MATRIX DIOPHANTINE EQUATIONS OVER QUADRATIC RINGS AND THEIR SOLUTIONS

LADZORYSHYN N.B.¹, PETRYCHKOVYCH V.M.¹, ZELISKO H.V.²

The method for solving the matrix Diophantine equations over quadratic rings is developed. On the basis of the standard form of matrices over quadratic rings with respect to \((z, k)\)-equivalence previously established by the authors, the matrix Diophantine equation is reduced to equivalent matrix equation of the same type with triangle coefficients. Solving this matrix equation is reduced to solving a system of linear equations that contains linear Diophantine equations with two variables, their solution methods are well-known. The structure of solutions of matrix equations is also investigated. In particular, solutions with bounded Euclidean norms are established. It is shown that there exists a finite number of such solutions of matrix equations over Euclidean imaginary quadratic rings. An effective method of constructing such solutions is suggested.

Key words and phrases: quadratic ring, matrix, \((z, k)\)-equivalence of matrices, matrix Diophantine equation, solution of matrix equation.

¹ Pidstryhach Institute for Applied Problems of Mechanics and Mathematics, 3b Naukova str., 79060, Lviv, Ukraine
² Ivan Franko National University, 1 Universytetska str., 79000, Lviv, Ukraine
E-mail: natalja.ladzoryshyn@gmail.com (Ladzoryshyn N.B.), vas_petrych@yahoo.com (Petrychkovych V.M.), zelisko_halya@yahoo.com (Zelisko H.V.)

INTRODUCTION AND PRELIMINARY RESULTS

The Sylvester-type matrix linear equations, the Lyapunov matrix equations, the matrix Diophantine equations arise in different sections of mathematics and are used in problems of control and dynamical systems theory [5,7,18,19,21]. New methods to solve such matrix equations over different domains, to describe the structure of their solutions are needed. There are some ways to solve such equations over the field, that is, the elements of their coefficient matrices are from the field [13]. For Sylvester-type polynomial matrix equations the conditions of the existence and uniqueness of the so-called minimum solutions are specified in the case when the coefficients of the equation are regular matrices [4]. In [1, 3] there are estimated degrees of the solutions of such matrix equations in the case where both the coefficients of the matrix equation may be nonregular. A special form of polynomial matrices, established in [6, 14, 15], with respect to semiscalar equivalence is applied. In [2], authors use obtained in [16, 17] the standard form of pair of matrices relative to generalized equivalence for describing solutions of matrix unilateral and bilateral equations over the principal ideal rings and Bezout rings. In [11], the criteria for solvability of matrix linear unilateral and bilateral equations over arbitrary quadratic rings are established, and in [9] integer solutions of these equations are described. In this article, it is proposed a method of constructing solutions of the matrix Diophantine equations over quadratic rings and described their structure with application.
Standard forms of matrices and their pairs with respect to \((z,k)\)-equivalence are established in the works [8, 10, 12, 20].

The quadratic ring \(K = \mathbb{Z} \left[ \sqrt{k} \right] \), where \(\mathbb{Z}\) is a ring of integers, \(k \in \mathbb{Z}, k \neq 0, 1\) and \(k\) is not divisible by the square of prime number, is formed by the following elements:

\[
\mathbb{Z} \left[ \sqrt{k} \right] = \left\{ a_1 + a_2 \sqrt{k} \mid a_1, a_2 \in \mathbb{Z} \right\} \quad \text{if } k \equiv 2, 3 \pmod{4};
\]

\[
\mathbb{Z} \left[ \sqrt{k} \right] = \left\{ \frac{a_1}{2} + \frac{a_2}{2} \sqrt{k} \mid a_1, a_2 \in \mathbb{Z}, (a_1 - a_2) \text{ divided by 2} \right\} \quad \text{if } k \equiv 1 \pmod{4}.
\]

The quadratic ring \(K = \mathbb{Z} \left[ \sqrt{k} \right] \) is called real if \(k > 0\). If \(k < 0\), then it is called an imaginary quadratic ring.

Let \(K\) be a Euclidean quadratic ring. Then the Euclidean norm of an element of \(K\) is defined as:

\[
\text{if } k < 0, \quad \mathcal{E}(a + b \sqrt{k}) = a^2 - kb^2 \quad \text{or} \quad \mathcal{E}\left(\frac{a}{2} + \frac{b}{2} \sqrt{k}\right) = \frac{1}{4} \left(a^2 - kb^2\right);
\]

\[
\text{if } k > 0, \quad \mathcal{E}(a + b \sqrt{k}) = \left|a^2 - kb^2\right| \quad \text{or} \quad \mathcal{E}\left(\frac{a}{2} + \frac{b}{2} \sqrt{k}\right) = \frac{1}{4} \left(a^2 - kb^2\right)
\]

depending on the appearance (1) or (2) of the element of a ring \(K\).

Associated elements have the same Euclidean norm. Note that \(u\) is a unit if and only if \(\mathcal{E}(u) = \pm 1\). The Euclidean norm is completely multiplicative, i.e. \(\mathcal{E}(ab) = \mathcal{E}(a)\mathcal{E}(b)\), from here we can get for the norm of the proportion of elements that \(\mathcal{E}\left(\frac{a}{b}\right) = \frac{\mathcal{E}(a)}{\mathcal{E}(b)}\).

In [12], the concept of \((z,k)\)-equivalence of matrices and their pairs over quadratic rings is introduced.

The matrices \(A, B \in M\left(m, n, \mathbb{Z} \left[ \sqrt{k} \right]\right)\) are called \((z,k)\)-equivalent if there exist invertible matrices \(S\) over a ring of integers \(\mathbb{Z}\) and \(Q\) over a quadratic ring \(K = \mathbb{Z} \left[ \sqrt{k} \right]\), such that \(A = SBQ\).

In the same article there is also established a standard form for matrices of order \(n\) over Euclidean quadratic rings and quadratic principal ideal rings. Using this form, the solutions of the matrix equation over these rings are described.

Without difficulty, we will write down the standard form for the rectangular matrix \(A\) of order \(m \times n\) with respect to \((z,k)\)-equivalence.

Let \(A \in M\left(m, n, K\right), m \leq n\), and

\[
D^A = \text{diag}\left(\mu_1^A, \ldots, \mu_m^A, 0, \ldots, 0\right), \quad \mu_i | \mu_{i+1}, i = 1, \ldots, m-1,
\]

is the Smith normal form of matrix \(A, \mu_i, i = 1, \ldots, m,\) are the invariant factors of matrix \(A\). Then a matrix \(A\) is \((z,k)\)-equivalent to the triangular matrix

\[
T^A = SAQ = \begin{vmatrix}
\mu_1 & 0 & \cdots & 0 & 0 & \cdots & 0 \\
t_{21} \mu_1 & \mu_2 & \cdots & 0 & 0 & \cdots & 0 \\
t_{m1} \mu_1 & t_{m2} \mu_2 & \cdots & \mu_m & 0 & \cdots & 0
\end{vmatrix},
\]

where \(S \in GL\left(m, \mathbb{Z}\right), Q \in GL\left(n, \mathbb{Z} \left[ \sqrt{k} \right]\right)\) and

\[
t_{ij} = 0, \quad \text{if } \mu_i = 1, \quad i, j = 1, \ldots, m, j < i;
\]
where A, K matrices over a Euclidean quadratic ring Z, over an imaginary Euclidean quadratic ring and the easy way to find them is proposed. It is established that there exists a finite number of such solutions of the matrix equation of these equations are described, in particular solutions of bounded Euclidean norms are isolated. The solutions with certain properties with matrices-coefficient in triangular standard forms. The solutions with certain properties of these equations are described, in particular solutions of bounded Euclidean norms are isolated. It is established that there exists a finite number of such solutions of the matrix equation over an imaginary Euclidean quadratic ring and the easy way to find them is proposed.

1 SOLUTIONS OF THE MATRIX DIOPHANTINE EQUATION

Consider the matrix Diophantine equation

\[ AX + BY = C, \]

where A, B, C ∈ M(m, n, K), m ≤ n, are known matrices and X, Y ∈ M(n, K) are unknown matrices over a Euclidean quadratic ring \( \mathbb{K} = \mathbb{Z} \left[ \sqrt{k} \right] \).

Let the pair of matrices \((A, B)\) from matrix equation (5) be \((z, k)\)-equivalent to the pair \((T^A, T^B)\) in standard forms \(T^A\) and \(T^B\) of matrices \(A\) and \(B\), that is

\[
T^A = SAQ^A = \begin{vmatrix}
\mu^A_1 & 0 & \cdots & 0 & 0 & \cdots & 0 \\
\mu^A_2 & 0 & \cdots & 0 & 0 & \cdots & 0 \\
\cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\
\mu^A_m & 0 & \cdots & 0 & 0 & \cdots & 0
\end{vmatrix}
\]

\[ (6) \]

and

\[
T^B = SBQ^B = \begin{vmatrix}
\mu^B_1 & 0 & \cdots & 0 & 0 & \cdots & 0 \\
\mu^B_2 & 0 & \cdots & 0 & 0 & \cdots & 0 \\
\cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\
\mu^B_m & 0 & \cdots & 0 & 0 & \cdots & 0
\end{vmatrix},
\]

\[ (7) \]

where \( S \in GL(m, Z) \), \( Q^A, Q^B \in GL(n, \mathbb{Z} \left[ \sqrt{k} \right]) \) and the elements \( t^A_{ij}, t^B_{ij}, i, j = 1, \ldots, m, i < j \), satisfy the conditions (3) and (4).

Then considering the ratio (6) and (7) between the matrices \(A, B\) and its standard forms \(T^A, T^B\) from the matrix equation (5) we obtain the following equation

\[ SAQ^A \left( Q^A \right)^{-1} X + SBQ^B \left( Q^B \right)^{-1} Y = SC. \]
Using the right elementary operations, reduce the matrix $SC$ to the lower triangular form, that is, for some invertible matrix $V \in GL(n, \mathbb{K})$ we have

$$SCV = \begin{vmatrix} \hat{c}_{11} & 0 & \ldots & 0 & \ldots & 0 \\ \hat{c}_{21} & \hat{c}_{22} & \ldots & 0 & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\ \hat{c}_{m1} & \hat{c}_{m2} & \ldots & \hat{c}_{mm} & \ldots & 0 \end{vmatrix} = \hat{C}.$$ 

Then from the matrix equation (8) we obtain the following equation

$$SAQ^A \left( \left( Q^A \right)^{-1} XV \right) + SBQ^B \left( \left( Q^B \right)^{-1} YV \right) = SCV$$

or

$$T^A H + T^B W = \hat{C}, \quad (9)$$

where

$$H = \left( Q^A \right)^{-1} XV, \quad W = \left( Q^B \right)^{-1} YV, \quad \hat{C} = SCV. \quad (10)$$

Matrix equations (5) and (9) are equivalent, i.e. the matrix equation (5) has a solution if and only if the matrix equation (9) is solvable and the solutions of these equations are related by a relation (10). Therefore, the description of the solutions of the matrix equation (5) is reduced to the description of the solutions of the matrix equation (9) with the matrix-coefficients of triangular forms, and therefore it is simpler. In [12], it is established that the Sylvester-type matrix equation $AX + YB = C$ with matrix-coefficients from Euclidean quadratic ring is equivalent to the matrix equation with the coefficients $T^A$ and $T^B$ in the standard forms of the matrices $A$ and $B$. If this matrix equation is solvable, then it has solutions with bounded Euclidean norms. It should be noted that not every solvable matrix Diophantine equation (9) over such a ring has solutions with such restrictions. We establish the matrix equations for which such solutions exist.

**Theorem 1.** Let $\mathbb{K}$ be a Euclidean quadratic ring, $A, B, C \in M(m, n, \mathbb{K}), m \leq n,$

$$D^B = \text{diag}(1, \ldots, 1, \mu_{i+1}^B, \mu_{i+2}^B, \ldots, \mu_{l}^B, 0, \ldots, 0), \quad \mu_{i+1}^B \neq 1, \quad l \geq 0,$$

be the Smith normal form of matrix $B$ with a matrix equation $(9)$, $d_m^A$ and $d_m^B$ are greatest common divisors of minors of the $m$-th order of matrices $A$ and $B$, respectively. If $(d_m^A, d_m^B) = 1$, then a matrix equation $(9)$ has such solutions

$$H = \begin{vmatrix} 0 & \ldots & 0 & 0 & \ldots & 0 & 0 & \ldots & 0 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & \ldots & 0 & 0 & \ldots & 0 & 0 & \ldots & 0 \\ h_{l+1,1} & \ldots & h_{l+1,l+1} & 0 & \ldots & 0 & 0 & \ldots & 0 \\ h_{l+2,1} & \ldots & h_{l+2,l+1} & h_{l+2,l+2} & \ldots & 0 & \ldots & 0 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ h_{m1} & \ldots & h_{m,l+1} & h_{m,l+2} & \ldots & h_{mm} & 0 & \ldots & 0 \\ 0 & \ldots & 0 & 0 & \ldots & 0 & 0 & \ldots & 0 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & \ldots & 0 & 0 & \ldots & 0 & 0 & \ldots & 0 \end{vmatrix}. $$
Proof. It is known that the matrix equation (5) is solvable if and only if the left greatest common divisor of the matrices $A$ and $B$ is the left divisor of the matrix $C$. Since $(d^A_m, d^B_m) = 1$, then it is obvious that this condition is true and the matrix equation (9) is solvable. From the matrix equation (9) we obtain the following system of equations:

$$\sum_{s=1}^{i} (t^A_{is} h^A_s w^B_j + t^B_{is} \mu^B_i w^B_j) = \xi_{ij}, \quad i = 1, \ldots, m, \quad j = 1, \ldots, n,$$

(13)

where $t^A_{ss} = t^B_{ss} = 1$ and $\xi_{ij} = 0, j > i$.

Consider the subsystem of system (13) at $i = 1, j = 1, \ldots, n$

$$\begin{align*}
\mu^A_1 h^A_{11} + \mu^B_1 w^B_{11} &= \xi_{11}, \\
\mu^A_1 h^A_{12} + \mu^B_1 w^B_{12} &= 0, \\
\vdots \\
\mu^A_1 h^A_{1m} + \mu^B_1 w^B_{1m} &= 0, \\
\mu^A_1 h^A_{1,m+1} + \mu^B_1 w^B_{1,m+1} &= 0, \\
\vdots \\
\mu^A_1 h^A_{1n} + \mu^B_1 w^B_{1n} &= 0.
\end{align*}

(14)

Since,

$$d^A_m = d^T_m = \mu^A_1 \mu^A_2 \cdots \mu^A_m, \quad d^B_m = d^T_m = \mu^B_1 \mu^B_2 \cdots \mu^B_m,$$

then $(\mu^A_i, \mu^B_j) = 1$ for all $i, j = 1, \ldots, m$. And therefore $(\mu^A_1, \mu^B_1) = 1$ and the first equation of this system has solutions, then obviously a subsystem (14) is solvable. From [12, Lemma 2] it is known that there exists solution $h^0_{11}, w^0_{11}$ of an equation

$$\mu^A_1 h^A_{11} + \mu^B_1 w^B_{11} = \xi_{11},$$

(15)

such that

$$\mathcal{E} \left( h^0_{11} \right) < \mathcal{E} \left( \mu^B_1 \right).$$

Obviously, the following $n - 1$ equations from subsystem (14) have zero solutions

$$h^0_{1j} = 0, \quad w^0_{1j} = 0, \quad j = 2, 3, \ldots, n.$$
For $i = 2, j = 1, \ldots, n$, we have such subsystem

$$
\begin{align*}
&\begin{cases}
   t_{21}^A \mu_1^A h_{11} + \mu_2^A h_{21} + t_{21}^B \mu_1^B w_{11} + \mu_2^B w_{21} = \epsilon_{21}, \\
   t_{21}^A \mu_1^B h_{12} + \mu_2^A h_{22} + t_{21}^B \mu_1^B w_{12} + \mu_2^B w_{22} = \epsilon_{22}, \\
   t_{21}^A \mu_1^A h_{13} + \mu_2^A h_{23} + t_{21}^B \mu_1^B w_{13} + \mu_2^B w_{23} = 0, \\
   \vdots \\
   t_{21}^A \mu_1^A h_{1m} + \mu_2^A h_{2m} + t_{21}^B \mu_1^B w_{1m} + \mu_2^B w_{2m} = 0, \\
   t_{21}^A \mu_1^A h_{1,{m+1}} + \mu_2^A h_{2,{m+1}} + t_{21}^B \mu_1^B w_{1,{m+1}} + \mu_2^B w_{2,{m+1}} = 0, \\
   \vdots \\
   t_{21}^A \mu_1^A h_{1n} + \mu_2^A h_{2n} + t_{21}^B \mu_1^B w_{1n} + \mu_2^B w_{2n} = 0.
\end{cases}
\end{align*}
$$

(16)

Consider the first equation of subsystem (16)

$$
t_{21}^A \mu_1^A h_{11} + \mu_2^A h_{21} + t_{21}^B \mu_1^B w_{11} + \mu_2^B w_{21} = \epsilon_{21}.
$$

(17)

Let us substitute the solution $h_{11}^0, w_{11}^0$ of the equation (15) from the subsystem (14) into the equation (17), we obtain the following equation:

$$
\mu_2^A h_{21} + \mu_2^B w_{21} = \epsilon_{21} - t_{21}^A \mu_1^A h_{11}^0 - t_{21}^B \mu_1^B w_{11}^0.
$$

Since $(\mu_2^A, \mu_2^B) = 1$, this equation is solvable and it has solution $h_{21}^1, w_{21}^1$, such that

$$
\mathcal{E} \left( h_{21}^0 \right) < \mathcal{E} \left( \mu_2^B \right).
$$

In equation $t_{21}^A \mu_1^A h_{12} + \mu_2^A h_{22} + t_{21}^B \mu_1^B w_{12} + \mu_2^B w_{22} = \epsilon_{22}$, substitute the solution $h_{12}^0 = 0, w_{12}^0 = 0$ from the subsystem (14), we will obtain $\mu_2^A h_{22} + \mu_2^B w_{22} = \epsilon_{22}$. This equation is solvable and there exists a solution $h_{22}^0, w_{22}^0$, such that

$$
\mathcal{E} \left( h_{22}^0 \right) < \mathcal{E} \left( \mu_2^B \right).
$$

Consider the following equation of a subsystem (16)

$$
t_{21}^A \mu_1^A h_{13} + \mu_2^A h_{23} + t_{21}^B \mu_1^B w_{13} + \mu_2^B w_{23} = 0.
$$

Since $h_{13}^0 = 0, w_{13}^0 = 0$, the solutions of this equation will be $h_{23}^0 = 0, w_{23}^0 = 0$.

Considering similarly, we establish that the system (13) has the solutions $h_{ij}^0, w_{ij}^0$, such that

$$
\mathcal{E} \left( h_{ij}^0 \right) < \mathcal{E} \left( \mu_i^B \right), \quad \text{if} \quad i = 1, \ldots, m, \quad j = 1, \ldots, i,
$$

and $h_{ij}^0, w_{ij}^0 = 0$ if $i = 1, \ldots, m, j = i + 1, i + 2, \ldots, n$. The theorem is proved. \(\square\)

**Theorem 2.** Let $K = \mathbb{Z} \left[ \sqrt{k} \right]$ be an imaginary Euclidean quadratic ring. Then the matrix equation (9) over a ring $K$ has a finite number solutions of the form (11) with conditions (12).

**Proof.** From solutions of system (13) we will get the solutions

$$
H = \| h_{ij} \|_{i,j=1}^n, \quad W = \| w_{ij} \|_{i,j=1}^n,
$$

such that elements $h_{ij}$, $i, j = 1, \ldots, n$, of a matrix $H$ have bounded Euclidean norms. It is known that there is a finite number of elements from the imaginary Euclidean quadratic ring $K$, which have the same Euclidean norm value. Therefore, there is a finite number of these solutions $H, W$ over the imaginary Euclidean quadratic ring. The proof is complete. \(\square\)
The Euclidean norm \( E(A) \) of the matrix \( A = \|a_{ij}\|_{i,j=1}^{m,n} \) is called the greatest Euclidean norm \( E(a_{pq}) \) of elements of the matrix \( A \).

The Euclidean norm \( E(H) \) of the matrix \( H \) from the solution (11) of the matrix equation (9) is less than the Euclidean norm \( E(\mu_B) \) of the last invariant multiplier \( \mu_n \) of the matrix \( H \) from the equation (5). The Euclidean norm \( E(D^B) \) of the canonical diagonal form \( D^B \) of the matrix \( B \) equals to the Euclidean norm \( E(\mu_n^B) \) of the invariant multiplier \( \mu_n^B \). Therefore we obtain the following result.

**Corollary 1.** Let the matrices \( A \) and \( B \) from the matrix equation (9) are such that \( (d_A^m, d_B^m) = 1 \). Then this equation has the solutions of \( H, W \), such that the Euclidean norm \( E(H) \) of the matrix \( H \) is less than the Euclidean norm \( E(D^B) \) of the canonical diagonal form \( D^B \) of matrix \( B \). If \( K \) is an imaginary Euclidean quadratic ring, then there exists a finite number of such solutions of the matrix equation (9).

Note that if for matrices \( A \) and \( B \) from the equation (9) \( (d_A^m, d_B^m) \neq 1 \), then the equation (9) may not have solutions \( H, W \) of the form (11) such that \( E(h_{ij}) < E(\mu_n^B) \), if \( h_{ij} \neq 0, i = l + 1, l + 2, \ldots, m, j = 1, \ldots, i \).

**REFERENCES**


Received 20.01.2020


Розроблено метод розв’язування матричних діофантових рівнянь над квадратичними кільцями. На основі раніше встановленої авторами стандартної форми матриці над квадратичними кільцями відносно \((z, k)\)-еквівалентності матричні діофантове рівняння зведено до еквівалентного такого ж типу матричного рівняння з трикутними коефіцієнтами. Розв’язування цього матричного рівняння зведено до розв’язування системи лінійних рівнянь, яка містить лінійні двочленні діофантові рівняння, методи розв’язування яких добре відомі. Досліджено також структуру розв’язків матричних рівнянь. Зокрема, встановлено розв’язки з обмеженими евклідовими нормами. Показано, що таких розв’язків матричних рівнянь над квадратичними евклідовими уявними кільцями є скінченна кількість. Запропоновано ефективний спосіб побудови таких розв’язків.

Ключові слова і фрази: квадратичне кільце, матриця, \((z,k)\)-еквівалентність матриць, матричне діофантове рівняння, розв’язок матричного рівняння.