On some applications of 2×2 integral matrices

A. GRYTCZUK and N. T. VOROBÈV

Abstract. In this paper we give a matrix representation for the fundamental solution of the Pellian type equation $x^2 - dy^2 = -1$. Using matrices the solutions of linear equations are also represented.

In 1970, in [1] some connections was given between integral 2×2 matrices and the Diophantine equation $ax - by = c$. Namely, we proved that the solution $\langle x_0, y_0 \rangle$ of this equation can be determined by the following equalities:

$$(1) \qquad \begin{pmatrix} a & y_0 \\ b & x_0 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^{q_0} \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}^{q_1} \cdots \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^{q_m} \begin{pmatrix} 0 & -c \\ 1 & 0 \end{pmatrix}$$

if m is even, and

$$(2) \qquad \begin{pmatrix} a & y_0 \\ b & x_0 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^{q_0} \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}^{q_1} \cdots \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}^{q_m} \begin{pmatrix} 1 & 0 \\ 0 & c \end{pmatrix}$$

if m is odd, where $\frac{a}{b} = [q_0; q_1, \ldots, q_m]$ is a representation of $\frac{a}{b}$ as a simple finite continued fraction.

For example, consider the equation

$$19x - 11y = -2.$$

We have $\frac{19}{11} = [1; 1, 2, 1, 2]$ and consequently $q_0 = 1, q_1 = 1, q_2 = 2, q_3 = 1, q_4 = 2$, thus $m = 4$ and by (1) we obtain

$$(3) \qquad \begin{pmatrix} 19 & y_0 \\ 11 & x_0 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^2 \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^2 \begin{pmatrix} 0 & 2 \\ 1 & 0 \end{pmatrix}.$$

By Cauchy's theorem on product of determinants it follows from (3) that

$$(4) \qquad 19x_0 - 11y_0 = -2.$$

So denote that $\langle x_0, y_0 \rangle$ is an integer solution of the equation $19x - 11y = -2$.

On the other hand by an easy calculation, from (3) we obtain

$$\begin{pmatrix} 19 & y_0 \\ 11 & x_0 \end{pmatrix} = \begin{pmatrix} 7 & 19 \\ 4 & 11 \end{pmatrix} \begin{pmatrix} 0 & 2 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 19 & 14 \\ 11 & 8 \end{pmatrix}. \tag{5}$$

By (5) it follows that $x_0 = 8, y_0 = 14$.

In 1986 A. J. van der Poorten [3] observed that if

$$\begin{pmatrix} c_0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} c_1 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} c_n & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} p_n & p_{n-1} \\ q_n & q_{n-1} \end{pmatrix}, \quad n = 0, 1, \ldots$$

then

$$\frac{p_n}{q_n} = [c_0; c_1, \ldots, c_n].$$

Based on this observation he gave many interesting applications to the theory of continued fraction and also to the description of the solutions of the well-known Pell's equation $x^2 - dy^2 = 1$. In [2] we gaves some connections between fundamental solution $\langle x_0, y_0 \rangle$ of the Pell's equation and representation of 2×2 integral matrix as a product of powers of the prime elements in the unimodular group.

In the present paper we give such connections between the fundamental solution $\langle x_0, y_0 \rangle$ of the non-Pellian equation $x^2 - dy^2 = -1$ and the corresponding matrix representation. We prove the following:

Theorem 1. Let

$$\sqrt{d} = [q_0; \overline{q_1, \ldots, q_s}], \quad d > 0 \quad \text{and} \quad s > 1 \quad \text{is odd}$$

is odd, be the representation of $\sqrt{d}$ as a simple periodic continued fraction. Then the fundamental solution $\langle x_0, y_0 \rangle$ of the non-Pellian equation

$$x^2 - dy^2 = -1 \tag{6}$$

in contained in the second column of the following matrix:

$$F_0 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^{q_0} \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}^{q_1} \cdots \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^{q_{s-1}}. \tag{7}$$

Proof. First we prove that if $k = 2n, n = 1, 2, \ldots$, then

$$\begin{pmatrix} 1 & q_0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ q_1 & 1 \end{pmatrix} \cdots \begin{pmatrix} 1 & q_k \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} P_{k-1} & P_k \\ Q_{k-1} & Q_k \end{pmatrix} \tag{8}$$

where $P_0 = q_0, Q_0 = 1, P_1 = q_0 q_1 + 1, Q_1 = q_1$ and

$$P_k = q_k P_{k-1} + P_{k-2}, \quad Q_k = q_k Q_{k-1} + Q_{k-2}; \quad k = 2n, n = 1, 2, \ldots \tag{9}$$

It is easy to see that (8) is true for $k = 2$. Suppose that (8) is true for some $k = 2m$. Then we have

$$\begin{pmatrix} P_{2m-1} & P_{2m} \\ Q_{2m-1} & Q_{2m} \end{pmatrix} \begin{pmatrix} 1 & 0 \\ q_{2m+1} & 1 \end{pmatrix} \begin{pmatrix} 1 & q_{2m+2} \\ 0 & 1 \end{pmatrix}$$

$$= \begin{pmatrix} P_{2m-1} + q_{2m+1} P_{2m} & P_{2m} \\ Q_{2m-1} + q_{2m+1} Q_{2m} & Q_{2m} \end{pmatrix} \begin{pmatrix} 1 & q_{2m+2} \\ 0 & 1 \end{pmatrix}. \tag{10}$$

By (9) and (10) it follows that

$$\begin{pmatrix} P_{2m-1} & P_{2m} \\ Q_{2m-1} & Q_{2m} \end{pmatrix} \begin{pmatrix} 1 & 0 \\ q_{2m+1} & 1 \end{pmatrix} \begin{pmatrix} 1 & q_{2m+2} \\ 0 & 1 \end{pmatrix}$$

$$= \begin{pmatrix} P_{2m+1} & P_{2m} \\ Q_{2m+1} & Q_{2m} \end{pmatrix} \begin{pmatrix} 1 & q_{2m+2} \\ 0 & 1 \end{pmatrix}. \tag{11}$$

Denoting the left hand side of (11) by F we obtain

$$F = \begin{pmatrix} P_{2m+1} & P_{2m} + q_{2m+2} P_{2m+1} \\ Q_{2m+1} & Q_{2m} + q_{2m+2} Q_{2m+1} \end{pmatrix} = \begin{pmatrix} P_{2m+1} & P_{2m+2} \\ Q_{2m+1} & Q_{2m+2} \end{pmatrix}. \tag{12}$$

By (12), (11) and (10) it follows that (8) is true for $k = 2m + 2$, thus by induction (8) is true for every $k = 2n$, $n = 1, 2, \ldots$

Now, we can consider the following product:

$$F_0 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^{q_0} \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}^{q_1} \cdots \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^{q_{s-1}}, \quad s > 1. \tag{13}$$

Since

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^m = \begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}^m = \begin{pmatrix} 1 & 0 \\ m & 1 \end{pmatrix}, \tag{14}$$

for every positive integer m, then by (13), (14) and (8) for the case $k = s-1$ we obtain

$$F_0 = \begin{pmatrix} P_{s-2} & P_{s-1} \\ Q_{s-2} & Q_{s-1} \end{pmatrix}. \tag{15}$$

On the other hand by (13) and (15) we get

$$\det F_0 = 1 = P_{s-2}Q_{s-1} - P_{s-1}Q_{s-2}. \tag{16}$$

Since

$$P_{s-1} = q_0 Q_{s-1} + Q_{s-2} \quad \text{and} \quad dQ_{s-2} = q_0 P_{s-1} + P_{s-2}, \tag{17}$$

by (17) we have

$$P_{s-1}^2 - dQ_{s-1}^2 = P_{s-1}Q_{s-2} - P_{s-2}Q_{s-1}. \tag{18}$$

On the other hand it is well-known that

$$P_{s-1}Q_{s-2} - P_{s-2}Q_{s-1} = (-1)^s. \tag{19}$$

Since $s > 1$ and s is odd then by (18), (19) and (16) we obtain

$$P_{s-1}^2 - dQ_{s-1}^2 = -1, \tag{20}$$

so $\langle x_0, y_0 \rangle = \langle P_{s-1}, Q_{s-1} \rangle$ and the proof is complete.

For example consider the following non-Pellian equation:

$$x^2 - 13y^2 = -1.$$

We have $\sqrt{13} = [3; 1, 1, 1, 1, 6]$ and $q_0 = 3$, $q_1 = q_2 = q_3 = q_4 = 1$, $q_5 = 6$; $s = 5$ is odd. Then by the Theorem 1 we have

$$F_0 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^3 \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} =$$

$$= \begin{pmatrix} 1 & 3 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} = \begin{pmatrix} 4 & 7 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} = \begin{pmatrix} 11 & 18 \\ 3 & 5 \end{pmatrix},$$

and consequently $x_0 = 18, y_0 = 5$.

Now, we gave a possibility for an application of 2×2 integral matrices to the examination of the equation:

$$a_1 x_1 + a_2 x_2 + \cdots + a_n x_n = b. \tag{22}$$

Namely, we prove the following:

Theorem 2. Let $(a_1, a_2, \ldots, a_n) = 1$ and $d = (a_i, a_j)$ for some $i, j \in \{1, 2, \ldots, n\}$, where $(a_1, a_2, \ldots, a_n)$ denote the greatest common divisor of $a_1, a_2, \ldots, a_n \in Z$. Then the integer solutions of (22) are of the form:

$$\langle v_1, v_2, \ldots, x_i, \ldots, x_j, \ldots, v_n \rangle,$$

where x_i, x_j are detemrined by the following matrix equalities:

$$(23) \quad \begin{pmatrix} a_i & -x_i \\ a_j & x_i \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^{q_0} \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}^{q_1} \cdots \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^{q_m} \begin{pmatrix} 0 & -\frac{D}{d} \\ d & 0 \end{pmatrix},$$

if m is even and

$$(24) \quad \begin{pmatrix} a_i & -x_i \\ a_j & x_i \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^{q_0} \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}^{q_1} \cdots \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}^{q_m} \begin{pmatrix} d & 0 \\ 0 & \frac{D}{d} \end{pmatrix},$$

if m is odd, where $\frac{a_i}{a_j} = [q_0; q_1, \ldots, q_m]$, $d \mid D$ and $D = b - \sum\limits_{\substack{k=1 \\ k \neq i,j}}^{m} a_k v_k$.

Proof. Let $(a_i, a_j) = d$. We can assume without loss of generality that $a_i \geq a_j > 0$. Applying to a_i, a_j the well-known theorem on division with remainder we obtain

$$(25) \quad a_i = a_j q_0 + r_1, \quad a_j = a_i q_1 + r_2, \ldots, r_{m-1} = r q_m,$$

$$0 < r_m < r_{m-1} < \ldots < r_1 < a_j$$

and

$$r_m = (a_i, a_j) = d.$$

Let $A = \begin{pmatrix} a_i & -x_j \\ a_j & x_i \end{pmatrix}$, then by (25) we obtain

$$A = \begin{pmatrix} a_j q_0 + r_1 & -x_j \\ a_j & x_i \end{pmatrix} = \begin{pmatrix} 1 & q_0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} r_1 & -(x_j + q_0 x_i) \\ a_j & x_i \end{pmatrix}.$$

Denoting by $x_j^{(1)} = -(x_j + q_0 x_i)$ and by $A_1 = \begin{pmatrix} r_1 & x_j^{(1)} \\ a_j & x_i \end{pmatrix}$ in similar way we obtain

$$A_1 = \begin{pmatrix} 1 & 0 \\ q_1 & 1 \end{pmatrix} \begin{pmatrix} r_1 & x_j^{(1)} \\ r_2 & x_i - q_1 x_j^{(1)} \end{pmatrix}.$$

Denoting by $x_j^{(1)} = x_i - q_1 x_j^{(1)}$ and by $A_2 = \begin{pmatrix} r_1 & x_j^{(1)} \\ r_2 & x_i^{(1)} \end{pmatrix}$ we obtain

$$A_2 = \begin{pmatrix} 1 & q_2 \\ 0 & 1 \end{pmatrix} A_3.$$

Continuing this process we obtain in the last step the following matrices

$$\begin{pmatrix} r_m & 0 \\ 0 & x_i^{(1)} \end{pmatrix} \quad \text{or} \quad \begin{pmatrix} 0 & x_j^{(1)} \\ r_m & 0 \end{pmatrix}.$$

Consequently we obtain the following representation:

$$A = \begin{pmatrix} a_i & -x_j \\ a_j & x_i \end{pmatrix} = \begin{pmatrix} 1 & q_0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ q_1 & 1 \end{pmatrix} \cdots \begin{pmatrix} 1 & q_m \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & x_j^{(1)} \\ d & 0 \end{pmatrix} \tag{26}$$

if m is even, or

$$A = \begin{pmatrix} 1 & q_0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ q_1 & 1 \end{pmatrix} \cdots \begin{pmatrix} 1 & 0 \\ q_m & 1 \end{pmatrix} \begin{pmatrix} d & 0 \\ 0 & x_i^{(1)} \end{pmatrix} \tag{27}$$

if m is odd. From (26) we have

$$\det A = a_i x_i + a_j x_j = D = -d x_j^{(1)}$$

and we obtain $d \mid D$. On the other hand putting $x_k = v_k$ for $k = 1, 2, \ldots, n$ and $k \neq i, j$ we have

$$D = a_i x_i + a_j x_j = b - \sum_{\substack{k=1 \\ k \neq i,j}}^{n} a_k v_k.$$

In similar way by (27) it follows that $\det A = D = d x_j^{(1)}$ and we obtain $d \mid D$. In both cases we have $x_i^{(1)} = -\frac{D}{d}$ if m is even and $x_i^{(1)} = \frac{D}{d}$ if m is odd.
Hence, from (27) and (26) we obtain (23)–(24) and the proof is complete.

Consider the following equation:

$$12x + 7y + 5z = 24. \tag{28}$$

We have $(12, 7, 5) = 1$. Equation (28) can be represented in the form

$$7y + 5z = 24 - 12x = 12(2 - a); \quad x = a.$$

On the other hand, we have:

$$\frac{7}{5} = [1; 2, 2].$$

By the Theorem 2, we have:

$$A = \begin{pmatrix} 7 & -z \\ 5 & y \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}^2 \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^2 \begin{pmatrix} 0 & -(24 - 12a) \\ 1 & 0 \end{pmatrix},$$

where $D = \det A = 24 - 12a$, $d = (7, 5) = 1$, thus $d \mid D$. So we obtain

$$A = \begin{pmatrix} 7 & -z \\ 5 & y \end{pmatrix} = \begin{pmatrix} 3 & 1 \\ 2 & 1 \end{pmatrix} \begin{pmatrix} 2 & -(24 - 12a) \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 7 & -3(24 - 12a) \\ 5 & -2(24 - 12a) \end{pmatrix}.$$

and we have

$$x = a, \quad y = -2(24 - 12a), \quad z = 3(24 - 12a),$$

where a is an arbitrary integer.

References

[1] A. GRYTCZUK, Application of integral matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ to the determination of integer solutions of the equation $ax - by = \pm 1$, *Biul. WSInz. Mat.–Fiz.* № 4., (1970), Zielona Góra, 149–153, (in Polish).

[2] A. GRYTCZUK and N. T. VOROB'EV, Applicaiton of matrices to the solutions of Diophantine equations, Vitebsk, Bielyorussia, (1990), (pp. 44), (in Russian).

[3] A. J. VAN DER POORTEN, An introduction to continued fractions, *London Math. Soc. Lect. Note Ser.* № 109., (1986), 99–138.