\mathrm{Y} = \begin{pmatrix} t_4 & \frac{b}{g}t_2 \\ \frac{b}{g}t_3 & bt_1 - at_4 \end{pmatrix} = \begin{pmatrix} t_4 & t_2 \\ t_3 & t_1 \end{pmatrix}$$

where $t_1, t_2, t_3, t_4 \in \mathbb{Z}$ satisfy $t_1^2 - dt_4^2 - 2(a-1)t_2t_3/g^2 = 1$, that is $t_1^2 + t_4^2 + 2t_2t_3 = 1$. Similarly, for $(a, b) = (0, -1)$, we get the following matrix solutions:

$$\mathrm{X} = \begin{pmatrix} t_1 & -t_2 \\ -t_3 & -t_4 \end{pmatrix} \quad ; \quad \mathrm{Y} = \begin{pmatrix} t_4 & -t_2 \\ -t_3 & -t_1 \end{pmatrix}$$

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

In particular, assigning $t_1 = 3$, $t_2 = -1$, $t_3 = 6$ and $t_4 = -2$ in the last set of solutions yields

$$\mathrm{X} = \begin{pmatrix} 3 & 1 \\ -6 & 2 \end{pmatrix} \quad ; \quad \mathrm{Y} = \begin{pmatrix} -2 & 1 \\ -6 & -3 \end{pmatrix}.$$

Indeed

$$\mathrm{X}^2 + \mathrm{Y}^2 = \begin{pmatrix} 3 & 1 \\ -6 & 2 \end{pmatrix}^2 + \begin{pmatrix} -2 & 1 \\ -6 & -3 \end{pmatrix}^2 = \begin{pmatrix} 3 & 5 \\ -30 & -2 \end{pmatrix} + \begin{pmatrix} -2 & -5 \\ 30 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \mathrm{I}.$$

By Theorem 2.1, the solutions of the matrix Pell equations $\mathrm{X}^2 - d\mathrm{Y}^2 = \pm\mathrm{I}$ are parameterized using six parameters which satisfying certain conditions. The following theorem discusses the solvability of these conditions.

Theorem 2.4. *Let d be a non-zero square-free integer and let a, b be solutions of the ordinary Pell equation $a^2 - b^2 d = 1$.*

(a) *$t_1, t_2, t_3, t_4 \in \mathbb{Z}$ satisfy $t_1^2 - dt_4^2 - dt_2t_3 = \pm 1$ iff*

$$t_2t_3 = \frac{t_1^2 \mp 1}{d} - t_4^2 \quad \textit{and} \quad t_1^2 \equiv \pm 1 (\mathrm{mod}\, d).$$

(b) *If $a \neq \pm 1$, then $t_1, t_2, t_3, t_4 \in \mathbb{Z}$ satisfy $t_1^2 - dt_4^2 \mp \dfrac{2(a \mp 1)}{g^2} t_2t_3 = \pm 1$, where $g = \gcd(a \mp 1, b)$ iff*

$$t_2t_3 = \pm \frac{g^2}{2(a \mp 1)} \left(t_1^2 \mp 1 - dt_4^2\right)$$

and

$$t_1^2 \equiv \begin{cases} \pm 1 \left(\mathrm{mod}\, \dfrac{2(a \mp 1)}{g^2}\right) & g \textit{ is even} \\ \pm 1 \left(\mathrm{mod}\, \dfrac{a \mp 1}{g^2}\right) & g \textit{ is odd.} \end{cases}$$

Proof. (a) If $t_2t_3 = (t_1^2 \mp 1)/d - t_4^2$, then clearly $t_1^2 - dt_4^2 - dt_2t_3 = \pm 1$. Suppose that $t_1^2 - dt_4^2 - dt_2t_3 = \pm 1$. Then $t_2t_3 = (t_1^2 \mp 1)/d - t_4^2$. In addition, $t_1^2 \mp 1 = d(t_4^2 + t_2t_3)$, so $d \mid t_1^2 \mp 1$, as required.

(b) If $t_2t_3 = \pm g^2(t_1^2 \mp 1 - dt_4^2)/2(a \mp 1)$, then clearly $t_1^2 - dt_4^2 \mp 2(a \mp 1)t_2t_3/g^2 = \pm 1$. Suppose that $t_1^2 - dt_4^2 \mp 2(a \mp 1)t_2t_3/g^2 = \pm 1$. Note that in order to prove our claim it suffices to prove that whenever g is even, then $2(a \mp 1)/g^2$ is an integer that divides d and whenever g is odd, then $(a \mp 1)/g^2$ is an integer that divides d.

We begin by proving that $g^2 \mid 2(a \mp 1)$. By the assumption $a^2 - b^2 d = 1$, so $(a-1)(a+1) = b^2 d$. Since $g^2 \mid b^2$, it follows that $g^2 \mid (a-1)(a+1)$. Note that $\gcd(a-1, a+1) \in \{1, 2\}$. We shall distinguish between these two cases:

Case 1. $\gcd(a-1, a+1) = 1$. Since $g \mid (a \mp 1)$, it follows that $\gcd(g, a \pm 1) = 1$. But $g^2 \mid (a-1)(a+1)$, so $g^2 \mid (a \mp 1)$ and hence also $g^2 \mid 2(a \mp 1)$, as claimed.

Case 2. $\gcd(a-1, a+1) = 2$. Since $g^2 \mid (a-1)(a+1)$ and $g \mid (a \mp 1)$, it follows that $g^2 \mid 4(\frac{a-1}{2})(\frac{a+1}{2})$ and $g \mid 2(\frac{a \mp 1}{2})$. If g is odd, then $g^2 \mid (\frac{a-1}{2})(\frac{a+1}{2})$ and $g \mid \frac{a \mp 1}{2}$. But $\gcd(\frac{a-1}{2}, \frac{a+1}{2}) = 1$, so $g^2 \mid \frac{a \mp 1}{2}$ and hence $g^2 \mid 2(a \mp 1)$, as claimed. If g is even, then $\left(\frac{g}{2}\right)^2 \mid (\frac{a-1}{2})(\frac{a+1}{2})$ and $\frac{g}{2} \mid \frac{a \mp 1}{2}$. Again, since $\gcd(\frac{a-1}{2}, \frac{a+1}{2}) = 1$, it follows that $\left(\frac{g}{2}\right)^2 \mid \frac{a \mp 1}{2}$, so $g^2 \mid 2(a \mp 1)$, as claimed.

Now we shall prove that $\frac{2(a \mp 1)}{g^2} \mid d$ if g is even, and that $\frac{a \mp 1}{g^2} \mid d$ if g is odd. Recall that by the above proof $g^2 \mid 2(a \mp 1)$.

If g is odd, then $g^2 \mid (a \mp 1)$. Since $(a-1)(a+1) = b^2 d$, it follows that $(\frac{a \mp 1}{g^2})(a \pm 1) = (\frac{b}{g})^2 d$. Thus $\frac{a \mp 1}{g^2} \mid (\frac{b}{g})^2 d$. But $\gcd(\frac{a \mp 1}{g}, \frac{b}{g}) = 1$ and $\frac{a \mp 1}{g^2} \mid \frac{a \mp 1}{g}$, so $\gcd(\frac{a \mp 1}{g^2}, (\frac{b}{g})^2) = 1$. Hence $\frac{a \mp 1}{g^2} \mid d$, as required.

Assume now that g is even. Hence $a-1$ and $a+1$ are even. As above $\frac{2(a \mp 1)}{g^2}(\frac{a \pm 1}{2}) = (\frac{b}{g})^2 d$, so $\frac{2(a \mp 1)}{g^2} \mid (\frac{b}{g})^2 d$. But $\frac{2(a \mp 1)}{g^2} \cdot \frac{g}{2} = \frac{a \mp 1}{g}$, so $\frac{2(a \mp 1)}{g^2} \mid \frac{a \mp 1}{g}$ and since $\gcd(\frac{a \mp 1}{g}, \frac{b}{g}) = 1$ it follows that $\gcd(\frac{2(a \mp 1)}{g^2}, (\frac{b}{g})^2) = 1$. Hence $\frac{2(a \mp 1)}{g^2} \mid d$, as required. ∎

Example 2.5. Let us construct a set of commutative solutions for the negative matrix Pell equation $\mathrm{X}^2 - 3\mathrm{Y}^2 = -\mathrm{I}$.

Theorem 2.1 suggest two sets of solutions. The first set consists of all matrices of the form

$$\mathrm{X} = \begin{pmatrix} t_1 & 0 \\ 0 & t_1 \end{pmatrix} \quad ; \quad \mathrm{Y} = \begin{pmatrix} t_4 & t_2 \\ t_3 & -t_4 \end{pmatrix}$$

where $t_1, t_2, t_3, t_4 \in \mathbb{Z}$ satisfy $t_1^2 - 3t_4^2 - 3t_2 t_3 = -1$. In this case, by Theorem 2.4(a), t_1 must satisfy the congruence $t_1^2 \equiv -1 (\mathrm{mod}\, 3)$. But this congruence has no solutions, so the first set does not yield any solution.

For the second set, let us choose a solution for the Pell equation $a^2 - 3b^2 = 1$, say $(a, b) = (7, -4)$. In this case $g = \gcd(a+1, b) = \gcd(8, -4) = 4$, so the corresponding matrix solutions are

$$\mathrm{X} = \begin{pmatrix} t_1 & \frac{a+1}{g} t_2 \\ \frac{a+1}{g} t_3 & 3bt_4 - at_1 \end{pmatrix} = \begin{pmatrix} t_1 & 2t_2 \\ 2t_3 & -12t_4 - 7t_1 \end{pmatrix}$$

and

$$\mathrm{Y} = \begin{pmatrix} t_4 & \frac{b}{g} t_2 \\ \frac{b}{g} t_3 & at_4 - bt_1 \end{pmatrix} = \begin{pmatrix} t_4 & -t_2 \\ -t_3 & 7t_4 + 4t_1 \end{pmatrix}$$

where $t_1, t_2, t_3, t_4 \in \mathbb{Z}$ satisfy $t_1^2 - 3t_4^2 + t_2t_3 = -1$, that is $t_2t_3 = 3t_4^2 - t_1^2 - 1$. Clearly, for any $t_1, t_4 \in \mathbb{Z}$, we can find suitable $t_2, t_2 \in \mathbb{Z}$. For example, if $t_1 = 1$ and $t_4 = -1$, then a suitable $t_2, t_3 \in \mathbb{Z}$ are such that $t_2t_3 = 1$. Taking in particular $t_2 = t_3 = -1$ yields the solutions

$$\mathrm{X} = \begin{pmatrix} 1 & -2 \\ -2 & 5 \end{pmatrix} \quad ; \quad \mathrm{Y} = \begin{pmatrix} -1 & 1 \\ 1 & -3 \end{pmatrix}.$$

Indeed

$$\mathrm{X}^2 - 3\mathrm{Y}^2 = \begin{pmatrix} 1 & -2 \\ -2 & 5 \end{pmatrix}^2 - 3\begin{pmatrix} -1 & 1 \\ 1 & -3 \end{pmatrix}^2 = \begin{pmatrix} 5 & -12 \\ -12 & 29 \end{pmatrix} - 3\begin{pmatrix} 2 & -4 \\ -4 & 10 \end{pmatrix} = -\mathrm{I}.$$

It is worthwhile mentioning that *not* every solution of $a^2 - 3b^2 = 1$ yields a set of solutions for $\mathrm{X}^2 - 3\mathrm{Y}^2 = -\mathrm{I}$. For example, if $(a, b) = (2, 1)$, then $g = 1$ and by Theorem 2.4(b) a suitable solution of $\mathrm{X}^2 - 3\mathrm{Y}^2 = -\mathrm{I}$ depends upon the condition

$$t_1^2 \equiv -1 \left(\mathrm{mod}\, \frac{a+1}{g^2} \right), \quad \text{that is} \quad t_1^2 \equiv -1 \,(\mathrm{mod}\, 3)\,.$$

Since this congruence is not solvable, it follows that $(a, b) = (2, 1)$ does not yield any solutions.

Note that if one changes the condition $t_1^2 - dt_4^2 \mp 2(a \mp 1)t_2t_3/g^2 = \pm 1$ to the condition $t_1^2 - dt_4^2 \mp 2(a \mp 1)t_2t_3/g^2 = c$ (where a, b and g are defined in the same manner), then it follows to (4) that the family of solutions describes in Theorem 2.1 is an infinite set of commuting solutions of the matrix Pell equations $\mathrm{X}^2 - d\mathrm{Y}^2 = c\mathrm{I}$ for arbitrary c. However, it is not clear whether the condition $t_1^2 - dt_4^2 \mp 2(a \mp 1)t_2t_3/g^2 = c$ is necessary. This is an interesting problem that lies out of the scope of this paper.

We end this section with a brief discussion concerning the cost of computing solutions. Our results imply that solving the matrix Pell equation involves solving the classical Pell equation over $\mathbb{Z}$, which is the bottleneck in these computations. If the solutions of the classical Pell equation $x^2 - dy^2 = 1$ are ordered by magnitude, then the n-th solution (x_n, y_n) with $x_n > 0$ and $y_n > 0$ can be expressed in terms of the first one (x_1, y_1) by $x_n + y_n\sqrt{d} = (x_1 + y_1\sqrt{d})^n$. Accordingly, the first solution (x_1, y_1) is called the *fundamental solution*. Therefore, solving the Pell-equation reduces to finding a fundamental solution. The standard method for finding the fundamental solution is computing the continued fractions for $\sqrt{d}$. It can be shown that the continued fraction method running time is at most $\sqrt{d}(1+\log d)^c$, where c some constant. For more details the reader can consult [4] or [7].

3. Non-Commuting Matrix Solutions of the Generalized Matrix Pell Equation

In this section, we shall find the non-commutative solutions of the generalized matrix Pell equation (1), namely $\mathrm{X}^2 - d\mathrm{Y}^2 = c\mathrm{I}$, for an arbitrary integer c. The following proposition will be crucial in order to solve (1) with non-commutative solutions.

Proposition 3.1. *Suppose that* X *and* Y *are* 2×2 *matrices over* $\mathbb{C}$ *such that* $\mathrm{XY} \neq \mathrm{YX}$ *and let* $c \in \mathbb{C}$. *If* $\mathrm{X}^2 + \mathrm{Y}^2 = c\mathrm{I}$, *then* $\mathrm{tr}(\mathrm{X}) = \mathrm{tr}(\mathrm{Y}) = 0$ *and* $|\mathrm{X}| + |\mathrm{Y}| = -c$.

Proof. Set

$$\mathrm{X} = \begin{pmatrix} x_1 & x_2 \\ x_3 & x_4 \end{pmatrix} \quad ; \quad \mathrm{Y} = \begin{pmatrix} y_1 & y_2 \\ y_3 & y_4 \end{pmatrix},$$

where the x_i's and y_i's are complex numbers. Note that

$$\mathrm{X}^2 + \mathrm{Y}^2 = \begin{pmatrix} x_1^2 + y_1^2 + x_2x_3 + y_2y_3 & x_2(x_1 + x_4) + y_2(y_1 + y_4) \\ x_3(x_1 + x_4) + y_3(y_1 + y_4) & x_4^2 + y_4^2 + x_2x_3 + y_2y_3 \end{pmatrix}.$$

Set $\alpha = x_1 + x_4$, $\alpha' = x_1 - x_4$ and $\beta = y_1 + y_4$, $\beta' = y_1 - y_4$. We shall prove that $\alpha = \beta = 0$. Since $\mathrm{X}^2 + \mathrm{Y}^2 = c\mathrm{I}$, it follows that

$$(9) \qquad \begin{cases} x_1^2 + y_1^2 + x_2x_3 + y_2y_3 = c & \text{(i)} \\ x_4^2 + y_4^2 + x_2x_3 + y_2y_3 = c & \text{(ii)} \\ x_3\alpha + y_3\beta = 0 & \text{(iii)} \\ x_2\alpha + y_2\beta = 0 & \text{(iv)}. \end{cases}$$

Let us look at the equations (iii) and (iv) of (9) as a homogeneous system of linear equations with two unknowns α and β.

If $x_3y_2 - x_2y_3 \neq 0$, then the solution of the this homogeneous system is $\alpha = \beta = 0$, as required. Next suppose that $x_3y_2 - x_2y_3 = 0$. By subtracting equation (ii) from (i), it follows that

$$x_1^2 + y_1^2 - (x_4^2 + y_4^2) = 0$$
$$(x_1 - x_4)(x_1 + x_4) + (y_1 - y_4)(y_1 + y_4) = 0,$$

that is

$$\alpha'\alpha + \beta'\beta = 0 \qquad \text{(v)}$$

If $x_3\beta' - y_3\alpha' \neq 0$, then the unique solution of the homogeneous system (iii) and (v) is $\alpha = \beta = 0$. Similarly, if $x_2\beta' - y_2\alpha' \neq 0$, then the unique solution of the homogeneous system (iv) and (v) is $\alpha = \beta = 0$, as required.

Suppose now that $x_3\beta' - y_3\alpha' = 0$ and $x_2\beta' - y_2\alpha' = 0$. Then

$$\begin{aligned} \mathrm{XY} - \mathrm{YX} &= \begin{pmatrix} x_2y_3 - x_3y_2 & y_2(x_1 - x_4) - x_2(y_1 - y_4) \\ x_3(y_1 - y_4) - y_3(x_1 - x_4) & x_3y_2 - x_2y_3 \end{pmatrix} \\ &= \begin{pmatrix} 0 & y_2\alpha' - x_2\beta' \\ x_3\beta' - y_3\alpha' & 0 \end{pmatrix} = \mathrm{O}, \end{aligned}$$

so $\mathrm{XY} = \mathrm{YX}$, which contradicts our assumptions.

It follows that $\alpha = \mathrm{tr}(\mathrm{X}) = 0$ and $\beta = \mathrm{tr}(\mathrm{Y}) = 0$. In order to prove that $|\mathrm{X}| + |\mathrm{Y}| = -c$, note that by the Cayley Hamilton Theorem

$$\mathrm{X}^2 + \mathrm{Y}^2 = \mathrm{tr}(\mathrm{X})\mathrm{X} + \mathrm{tr}(\mathrm{Y})\mathrm{Y} - (|\mathrm{X}| + |\mathrm{Y}|)\mathrm{I} = -(|\mathrm{X}| + |\mathrm{Y}|)\mathrm{I}.$$

Since $\mathrm{X}^2 + \mathrm{Y}^2 = c\mathrm{I}$, then it follows that $|\mathrm{X}| + |\mathrm{Y}| = -c$, as required. ■

Now we are ready to solve completely the generalized matrix Pell equation (1) for non-commutative 2×2 matrices over $\mathbb{Z}$. Note that in the following theorem we may assume that d is an arbitrary non-zero integer.

Theorem 3.2. *Suppose that* X *and* Y *are* 2×2 *matrices over* $\mathbb{Z}$, c *is an arbitrary integer and let* d *be a non-zero integer. Then* $\mathrm{X}^2 - d\mathrm{Y}^2 = c\mathrm{I}$ *and* $\mathrm{XY} \neq \mathrm{YX}$ *iff*

$$\mathrm{X} = \begin{pmatrix} t_1 & t_2 \\ t_3 & -t_1 \end{pmatrix} \quad ; \quad \mathrm{Y} = \begin{pmatrix} s_1 & s_2 \\ s_3 & -s_1 \end{pmatrix}$$

where $t_1, t_2, t_3, s_1, s_2, s_3 \in \mathbb{Z}$ *such that* $t_1^2 + t_2t_3 - d(s_1^2 + s_2s_3) = c$ *and the vectors* $\vec{t} = (t_1, t_2, t_3)$ *and* $\vec{s} = (s_1, s_2, s_3)$ *are linearly independent over the field* $\mathbb{Q}$ *of rational numbers.*

Proof. First we shall prove that the conditions in the theorem are sufficient. So suppose that

$$\mathrm{X} = \begin{pmatrix} t_1 & t_2 \\ t_3 & -t_1 \end{pmatrix} \quad ; \quad \mathrm{Y} = \begin{pmatrix} s_1 & s_2 \\ s_3 & -s_1 \end{pmatrix}$$

where $t_1, t_2, t_3, s_1, s_2, s_3 \in \mathbb{Z}$ such that $t_1^2 + t_2t_3 - d(s_1^2 + s_2s_3) = c$ and the vectors $\vec{t} = (t_1, t_2, t_3)$ and $\vec{s} = (s_1, s_2, s_3)$ are linearly independent over $\mathbb{Q}$. Then $\mathrm{tr}(\mathrm{X}) = \mathrm{tr}(\mathrm{Y}) = 0$ and $|\mathrm{X}| - d|\mathrm{Y}| = -c$. By the Cayley Hamilton Theorem $\mathrm{X}^2 - \mathrm{tr}(\mathrm{X})\mathrm{X} + |\mathrm{X}|\,\mathrm{I} = \mathrm{O}$ and $\mathrm{Y}^2 - \mathrm{tr}(\mathrm{Y})\mathrm{Y} + |\mathrm{Y}|\,\mathrm{I} = \mathrm{O}$. Hence

$$\mathrm{X}^2 - d\mathrm{Y}^2 = \mathrm{tr}(\mathrm{X})\mathrm{X} - |\mathrm{X}|\mathrm{I} - d\big(\mathrm{tr}(\mathrm{Y})\mathrm{Y} - |\mathrm{Y}|\mathrm{I}\big) = -\big(|\mathrm{X}| - d|\mathrm{Y}|\big)\mathrm{I} = c\mathrm{I},$$

as required.

Next we shall prove that $XY \neq YX$. Suppose otherwise that $XY = YX$. Hence $O = XY - YX$. Note that

$$XY - YX = \begin{pmatrix} s_3t_2 - s_2t_3 & 2(s_2t_1 - s_1t_2) \\ -2(s_3t_1 - s_1t_3) & -(s_3t_2 - s_2t_3) \end{pmatrix} = \begin{pmatrix} \begin{vmatrix} t_2 & t_3 \\ s_2 & s_3 \end{vmatrix} & 2\begin{vmatrix} t_1 & t_2 \\ s_1 & s_2 \end{vmatrix} \\ -2\begin{vmatrix} t_1 & t_3 \\ s_1 & s_3 \end{vmatrix} & -\begin{vmatrix} t_2 & t_3 \\ s_2 & s_3 \end{vmatrix} \end{pmatrix},$$

so

$$\begin{vmatrix} t_2 & t_3 \\ s_2 & s_3 \end{vmatrix} = 0 \quad ; \quad \begin{vmatrix} t_1 & t_3 \\ s_1 & s_3 \end{vmatrix} = 0 \quad ; \quad \begin{vmatrix} t_1 & t_2 \\ s_1 & s_2 \end{vmatrix} = 0.$$

The vector product of $\vec{t} = (t_1, t_2, t_3)$ and $\vec{s} = (s_1, s_2, s_3)$ is

$$\vec{t} \times \vec{s} = \begin{vmatrix} \hat{i} & \hat{j} & \hat{k} \\ t_1 & t_2 & t_3 \\ s_1 & s_2 & s_3 \end{vmatrix} = \hat{i}\begin{vmatrix} t_2 & t_3 \\ s_2 & s_3 \end{vmatrix} - \hat{j}\begin{vmatrix} t_1 & t_3 \\ s_1 & s_3 \end{vmatrix} + \hat{k}\begin{vmatrix} t_1 & t_2 \\ s_1 & s_2 \end{vmatrix},$$

where $\hat{i} = (1,0,0)$, $\hat{j} = (0,1,0)$ and $\hat{k} = (0,0,1)$. Therefore, $\vec{t} \times \vec{s} = \vec{0}$, so the vectors $\vec{t}$ and $\vec{s}$ are linearity dependent over $\mathbb{Q}$, which contradicts our assumption.

Now we shall prove that these conditions are necessary. Set

$$X = \begin{pmatrix} t_1 & t_2 \\ t_3 & t_4 \end{pmatrix} \quad ; \quad Y = \begin{pmatrix} s_1 & s_2 \\ s_3 & s_4 \end{pmatrix},$$

where the t's and s's are integers such that $XY \neq YX$ and $X^2 - dY^2 = cI$. Notice first, that the equation $X^2 - dY^2 = cI$ is equivalent to the equation $X^2 + (\sqrt{-d}Y)^2 = cI$. In addition, since $d \neq 0$, it follows that $XY \neq YX$ iff $X(\sqrt{-d}Y) \neq (\sqrt{-d}Y)X$. By Proposition 3.1 it follows that

$$|X| + |\sqrt{-d}Y| = -c$$

and

$$\mathrm{tr}(X) = 0 \text{ and } \mathrm{tr}(\sqrt{-d}Y) = 0,$$

that is

$$|X| - d|Y| = -c$$

and

$$\mathrm{tr}(X) = 0 \text{ and } \mathrm{tr}(Y) = 0.$$

Since $\mathrm{tr}(X) = t_1 + t_4$, it follows that $t_4 = -t_1$ and similarly that $s_4 = -s_1$. Consequently, $|X| = -t_1^2 - t_2t_3$ and $|Y| = -s_1^2 - s_2s_3$. Since $|X| - d|Y| = -c$ we deduce the condition $t_1^2 + t_2t_3 - d(s_1^2 + s_2s_3) = c$, as required.

In addition, recall that since $\mathrm{tr}(X) = 0$ and $\mathrm{tr}(Y) = 0$ it follows from the proof of the first part that $XY = YX$ iff $\vec{t} \times \vec{s} = \vec{0}$. Hence, if $XY \neq YX$, then $\vec{t}$ and $\vec{s}$ are linearly independent over $\mathbb{Q}$, as required. ∎

Example 3.3. Let us construct a non-commutative solution for the matrix Pell equation $X^2 - 2Y^2 = I$.

First let us choose a 2×2 matrix with zero trace, say

$$Y = \begin{pmatrix} -3 & 4 \\ -2 & 3 \end{pmatrix}.$$

The corresponding matrix X should be also with zero trace and should satisfy $|X| - 2|Y| = -1$, that is $|X| = -3$. As one can verify, the following matrix is suitable:

$$X = \begin{pmatrix} 1 & 1 \\ 2 & -1 \end{pmatrix}.$$

Note that the vectors $\vec{s} = (-3, 4, -2)$ and $\vec{t} = (1, 1, 2)$ are linearly independent over $\mathbb{Q}$, so X and Y are non-commutative. Now,

$$X^2 - 2Y^2 = \begin{pmatrix} 1 & 1 \\ 2 & -1 \end{pmatrix}^2 - 2\begin{pmatrix} -3 & 4 \\ -2 & 3 \end{pmatrix}^2 = \begin{pmatrix} 3 & 0 \\ 0 & 3 \end{pmatrix} - 2\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I.$$

Example 3.4. Let us construct a non-commutative solution for the matrix Pell Equation $X^2 + Y^2 = I$.

First let us choose a 2×2 matrix with zero trace, say

$$X = \begin{pmatrix} 1 & 2 \\ 3 & -1 \end{pmatrix}.$$

The corresponding matrix Y should be also with zero trace and should satisfy $|X| + |Y| = -1$, that is $|Y| = 6$. As one can verify, the following matrix is suitable:

$$Y = \begin{pmatrix} 2 & 2 \\ -5 & -2 \end{pmatrix}.$$

Note that the vectors $\vec{s} = (2, 2, -5)$ and $\vec{t} = (1, 2, 3)$ are linearly independent over $\mathbb{Q}$, so X and Y are non-commutative. Now,

$$X^2 + Y^2 = \begin{pmatrix} 1 & 2 \\ 3 & -1 \end{pmatrix}^2 + \begin{pmatrix} 2 & 2 \\ -5 & -2 \end{pmatrix}^2 = \begin{pmatrix} 7 & 0 \\ 0 & 7 \end{pmatrix} + \begin{pmatrix} -6 & 0 \\ 0 & -6 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I.$$

Example 3.5. Let us construct a non-commutative solution for the matrix equation $X^2 = 2Y^2$.

Note that equation $X^2 = 2Y^2$ can be written in the form $X^2 - 2Y^2 = 0I$. Hence we can apply Theorem 3.2 with $c = 0$. Therefore, the set of non-commutative solutions of the equation $X^2 = 2Y^2$ consist of the matrices

$$X = \begin{pmatrix} t_1 & t_2 \\ t_3 & -t_1 \end{pmatrix} \quad ; \quad Y = \begin{pmatrix} s_1 & s_2 \\ s_3 & -s_1 \end{pmatrix}$$

where $t_1, t_2, t_3, s_1, s_2, s_3 \in \mathbb{Z}$ such that $t_1^2 + t_2 t_3 = 2(s_1^2 + s_2 s_3)$ and the vectors $\vec{t} = (t_1, t_2, t_3)$ and $\vec{s} = (s_1, s_2, s_3)$ are linearly independent over $\mathbb{Q}$. In particular, let us take the vectors $\vec{s} = (3, -1, 4)$ and $\vec{t} = (2, 2, 3)$. Clearly, $\vec{s}$ and $\vec{t}$ are linearly independent over $\mathbb{Q}$, so X and Y are non-commutative. Now,

$$\mathrm{X}^2 - 2\mathrm{Y}^2 = \begin{pmatrix} 2 & 2 \\ 3 & -2 \end{pmatrix}^2 - 2\begin{pmatrix} 3 & -1 \\ 4 & -3 \end{pmatrix}^2 = \begin{pmatrix} 10 & 0 \\ 0 & 10 \end{pmatrix} - 2\begin{pmatrix} 5 & 0 \\ 0 & 5 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = \mathrm{O}.$$

REFERENCES

[1] Z. Cao and A. Grytczuk, *Fermat's type equations in the set of* 2×2 *integral matrices*, Tsukuba J. Math. **22** (1998) 637–643.

[2] A. Grytczuk and I. Kurzydło, *On the matrix negative Pell equation*, Discuss. Math. GAA **29** (2009) 35–45.
doi:10.7151/dmgaa.1150

[3] K. Hoffman and R. Kunze, Linear Algebra, 2 ed. (Prentice Hall, Englewood Cliffs, New Jersey, 1971).

[4] H.W. Lenstra, Jr., *Solving the Pell equation*, Sci. Res. Inst. Publ. **44** (2008) 1–23.

[5] W.J. LeVeque, Topics in Number Theory, vol. 1, (Addison-Wesley Publishing Co., Reading Massachusetts, 1956).

[6] Ch. Li and M. Le, *On Fermat's equation in integral* 2×2 *matrices*, Periodica Mathematica Hungarica **31** (1995) 219–222.

[7] R. Sawilla, A. Silvester and H.C. Williams, *A new look at an old equation*, Algorithmic Number Theory, proceedings of ANTS-VIII, Lecture Notes in Computer Science **5011** (2008) 39–59.
doi:10.1007/978-3-540-79456-1_2

[8] L.N. Vaserstein, *Non-commutative number theory in Algebraic K-theory and algebraic number theory*, Amer. Math. Soc. **83** (1989) 445–449.
doi:http://dx.doi.org/10.1090/conm/083

[9] W. Intrarapak and S. Prugsapitak, *On some Diophantine problems in* 2×2 *integer matrices*, ScienceAsia **39** (2013) 653–655.
doi:10.2306/scienceasia1513-1874.2013.39.653

Received 27 January 2016
1st Revised 29 January 2016
2st Revised 6 December 2016