Linear Algebra and its Applications 435 (2011) 1903–1919

Contents lists available at ScienceDirect

Linear Algebra and its Applications

journal homepage: www.elsevier.com/locate/laa

Reduction of matrices over orders of imaginary quadratic fields ☆

Miroslav Kureš *, Ladislav Skula

Institute of Mathematics, Brno University of Technology, Technická 2, 61669 Brno, Czech Republic

ARTICLE INFO

Article history:
Received 1 June 2010
Accepted 19 March 2011
Available online 27 April 2011

Submitted by H. Schneider

AMS classification:
13F07
15A33
11R11

Keywords:
Order of an imaginary quadratic field
Normed ring
Generalized Euclidean ring
Invertible matrix
Elementary matrix
(1,2)-Matrix

ABSTRACT

A special decomposition (called the near standard form) of (1,2)-matrices over a ring is introduced and a method for a reduction of such matrices is explained. This can be applied for a detection of elementary second order matrices among invertible second order matrices. The tool is used in detail over orders of imaginary quadratic fields, where an algorithm, a number of properties and examples are presented.

1. Introduction

We start with some motivation. Let R be a ring with the identity $1_R \neq 0_R$. All elementary matrices (which are defined as finite products of elementary transvections and elementary dilations, see e.g. [2]) of size $n \times n$ with entries in R form a subgroup $\mathrm{GE}_n(R)$ of the group $\mathrm{GL}_n(R)$ of all invertible matrices. If for any $n \in \mathbb{N}$ and a ring R, the equality $\mathrm{GL}_n(R) = \mathrm{GE}_n(R)$ is satisfied, we say R is a GE_n-*ring*. If R is a GE_n-ring for all $n \in \mathbb{N}$, then R is called a GE-*ring* or a *generalized Euclidean ring*.

For square matrices of size 2×2, Cohn has used the concept of a standard form which is a very important tool for the investigation of GE_2-rings. In this paper, we introduce the concept of a near

☆ Published results were acquired using the subsidization of the Ministry of Education, Youth and Sports of the Czech Republic, research plan MSM 0021630518 "Simulation modeling of mechatronic systems".
* Corresponding author.
E-mail addresses: kures@fme.vutbr.cz (M. Kureš), skula@fme.vutbr.cz (L. Skula).

0024-3795/$ - see front matter © 2011 Elsevier Inc. All rights reserved.
doi:10.1016/j.laa.2011.03.037

standard form close to that of a standard form. This is done by means of the reduction of matrices of size 1×2, since the investigated considerations for square matrices of order 2 depend only on the first row.

In particular, we apply results to rings of integers of imaginary quadratic fields $\mathbb{Q}[\sqrt{d}]$, where d is a negative square-free integer. For such a ring R, Cohn has proved in [3], Theorem 6.1, that R is GE_2-ring if and only if $d \in \{-1, -2, -3, -7, -11\}$. We remark that the fields $\mathbb{Q}[\sqrt{d}]$ with $d \in \{-1, -2, -3, -7, -11\}$ are nothing but just all Euclidean imaginary quadratic fields ([4], Corollary to Proposition 3.11). Nevertheless, we study not only rings of integers of imaginary quadratic fields but somewhat more general rings: orders of imaginary quadratic fields (including non-maximal, of course).

2. Notation and basic assertions

In this section, a ring R means a ring with the identity $1_R \neq 0_R$, not necessarily commutative. The group of all units of R is denoted by $\mathrm{U}(R)$ and $\mathrm{U}(R) \cup \{0_R\}$ is denoted shortly by $\mathrm{U}_0(R)$. Further, $M_{m\times n}(R)$ denotes the set of all $m \times n$ matrices with entries in R; we will also use special matrices from $M_{2\times 2}(R)$, namely

$$E(a) = \begin{bmatrix} a & 1_R \\ -1_R & 0_R \end{bmatrix} \quad \text{and} \quad [\alpha, \beta] = \begin{bmatrix} \alpha & 0_R \\ 0_R & \beta \end{bmatrix},$$

$a \in R, \alpha, \beta \in \mathrm{U}(R)$. In Theorem 2.2 of [3] it was shown that each matrix $A \in \mathrm{GE}_2(R)$ can be expressed in the *standard form* which is the following expression:

$$A = [\alpha, \beta]E(a_1) \cdots E(a_r),$$

where $\alpha, \beta \in \mathrm{U}(R)$, $r \in \mathbb{N} \cup \{0\}$, $a_i \notin \mathrm{U}_0(R)$ for $2 \leq i \leq r-1$ and in the case of $r = 2$ the pair $(a_1, a_2) \neq (0_R, 0_R)$; for $r = 0$ we put $A = [\alpha, \beta]$. In general, the standard form need not be determined uniquely.

For a more detailed investigation, notions of a norm and a discrete norm are needed. We recall these definitions.

Definition 1. A mapping $|\ |: R \to \mathbb{R}^+$ ($\mathbb{R}^+$ are non-negative real numbers) is called a *norm on the ring R* if

(N1) $|x| = 0$ if and only if $x = 0_R$;
(N2) $|x + y| \leq |x| + |y|$;
(N3) $|xy| = |x||y|$.

for all x, y is satisfied. A ring R with a fixed norm is called a *normed ring*.

Clearly, then R has no zero divisors, therefore normed rings are always integral domains (still not necessarily commutative).

Definition 2. Let R be a normed ring. If the conditions

(N4) $|x| \geq 1$ for all $0_R \neq x \in R$ and $|x| = 1$ if and only if $x \in \mathrm{U}(R)$;
(N5) there does not exist any $x \in R$ such that $1 < |x| < 2$.

are satisfied, then the norm is called a *discrete norm on the ring R* and R is called a *discretely normed ring*.

In [3], (5.5), one more condition is used for certain purposes:

(N0) if $|x| = 1$ and $|x + 1| = 2$, then $x = 1_R$.

Cohn's results contain the following proposition. (Here from we simply denote by $\left[\, {}^{a\ b} \,\right]$ a matrix of size 2×2 having a and b in the first row and any elements in the second row.)

Proposition 1. *Let R be a discretely normed ring fulfilling (N0), $r \geq 2$ an integer, $a_1, \ldots, a_r \in R$ and $a_i \notin \mathrm{U}_0(R)$ for every i, $2 \leq i \leq r$, and let*

$$A = E(a_1)\cdots E(a_r) = \left[\, {}^{a\ b} \,\right].$$

Then $|a| > |b|$ or $a_1 = \alpha \in \mathrm{U}(R)$ and

$$A = \begin{bmatrix} 1_R\ \alpha \\ \ \end{bmatrix} \text{ for } r \text{ even or } A = \begin{bmatrix} \alpha\ 1_R \\ \ \end{bmatrix} \text{ for } r \text{ odd.}$$

Proof. The assertion is nothing but slightly reformulated Lemma 5.1 in [3]. □

The following theorem is crucial for our theory.

Theorem 1. *Let R be a discretely normed ring fulfilling (N0), $A = \left[\, {}^{a\ b} \,\right] \in \mathrm{GE}_2(R)$ and $b \neq 0_R$. Then there exists $q \in R$ such that*

$$AE(q)^{-1} = \left[\, {}^{b\ c} \,\right] \quad \text{and} \quad |b| > |c|.$$

If $|b| \geq 2$, then $c \neq 0_R$, therefore $|c| \geq 1$. If $|b| = 1$, then $c = 0_R$.

Proof. Let $A = [\alpha, \beta]E(a_1)\cdots E(a_r)$ be a standard form of the matrix A, where r is a non-negative integer, $\alpha, \beta \in \mathrm{U}(R)$, $a_1, \ldots, a_r \in R$ with $a_i \notin \mathrm{U}_0(R)$ for $2 \leq i \leq r-1$. Since $b \neq 0_R$, $r \geq 1$. Now, we observe four situations.

(i) If $b \in \mathrm{U}(R)$, we set $q = b^{-1}a$. Then

$$AE(q)^{-1} = \begin{bmatrix} a\ b \\ \ \end{bmatrix}\begin{bmatrix} 0_R & -1_R \\ 1_R & b^{-1}a \end{bmatrix} = \begin{bmatrix} b\ 0_R \\ \ \end{bmatrix},$$

therefore $c = 0_R$ and we are done.

(ii) If $r = 1$, we have

$$A = \begin{bmatrix} \alpha & 0_R \\ 0_R & \beta \end{bmatrix}\begin{bmatrix} a_1 & 1_R \\ -1_R & 0_R \end{bmatrix} = \begin{bmatrix} \alpha a_1\ \alpha \\ \ \end{bmatrix},$$

hence $b = \alpha$ and the result follows from (i).

(iii) Let $r = 2$. Then

$$A = \begin{bmatrix} \alpha & 0_R \\ 0_R & \beta \end{bmatrix}\begin{bmatrix} a_1 & 1_R \\ -1_R & 0_R \end{bmatrix}\begin{bmatrix} a_2 & 1_R \\ -1_R & 0_R \end{bmatrix} = \begin{bmatrix} \alpha a_1\ \alpha \\ \ \end{bmatrix}\begin{bmatrix} a_2 & 1_R \\ -1_R & 0_R \end{bmatrix} = \begin{bmatrix} \alpha a_1 a_2 - \alpha\ \ \alpha a_1 \\ \ \end{bmatrix},$$

thus $b = \alpha a_1$. Since $b \neq 0_R$, we can suppose $|a_1| > 1$ as the case $b \in \mathrm{U}(R)$ is already done by (i). Set $q = a_2$. Since

$$AE(q)^{-1} = \begin{bmatrix} \alpha a_1\ \alpha \\ \ \end{bmatrix},$$

we obtain $|\alpha| = 1 < |\alpha a_1|$, which is the wanted result.

(iv) Let $r \geq 3$. Put $s = r - 1$ and $B = E(a_1)\cdots E(a_s)$. Since $s \geq 2$, we can use Proposition 1 for the matrix B. If $B = \begin{bmatrix} \gamma\ \delta \\ \ \end{bmatrix}$, where $\gamma, \delta \in \mathrm{U}(R)$, then $b = \alpha\gamma \in \mathrm{U}(R)$, since

$$A = \begin{bmatrix} \alpha & 0_R \\ 0_R & \beta \end{bmatrix} B \begin{bmatrix} a_r & 1_R \\ -1_R & 0_R \end{bmatrix} = \begin{bmatrix} \alpha\gamma\ \alpha\delta \\ \ \end{bmatrix}\begin{bmatrix} a_r & 1_R \\ -1_R & 0_R \end{bmatrix} = \begin{bmatrix} \alpha\gamma a_r - \alpha\delta\ \ \alpha\gamma \\ \ \end{bmatrix}.$$

According to (i) we are done. If B has another form, say $B = \left[\, {}^{x\ y} \,\right]$, then $|x| > |y|$ holds. It follows

$$A = \begin{bmatrix} \alpha & 0_R \\ 0_R & \beta \end{bmatrix} BE(a_r) = \left[\, {}^{\alpha x\ \alpha y} \,\right]\begin{bmatrix} a_r & 1_R \\ -1_R & 0_R \end{bmatrix} = \left[\, {}^{\alpha x a_r - \alpha y\ \ \alpha x} \,\right],$$

thus $b = \alpha x$. If we set $q = a_r$, we get

$$AE(q)^{-1} = \begin{bmatrix} \alpha & 0_R \end{bmatrix} B = \begin{bmatrix} \alpha x & \alpha y \end{bmatrix}$$

and $|b| = |x| > |y| = |c|$. This completes the proof of the main part.

Suppose that $q \in R$, $AE(q)^{-1} = \begin{bmatrix} b & c \end{bmatrix}$, $|b| \geq 2$ and $|b| > |c|$. Since $c = -a + bq$, then for $c = 0_R$ we have $a = bq$ and $A = \begin{bmatrix} bq & b \end{bmatrix}$, which is in contradiction to the invertibility of A. Finally, the case $|b| = 1$ is evident. □

This theorem motivates the following definition.

Definition 3. Let R be a normed ring and $A = [\, a\ b \,] \in M_{1\times 2}(R)$. The matrix A is said to be *reducible* if there exists an element $q \in R$ such that

$$AE(q)^{-1} = [\, b\ c \,]$$

and $|b| > |c|$. The element q will be called a *reduction element of the matrix A*. Note that $E(q)^{-1} = \begin{bmatrix} 0_R & -1_R \\ 1_R & q \end{bmatrix}$ and $c = -a + bq$.

In the opposite case we call the matrix A *non-reducible*.

Proposition 2. *Let R be a normed ring. Then each matrix $A = [\, r\ 0 \,] \in M_{1\times 2}(R)$ is non-reducible. If $B = [\, a\ b \,] \in M_{1\times 2}(R)$ is non-reducible, then $|a| \geq |b|$.*

Proof. The first statement is easy. Assume that $B = [\, a\ b \,]$ is non-reducible. If $|a| < |b|$, set $q = 0$. Then

$$BE(q)^{-1} = [\, a\ b \,] \begin{bmatrix} 0_R & -1_R \\ 1_R & 0_R \end{bmatrix} = [\, b\ -a \,].$$

This is a contradiction because we have found a reduction. □

The opposite direction to the first statement of Proposition 2 holds for discretely normed rings with (N0) in the following sense.

Proposition 3. *Let R be a discretely normed ring fulfilling (N0) and $A = \begin{bmatrix} a & b \end{bmatrix} \in \mathrm{GE}_2(R)$. Then the matrix $[\, a\ b \,]$ is non-reducible if and only if $b = 0_R$. In this case $A = \begin{bmatrix} \alpha & 0_R \\ r & \beta \end{bmatrix}$, where $\alpha, \beta \in \mathrm{U}(R)$ and $r \in R$.*

Proof. If $b = 0_R$, according to Proposition 2 the matrix $[\, a\ b \,] = [\, a\ 0_R \,]$ is non-reducible. Let us suppose that the matrix $[\, a\ b \,]$ is non-reducible. By Theorem 1, only $b = 0_R$ is possible. The expression $A = \begin{bmatrix} \alpha & 0_R \\ r & \beta \end{bmatrix}$ follows from the fact that A is invertible. □

Of course, Proposition 3 is still valid for non-commutative rings, too.

Definition 4. Let R be a normed ring and $A = [\, a\ b \,] \in M_{1\times 2}(R)$, s be a positive integer, $q_1, \ldots, q_s \in R$ and $B \in M_{1\times 2}(R)$ a non-reducible matrix. Let $b_0, b_1, \ldots, b_{s+1} \in R$ be defined by $[\, b_{i-1}\ b_i \,] = BE(q_s) \cdots E(q_i)$ for $1 \leq i \leq s$ and by $[\, b_s\ b_{s+1} \,] = B$. If A is expressed as

$$A = BE(q_s) \cdots E(q_1) \qquad (*)$$

and

$$|b_i| > |b_{i+1}|$$

is satisfied for every i, $1 \leq i \leq s$, then the expression $(*)$ is called a *nearly standard form for the matrix A*.

If A is non-reducible, then the expression $A = B$ is considered to be a nearly standard form for the matrix A (so $s = 0$).

Remark 1. The elements b_i ($0 \le i \le s+1$) can be defined recursively as follows:

$$b_0 := a,\, b_1 := b,\, \dots,\, b_{i+1} := b_i q_i - b_{i-1} \quad \text{for } 1 \le i \le s.$$

Further we will use the “descending chain condition” for norms in the following form.

Definition 5. Let R be a normed ring. We say that its *norm* $|\ |$ *satisfies the descending chain condition* if it shares the following property:

(N_∞) for $r_1, r_2, \dots \in R$ with $|r_1| \ge |r_2| \ge \cdots$ there exists a positive integer N such that for every integer $j \ge N$ the equality $|b_N| = |b_j|$ holds.

Now we are able to state the theorem.

Theorem 2. *Let R be a normed ring fulfilling (N_∞). Then each matrix $A \in M_{1\times 2}(R)$ has a nearly standard form.*

Proof. Let $A = [\, a\ b\,] \in M_{1\times 2}(R)$. If A is non-reducible, then $A = B$ is the nearly standard form. Assume that A is reducible. Then there exists $q_1 \in R$ with $AE(q_1)^{-1} = [\, b_1\ b_2\,]$ and $|b_1| > |b_2|$ (where $b_1 = b$). Set $A_0 = A$ and $A_1 = AE(q_1)^{-1}$ and assume that s is a positive integer, $q_1, \dots, q_s, b_1, \dots, b_{s+1} \in R$ and $A_i = [\, b_i\ b_{i+1}\,]$ satisfies $A_i = A_{i-1}E(q_i)^{-1}$ and $|b_i| > |b_{i+1}|$ for every i, $1 \le i \le s$. If A_s is reducible then there exists $q_{s+1} \in R$ with the property $A_sE(q_{s+1})^{-1} = [\, b_{s+1}\ b_{s+2}\,]$, $|b_{s+1}| > |b_{s+2}|$. According to the condition (N_∞) this process cannot be arbitrarily lengthened, therefore we can assume that $A_s = B$ is a non-reducible matrix. Then we get

$$A = A_1E(q_1) = A_2E(q_2)E(q_1) = \cdots = BE(q_s)\cdots E(q_1)$$

which is a nearly standard form for the matrix A. $\square$

Remark 2. Theorem 2 can be used for a determining if a matrix $M \in \mathrm{GL}_2(R)$ with entries in a discretely normed ring R fulfilling (N0) and (N_∞) belongs to $\mathrm{GE}_2(R)$. Indeed, the first row of M is a (1,2)-matrix A and if A is non-reducible, then it has a nearly standard form given by Definition 4 with a non-reducible B. If $M \in \mathrm{GE}_2(R)$, then $\begin{bmatrix} B \\ \end{bmatrix} \in \mathrm{GE}_2(R)$. For $B = [\, a\ b\,]$, it follows from Proposition 3 that $M \in \mathrm{GE}_2(R)$ if and only if $b = 0_R$. (We will demonstrate this method in Section 6.)

We remark that Cohn’s and Tuler’s well-known examples of non-elementary invertible matrices (see Section 7) easily can be checked by our method; let us notice that the special nearly standard form $A = B$ occurs in either case.

The following proposition demonstrates the relationship between the notions of the nearly standard form and the standard form.

Proposition 4. *Let R be a discretely normed ring fulfilling (N0). Let s be a positive integer, $a_1, \dots, a_s \in R - \mathrm{U}_0(R)$ and let*

$$\begin{bmatrix} a & b \\ & \end{bmatrix} = A = E(a_1)\cdots E(a_s) \in M_{2\times 2}(R)$$

be a standard form for the matrix A. Set $B = [\, 1_R\ 0_R\,] \in M_{1\times 2}(R)$. Then

$$[\, a\ b\,] = BE(a_1)\cdots E(a_s)$$

is a nearly standard form for the matrix $[\, a\ b\,]$.

Proof. Since for each $q \in R$ the expression $[\, q\ 1\,] = BE(q)$ is a nearly standard form for the matrix $[\, a\ b\,]$, we can assume $s \ge 2$. Put for every i, $1 \le i \le s$, $q_i = a_{s-i+1}$ and $[\, b_{i-1}\ c_i\,] = B_i = BE(q_s)\cdots E(q_i)$ and $b_s = 1_R$. Since for every i, $1 \le i \le s-1$, $[\, b_i\ c_{i+1}\,] = B_{i+1} = B_iE(q_i)^{-1} = [\, c_i\ -b_{i-1}+c_iq_i\,]$, we have $c_i = b_i$. Let $1 \le i \le s-1$. Put $r = s-i+1$. Then $2 \le r \le s$ and

$$E(a_1)\cdots E(a_r) = E(q_s)\cdots E(q_i) = \left[\, b_{i-1}\ b_i \,\right].$$

Using Proposition 1, we get $|b_{i-1}| > |b_i|$, hence $|b_j| > |b_{j+1}|$ for every $0 \le j \le s-2$. Since $[\, b_{s-1}\ b_s \,] = [\, q_s\ 1_R \,] = [\, a_1\ 1_R \,]$, we have $|b_{s-1}| > |b_s|$, which completes the proof. □

3. Matrix reduction in orders of imaginary quadratic fields

From here throughout this paper we will assume that d is a negative square-free integer and C a positive integer. We will distinguish two cases:

(I) $d \equiv 1 \pmod 4$,
(II) $d \equiv 2$ or $d \equiv 3 \pmod 4$.

Further, we set

$$\varepsilon = \begin{cases} 1 & \text{for the case (I)} \\ 0 & \text{for the case (II);} \end{cases}$$

we will use this ε for a formal integration of the two cases described above to a single one in a number of formulas below. Let

$$\theta = \sqrt{d} + \frac{\varepsilon}{2}(1 - \sqrt{d})$$

and

$$D = -d + \frac{\varepsilon}{4}(1 + 3d).$$

Further, we denote by $\mathbb{Z}[C\theta]$ an order of the imaginary quadratic field $\mathbb{Q}[\sqrt{d}]$ (cf. e.g. [1], Chapter 2, 2.2), so

$$\mathbb{Z}[C\theta] = \{x + yC\theta;\, x, y \in \mathbb{Z}\}.$$

The order $\mathbb{Z}[C\theta]$ is a normed ring with the norm $|\ |: \mathbb{Z}[C\theta] \to \mathbb{R}^+$ equal to the complex numbers absolute value. Then for $z = x + yC\theta \in \mathbb{Z}[C\theta]$ we have

$$|z|^2 = x^2 + \varepsilon xyC + y^2C^2D.$$

It is easy to see that this norm satisfies (N4) and (N0). The condition (N5) is also satisfied with the exception for $d = -1, -2, -3, -7, -11$ and $C = 1$ (see [3], Section 6). Clearly, the condition (N_∞) is satisfied as well.

Further, we will suppose

$$A = [\, a\ b \,] \in M_{1\times 2}(\mathbb{Z}[C\theta]), \quad a, b \in \mathbb{Z}[C\theta], \quad b \neq 0,$$
$$a = u + vC\theta, \quad b = r + sC\theta, \quad u, v, r, s \in \mathbb{Z}.$$

The aim of this section is a search of reduction elements of the matrix A and to give a result about an upper bound for the number of such elements.

According to the definition of the reduction element of a matrix we have the following assertion.

Proposition 5. *An element $q \in \mathbb{Z}[C\theta]$ is a reduction element of the matrix A if and only if*

$$|-a + bq|^2 < |b|^2.$$

Proof. See Definition 3. □

To specify a reduction element q of A we define

$$\begin{aligned}
R &:= |b|^2 = r^2 + \varepsilon rsC + s^2C^2D,\\
S &:= |a|^2 = u^2 + \varepsilon uvC + v^2C^2D,\\
\alpha &:= -(ur + vsC^2D) - \frac{\varepsilon C}{2}(vr + us),\\
\beta &:= (us - vr)C^2D - \frac{\varepsilon C}{2}(ur + usC + vsC^2D),\\
\gamma &:= S - R.
\end{aligned}$$

Now, we set for $x, y \in \mathbb{R}$

$$K(x, y) := x^2 + \varepsilon xyC + y^2C^2D + \frac{2\alpha}{R}x + \frac{2\beta}{R}y + \frac{\gamma}{R}.$$

The equation $K(x, y) = 0$ represents an equation of a quadratic curve in the real plane. Its invariants are

$$I_1 = 1 + C^2D > 0, \quad I_2 = \frac{C^2}{4}(4D - \epsilon) > 0, \quad I_3 = -\frac{C^2}{4}(4D - \varepsilon) < 0,$$

hence $K(x, y) = 0$ is a real ellipse; we call it a *reduction ellipse of the matrix A* and denote it by $\mathcal{E}_{\text{red}}$. Points $[x, y]$ of the plane satisfying $K(x, y) < 0$ will be called *interior points* of the reduction ellipse. (This notion we use also for other ellipses below.) The center of $\mathcal{E}_{\text{red}}$ will be denoted by $S_{\text{red}} = [s_1, s_2]$. For s_1, s_2

$$s_1 = \frac{1}{R}\left(\frac{\varepsilon(2\beta - \alpha C)}{C(4D - 1)} - \alpha\right), \quad s_2 = \frac{1}{C^2DR}\left(\frac{\varepsilon(2\alpha CD - \beta)}{4D - 1} - \beta\right)$$

holds.

The following theorem specifies a relation between a reduction ellipse and a reduction element.

Theorem 3. *An element $q = x + yC\theta \in \mathbb{Z}[C\theta]$ is a reduction element of the matrix A if and only if $K(x, y) < 0$, i.e. $[x, y]$ is an interior point of the reduction ellipse $\mathcal{E}_{\text{red}}$.*

Proof. By Proposition 5, an element $q \in \mathbb{Z}[C\theta]$ is a reduction element of the matrix A if and only if $|-a + bq|^2 < |b|^2$; a direct calculation gives this inequality in the equivalent form $K(x, y) < 0$. □

So, the reduction elements of A correspond one-to-one to the interior points of the reduction ellipse having integer coordinates (such points will be called *interior lattice points*) by $q = x + yC\theta \mapsto [x, y]$. Now, we will find an upper bound of the number of these lattice points: to that end we use the translation of the reduction ellipse $\mathcal{E}_{\text{red}}$ to the ellipse $\mathcal{E}_1$. This translation is determined by the translation of the center S_{red} into $P = [0, 0]$.

Proposition 6. *The ellipse $\mathcal{E}_1$ has the equation*

$$x^2 + \varepsilon xyC + y^2C^2D = 1.$$

Proof. Since $P = [0, 0]$ is the center of the ellipse $\mathcal{E}_1$, the ellipse $\mathcal{E}_1$ has the equation

$$x^2 + \varepsilon xyC + y^2C^2D + \Gamma = 0,$$

where $\Gamma \in \mathbb{R}$. We compute Γ by means of the invariant I_3:

$$-\frac{C^2}{4}(4D - \varepsilon) = I_3 = \begin{vmatrix} 1 & \frac{\varepsilon C}{2} & 0 \\ \frac{\varepsilon C}{2} & C^2D & 0 \\ 0 & 0 & \Gamma \end{vmatrix} = \Gamma\left(C^2D - \frac{\varepsilon C^2}{4}\right).$$

This proves $\Gamma = -1$. □

Coordinates $[s_1, s_2]$ of the center of $\mathcal{E}_{red}$ have integer parts $k := [s_1]$, $l := [s_2]$ and fractional parts $\xi := \{s_1\} = s_1 - k$, $\eta := \{s_2\} = s_2 - l$, i.e. $s_1 = k + \xi$, $s_2 = l + \eta$, $k, l \in \mathbb{Z}$, $\xi, \eta \in \mathbb{Q}$, $0 \leq \xi, \eta < 1$. We put $\Sigma := [\xi, \eta] \in \mathbb{R}^2$ and denote the translation $[k, l] \mapsto [0, 0] = P$ by $\mathcal{T}$. Then $\mathcal{T}$ transfers the square $\{[x, y] \in \mathbb{R}^2; k \leq x < k + 1; l \leq y < l + 1\}$ into the square $\{[x, y] \in \mathbb{R}^2; 0 \leq x < 1; 0 \leq y < 1\}$ and the reduction ellipse $\mathcal{E}_{red}$ with the center S_{red} into the ellipse denoted by $\mathcal{E}$ with the center Σ.

Let us notice that the translation $\mathcal{T}$ can be composed from translations $S_{red} \mapsto P$ and $P \mapsto \Sigma$. Thus, the ellipse $\mathcal{E}$ can be viewed as the transferred ellipse $\mathcal{E}_1$. We obtain easily:

Proposition 7. *The ellipse $\mathcal{E}$ has the equation*

$$(x - \xi)^2 + \varepsilon(x - \xi)(y - \eta)C + (y - \eta)^2 C^2 D = 1.$$

Proof. This follows immediately from the Proposition 6. □

Obviously, interior lattice points of $\mathcal{E}_{red}$ transfer into interior lattice points of $\mathcal{E}$ by the translation $\mathcal{T}$. Reciprocally, interior lattice points of $\mathcal{E}$ transfer into interior lattice points of $\mathcal{E}_{red}$ by the inverse translation $\mathcal{T}^{-1}$. Proposition 5 gives a way to derive reduction elements of the matrix A. It follows that a detection of interior lattice points of $\mathcal{E}$ is needful. First, we deduce the assertion.

Proposition 8. *The interior points of the ellipse $\mathcal{E}$ lie in the rectangle $\mathcal{O}$ defined by its vertices by the following way:*

(a) vertices of $\mathcal{O}$ are $[-2, -2]$, $[3, -2]$, $[3, 3]$, $[-2, 3]$ for the case $C = 1$, $d = -3$;
(b) vertices of $\mathcal{O}$ are $[-2, -1]$, $[3, -1]$, $[3, 2]$, $[-2, 2]$ for the case (I), $(C, d) \neq (1, -3)$;
(c) vertices of $\mathcal{O}$ are $[-1, -1]$, $[2, -1]$, $[2, 2]$, $[-1, 2]$ for the case (II).

Proof. The bounds are derived by a direct calculation. □

For further investigation, we introduce the following notation of points in real plane:

$$P_1 := P = [0, 0], \quad P_2 := [1, 0], \quad P_3 := [2, 0], \quad P_4 := [-1, 1], \quad P_5 := [0, 1],$$
$$P_6 := [1, 1], \quad P_7 := [1, -1], \quad P_8 := [0, 2].$$

Now, we find out the following fact (cases denoted as in Proposition 8).

Theorem 4. *(The 1st claim about an upper bound of number of reduction elements.) Only*

(a) $P_1, P_2, P_3, P_4, P_5, P_6, P_7, P_8$,
(b) $P_1, P_2, P_3, P_4, P_5, P_6$,
(c) P_1, P_2, P_5, P_6

can be possible interior lattice points of the ellipse $\mathcal{E}$.

Proof

(a) The rectangle $\mathcal{O}$ contains all points $P_1, P_2, P_3, P_4, P_5, P_6, P_7, P_8$ and, moreover, points $[-1, 2]$, $[1, 2]$, $[2, 2]$, $[2, 1]$, $[-1, 0]$, $[-1, -1]$, $[0, -1]$, $[2, -1]$. We verify by a direct calculation that these eight additional points cannot be interior points of $\mathcal{E}$.
(b) Now, the rectangle $\mathcal{O}$ contains all points $P_1, P_2, P_3, P_4, P_5, P_6$ and, moreover, points $[2, 1]$ and $[0, -1]$. These two points cannot be interior points of $\mathcal{E}$.
(c) Easily, the rectangle $\mathcal{O}$ contains only points P_1, P_2, P_5, P_6. □

4. The 2nd and the 3rd claims about an upper bound of number of reduction elements of the matrix *A*

For an improvement of estimations of number of interior lattice points we use the following theorem.

Theorem 5 (Reciprocity theorem). *Let $\mathcal{F}$, $\mathcal{G}$ are two real ellipses in $\mathbb{R}^2$ with centers C_1, C_2, respectively, such that the ellipse $\mathcal{G}$ is a transferred ellipse $\mathcal{F}$ with respect to the translation $C_1 \mapsto C_2$. Then C_1 is an interior point of $\mathcal{G}$ if and only if C_2 is an interior point of $\mathcal{F}$.*

Proof. The theorem is familiar. □

For $1 \leq i \leq 8$, let $\mathcal{E}_i$ denote the transferred ellipse $\mathcal{E}$ by the translation $\Sigma \mapsto P_i$. (Or, the transferred ellipse $\mathcal{E}_1$ by the translation $P = P_1 \mapsto P_i$.) The equation of the ellipse $\mathcal{E}_i$ is

$$(x - x_i)^2 + \varepsilon(x - x_i)(y - y_i)C + (y - y_i)^2C^2D = 1,$$

where $P_i = [x_i, y_i]$. We observe:

Corollary 1. *For $1 \leq i \leq 8$, P_i is an interior point of $\mathcal{E}$ if and only if Σ is an interior point of $\mathcal{E}_i$.*

Proof. The corollary is an immediate consequence of Theorem 5. □

Therefore we investigate for which of the ellipses $\mathcal{E}_i$ is the point Σ an interior point of $\mathcal{E}_i$; then we use the reciprocity theorem. For calculation below, we use the orthogonal transformation $\mathrm{T}\colon \mathbb{R}^2 \to \mathbb{R}^2$, $\mathrm{T}\colon X = [x, y] \mapsto X' = [x', y']$ defined by

$$x' = -x + 1,$$
$$y' = -y + 1.$$

Proposition 9. $\mathrm{T}(P_1) = P_6, \mathrm{T}(P_2) = P_5, \mathrm{T}(P_3) = P_4, \mathrm{T}(P_7) = P_8; \mathrm{T}(\mathcal{E}_1) = \mathcal{E}_6, \mathrm{T}(\mathcal{E}_2) = \mathcal{E}_5, \mathrm{T}(\mathcal{E}_3) = \mathcal{E}_4$, $\mathrm{T}(\mathcal{E}_7) = \mathcal{E}_8$.

Proof. One can verify this proposition by a direct calculation. □

Proposition 10. *Let us consider the case (I), $C^2D \geq 5$ and let us take two straight lines p, q in $\mathbb{R}^2$ with equations $p\colon y = \frac{1}{2}$, $q\colon y = -\frac{1}{2}$. Then neither p nor q has a common point with an ellipse $\mathcal{E}_i$, $1 \leq i \leq 6$.*

Proof. A direct calculation gives this assertion for the ellipse $\mathcal{E}_1$. As every ellipse $\mathcal{E}_i$, $1 \leq i \leq 6$ is nothing but a transferred ellipse $\mathcal{E}_1$ and the center P_i has integer coordinates, we have finished the proof. □

This enables to formulate the theorem.

Theorem 6. *(The 2nd claim about an upper bound of number of reduction elements for the case (I).) For the case (I) and $C^2D \geq 5$ we have:*

(i) if $\eta \leq \frac{1}{2}$, then no point of P_4, P_5, P_6 is an interior point of $\mathcal{E}$;
(ii) if $\eta \geq \frac{1}{2}$, then no point of P_1, P_2, P_3 is an interior point of $\mathcal{E}$.

Proof. The result follows directly from Proposition 10 and Theorem 5. □

For the case (II), we have:

Proposition 11. *Let us consider the case (II) and let us take the straight line p with the equation $p\colon y = \frac{1}{2}$. Then*

(i) if $C^2D > 4$, then p has not any common point with an ellipse $\mathcal{E}_i$, $i \in \{1, 2, 5, 6\}$;
(ii) if $C^2D = 4$ (i.e. $C = 2$, $D = 1$), then p is a tangent to every ellipse $\mathcal{E}_i$, $i \in \{1, 2, 5, 6\}$, namely with $\left[0, \frac{1}{2}\right]$ as the common point of contact for $i \in \{1, 5\}$ and with $\left[1, \frac{1}{2}\right]$ as the common point of contact for $i \in \{2, 6\}$.

Proof. One can verify this proposition by a direct calculation. □

We can formulate the following theorem.

Theorem 7. *(The 2nd claim about an upper bound of number of reduction elements for the case (II).) For the case (II) and $C^2D \geq 4$ we have:*

(i) if $\eta \leq \frac{1}{2}$, then no point of P_5, P_6 is an interior point of $\mathcal{E}$;
(ii) if $\eta \geq \frac{1}{2}$, then no point of P_1, P_2 is an interior point of $\mathcal{E}$.

Proof. The result follows directly from Proposition 11 and Theorem 5. □

Now, we determine a number of reduction elements of the matrix A for the case, when the center Σ of the ellipse $\mathcal{E}$ equals $P = P_1$.

Proposition 12. *For $1 \leq i \leq 8$, P is an interior point of $\mathcal{E}_i$ if and only if $i = 1$.*

Proof. The equation of the ellipse $\mathcal{E}_i$ is

$$(x - x_i)^2 + \varepsilon(x - x_i)(y - y_i)C + (y - y_i)^2C^2D = 1,$$

where $P_i = [x_i, y_i]$. For $1 \leq i \leq 8$, let us put

$$V(i) = x_i^2 + \varepsilon x_i y_i C + y_i^2 C^2 D - 1.$$

The values $V(i)$ are the following:

i	1	2	3	4	5	6	7	8
$V(i)$	-1	0	3	$C(CD - \varepsilon)$	$C^2D - 1$	$C(CD + \varepsilon)$	$C(CD - \varepsilon)$	$4C^2D - 1$

Since P is an interior point of $\mathcal{E}_i$ if and only if P_i is an interior point of $\mathcal{E}_1$, we have the result. □

Corollary 2. *If $\Sigma = P$, then the matrix A has only one reduction element, namely $s_1 + s_2C\theta$, where $S_{\text{red}} = [s_1, s_2]$ is the center of the reduction ellipse $\mathcal{E}_{\text{red}}$.*

Proof. See Theorem 3. □

Let us consider the case (I).

Proposition 13. *For the case (I)*

$$\mathcal{E}_1 \cap \mathcal{E}_3 = \{[1, 0]\} \quad \text{and} \quad \mathcal{E}_4 \cap \mathcal{E}_6 = \{[0, 1]\}$$

hold, it follows there are no common interior points of $\mathcal{E}_1$ and $\mathcal{E}_3$ and no common interior points of $\mathcal{E}_4$ and $\mathcal{E}_6$.

Proof. One can verify this proposition by a direct calculation. □

Now, we can formulate the following theorem.

Theorem 8. *(The 3rd claim about an upper bound of number of reduction elements.) For the case (I) and $C^2D \geq 5$ and for the case (II) and $C^2D \geq 4$ the number of reduction elements of the matrix A is less or equal 2.*

Proof. The result follows directly from Proposition 13, Theorem 5, Theorem 6 and Theorem 7. □

We put

$$\mathcal{Q} = \{[x, y] \in \mathbb{R}^2; 0 \leq x, y < 1\} - \{[0, 0]\}$$

and we denote by $\hat{\mathcal{E}}_i$ interior points of $\mathcal{E}_i$ belonging to $\mathcal{Q}$, $1 \leq i \leq 8$. We have:

Proposition 14. *For the case (I)*

$$\hat{\mathcal{E}}_3 \subseteq \hat{\mathcal{E}}_2 \quad \textit{and} \quad \hat{\mathcal{E}}_4 \subseteq \hat{\mathcal{E}}_5$$

hold.

Proof. One can verify this proposition by a direct calculation. □

Further, we denote

$$\mathcal{Z}_{\text{nonred}} = \begin{cases} \mathcal{Q} - \{\hat{\mathcal{E}}_1 \cup \hat{\mathcal{E}}_2 \cup \hat{\mathcal{E}}_3 \cup \hat{\mathcal{E}}_4 \cup \hat{\mathcal{E}}_5 \cup \hat{\mathcal{E}}_6\} & \text{for the case (I)}, \\ \mathcal{Q} - \{\hat{\mathcal{E}}_1 \cup \hat{\mathcal{E}}_2 \cup \hat{\mathcal{E}}_5 \cup \hat{\mathcal{E}}_6\} & \text{for the case (II)}. \end{cases}$$

If $\Sigma \in \mathcal{Z}_{\text{nonred}}$, then the matrix A has no reduction element. That is why we call the set $\mathcal{Z}_{\text{nonred}}$ the *zone of non-reductionability*. Then the matrix A is non-reducible.

Proposition 15. *If A represents the first row of a square matrix $H \in M_{2\times 2}(\mathbb{Z}[C\theta])$ and $\Sigma \in \mathcal{Z}_{\text{nonred}}$, then H is not elementary.*

Proof. The complex numbers absolute value is a norm $|\ |\colon \mathbb{Z}[C\theta] \to \mathbb{R}^+$ fulfilling (N4) and (N0). (This norm also fulfills (N5) with the exception for $d = -1, -2, -3, -7, -11$ and $C = 1$; these cases will be discussed in the next section.) Then the assertion follows from Proposition 3. □

5. Special cases

In this section, we describe situations which are not covered by Theorem 8, i.e. in the

case (I) it is $C^2D \leq 4$, so	$C = 1, D = 1, d = -3$
	$C = 2, D = 1, d = -3$
	$C = 1, D = 2, d = -7$
	$C = 1, D = 3, d = -11$
	$C = 1, D = 4, d = -15$
case (II) it is $C^2D \leq 3$, so	$C = 1, D = 1, d = -1$
	$C = 1, D = 2, d = -2.$

Remark 3. Notice that for the case (II) and $C = 1, D = 1, d = -1$ the ring $\mathbb{Z}[C\theta]$ is the ring of Gaussian integers and for the case (I) and $C = 1, D = 1, d = -3$ the ring $\mathbb{Z}[C\theta]$ is the ring of Eisenstein integers.

Proposition 16. *For the case (I) and $C = D = 1$ all points of $\mathcal{Q}$ are interior points of $\mathcal{E}_2$ and simultaneously interior points of $\mathcal{E}_5$. Further, $\mathcal{E}_7 \cap \mathcal{E}_8 = \emptyset$, $\mathcal{E}_7 \cap \mathcal{E}_6 = \{[1, 0]\}$, $\mathcal{E}_7 \cap \mathcal{E}_4 = \{[0, 0]\}$, $\mathcal{E}_7 \cap \mathcal{E}_3 = \{[1, 0], [2, -1]\}$, $\mathcal{E}_8 \cap \mathcal{E}_6 = \{[0, 1]\}$, $\mathcal{E}_8 \cap \mathcal{E}_4 = \{[0, 1], [-1, 2]\}$, $\mathcal{E}_8 \cap \mathcal{E}_3 = \{[1, 1]\}$.*

Proof. One can verify this proposition by a direct calculation. □

Hence we obtain:

Theorem 9. *For the case (I) and $C = D = 1$, the matrix A has only one reduction element if and only if $\Sigma = P = [0, 0]$. In other cases, A has at least 2 reduction elements and at most 4 reduction elements.*

Proof. The result follows directly from Proposition 16 and Proposition 13. □

For further investigation we recall that Theorem 4 asserts that P_7 and P_8 cannot be interior points of $\mathcal{E}$ (excluding the case (I) and $(C, D) = (1, 1)$).

Proposition 17. *For the case (I) and $(C, D) \neq (1, 1)$, we have:*

$$\mathcal{E}_2 \cap \mathcal{E}_4 = \left\{\left[0, \frac{1}{2}\right]\right\}, \quad \mathcal{E}_3 \cap \mathcal{E}_5 = \left\{\left[1, \frac{1}{2}\right]\right\} \quad \textit{for } CD = 2,$$
$$\mathcal{E}_1 \cap \mathcal{E}_6 = \left\{\left[\frac{1}{2}, \frac{1}{2}\right]\right\} \quad \textit{for } C = 1, D = 2,$$
$$\mathcal{E}_1 \cap \mathcal{E}_6 = \mathcal{E}_2 \cap \mathcal{E}_4 = \mathcal{E}_3 \cap \mathcal{E}_5 = \emptyset \quad \textit{in other cases.}$$

Proof. One can verify this proposition by a direct calculation. □

Now we are able to state the theorem.

Theorem 10. *For the case (I) and $(C, D) \neq (1, 1)$, the matrix A has at most three reduction elements. Namely, A has three reduction elements if and only if Σ lies in one of the following sets: $\hat{\mathcal{E}}_3 \cap \hat{\mathcal{E}}_2 \cap \hat{\mathcal{E}}_6$, $\hat{\mathcal{E}}_4 \cap \hat{\mathcal{E}}_1 \cap \hat{\mathcal{E}}_5$, $\hat{\mathcal{E}}_1 \cap \hat{\mathcal{E}}_2 \cap \hat{\mathcal{E}}_5$, $\hat{\mathcal{E}}_2 \cap \hat{\mathcal{E}}_5 \cap \hat{\mathcal{E}}_6$.*

Proof. We have $\hat{\mathcal{E}}_2 \cap \hat{\mathcal{E}}_4 = \hat{\mathcal{E}}_3 \cap \hat{\mathcal{E}}_5 = \hat{\mathcal{E}}_1 \cap \hat{\mathcal{E}}_6 = \emptyset$ from Proposition 17, $\hat{\mathcal{E}}_1 \cap \hat{\mathcal{E}}_3 = \hat{\mathcal{E}}_4 \cap \hat{\mathcal{E}}_6 = \emptyset$ from Proposition 13 and $\hat{\mathcal{E}}_3 \cap \hat{\mathcal{E}}_4 = \emptyset$ from Proposition 14.

Let Σ lies in an intersection of at least 4 sets $\hat{\mathcal{E}}_j$, $1 \leq j \leq 6$. As $\hat{\mathcal{E}}_3 \cap \hat{\mathcal{E}}_i = \emptyset$ for $i = 1, 4, 5$, we have $j \neq 3$. Analogously, we can show that $j \neq 4$. Hence $\Sigma \in \hat{\mathcal{E}}_1 \cap \hat{\mathcal{E}}_2 \cap \hat{\mathcal{E}}_5 \cap \hat{\mathcal{E}}_6$, but this is impossible because $\hat{\mathcal{E}}_1 \cap \hat{\mathcal{E}}_6 = \emptyset$. □

For the case (I) and $C^2D = 4$ (i.e. $C = 2, D = 1$ or $C = 1, D = 4$), the following proposition holds:

Proposition 18. *For the case (I) and $C^2D = 4$, we have:*

$$\mathcal{E}_1 \cap \mathcal{E}_5 = \left\{\left[0, \frac{1}{2}\right]\right\}, \quad \mathcal{E}_2 \cap \mathcal{E}_6 = \left\{\left[1, \frac{1}{2}\right]\right\}, \quad \mathcal{E}_3 \cap \mathcal{E}_6 = \left\{\left[1, \frac{1}{2}\right], \left[2, \frac{1}{2}\right]\right\},$$
$$\mathcal{E}_4 \cap \mathcal{E}_1 = \left\{\left[0, \frac{1}{2}\right], \left[-1, \frac{1}{2}\right]\right\} \quad \textit{for } C = 2, D = 1,$$
$$\mathcal{E}_2 \cap \mathcal{E}_5 = \left\{\left[\frac{1}{2}, \frac{1}{2}\right]\right\}, \quad \mathcal{E}_3 \cap \mathcal{E}_6 = \left\{\left[\frac{3}{2}, \frac{1}{2}\right]\right\}, \quad \mathcal{E}_4 \cap \mathcal{E}_1 = \left\{\left[\frac{-1}{2}, \frac{1}{2}\right]\right\} \quad \textit{for } C = 1, D = 4.$$

Proof. One can verify this proposition by a direct calculation. (The calculation is considerably facilitated thanks to using the orthogonal transformation T defined above and Proposition 9.) □

Theorem 11. *For the case (I) and $C^2D = 4$, the matrix A has at most two reduction elements.*

Proof. It follows easily from Proposition 18, that $\hat{\mathcal{E}}_1 \cap \hat{\mathcal{E}}_5 = \hat{\mathcal{E}}_2 \cap \hat{\mathcal{E}}_6 = \hat{\mathcal{E}}_3 \cap \hat{\mathcal{E}}_6 = \hat{\mathcal{E}}_1 \cap \hat{\mathcal{E}}_4 = \emptyset$ for $C = 2, D = 1$ and $\hat{\mathcal{E}}_2 \cap \hat{\mathcal{E}}_5 = \hat{\mathcal{E}}_3 \cap \hat{\mathcal{E}}_6 = \hat{\mathcal{E}}_1 \cap \hat{\mathcal{E}}_4 = \emptyset$ otherwise. Together with Theorem 9 this gives the assertion. □

We can formulate the summarizing theorem.

Theorem 12. *An upper bound for the number of reduction elements of the matrix A is given by the table:*

Case	Condition	Upper bound
(I)	$C^2D \geq 4$	2
(I)	$C = 1, D = 2$ or $C = 1, D = 3$	3
(I)	$C = D = 1$	4
(II)	$C^2D \geq 4$	2
(II)	$C = D = 1$ or $C = 1, D = 2$	4

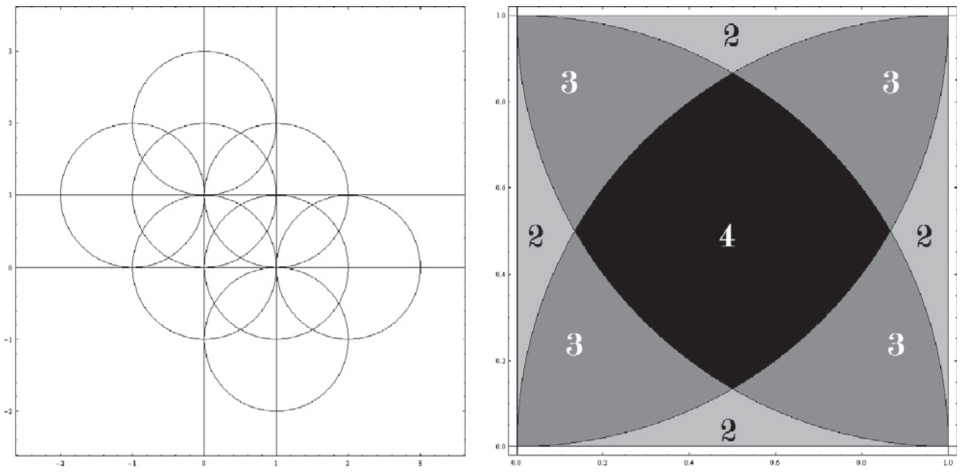

Fig. 1. The case of Gaussian integers ($d = -1$, $C = 1$). Numbers of overlapping ellipses in the quadrant $\{[x, y] \in \mathbb{R}^2; 0 \leq x < 1; 0 \leq y < 1\}$ are presented.

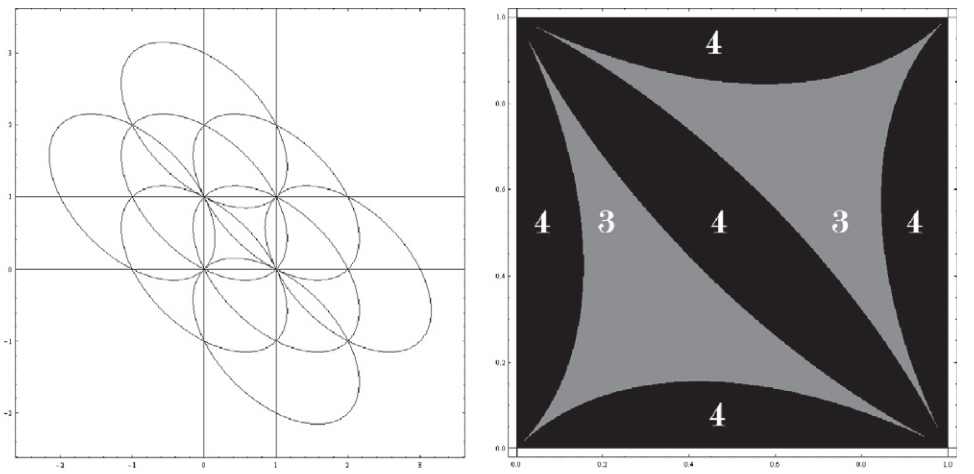

Fig. 2. The case of Eisenstein integers ($d = -3$, $C = 1$). Numbers of overlapping ellipses in the quadrant $\{[x, y] \in \mathbb{R}^2; 0 \leq x < 1; 0 \leq y < 1\}$ are presented.

Proof. See Theorem 4, Theorem 8, Theorem 9, Theorem 10 and Theorem 11. □

At the end of this section, we give two important examples graphically: Gaussian (Fig. 1) and Eisenstein (Fig. 2) integers.

6. The Mathematica package

In this section, we report on an algorithmization for finding reductions for a (1,2)-matrix with entries in an order of an imaginary quadratic field. For this, our main task is to realize the computation of reductions of such matrices as a computer program. It is done in Wolfram Mathematica as a new original package `ReMaOIF.m`.

Input is represented by six numbers: d (negative square-free integer), C (positive integer), u, v, r, s integers representing the matrix $A = [\, a \; b \,] = [\, u+vC\theta \;\; r+sC\theta \,]$. For some reasons, two names of variables are added to input in some commands (we use `x` and `y` here).

We have a number of commands for an investigation of reductionability and we present some of them in the following example.

Example 1. We set the input as $d = -3, C = 1, u = 4, v = 1, r = 1, s = -3$. So, we test the matrix $A = \left[\, 4+\frac{1}{2}(1+\sqrt{-3}) \;\; 1-\frac{3}{2}(1+\sqrt{-3}) \,\right]$.

`OIFella[d, C, u, v, r, s]`
This command gives the reduction ellipse parameters expressed as nine numbers: $R, S, \alpha, \beta, \gamma, s_1, s_2, \xi, \eta$ (see Section 3 for the denotation; $S_{\mathrm{red}} = [s_1, s_2]$, $\Sigma = [\xi, \eta]$).
Output: $\left(7, 21, \frac{9}{2}, -\frac{15}{2}, 14, -\frac{11}{7}, \frac{13}{7}, \frac{3}{7}, -\frac{6}{7}\right)$.

`OIFelld[d, C, u, v, r, s, x, y]`
This command draws the reduction ellipse with the equation $K(x, y) = 0$. (See Fig. 3.)
Output:

`OIFreel[d, C, u, v, r, s, x, y]`
This command gives a list of reduction elements.
Output: $(-1 + \sqrt{-3}, -1 + \frac{1}{2}(1 + \sqrt{-3}), \sqrt{-3})$.

`OIFmmre[d, C, u, v, r, s, x, y]`

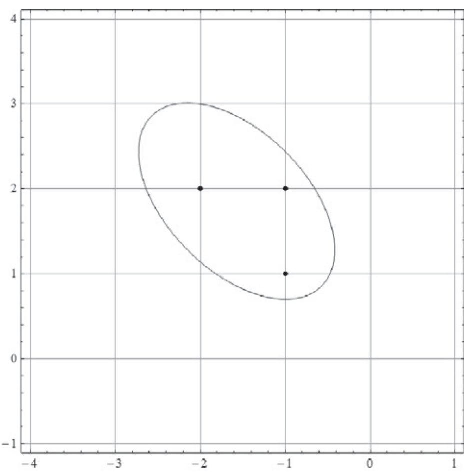

Fig. 3. The reduction ellipse. The three lattice interior points are evident.

This command gives a list of new u, v, r, s after reductions (with respect to every reduction element). Output: ((1, −3, 0, 1), (1, −3, −2, 0), (1, −3, 1, −2)).

Application (Continuation of Example 1). We show an iteration of the procedure. For instance, we choose the second reduction element $q_1 = -1 + \frac{1}{2}(1 + \sqrt{-3})$. We obtain the matrix $A_1 = AE(q_1)^{-1} = \left[\begin{smallmatrix} 1-\frac{3}{2}(1+\sqrt{-3}) & -2 \end{smallmatrix}\right]$. Now, the package `ReMaOIF.m` enables a comfortable repetition of the procedure for A_1: we choose the reduction element $q_2 = \frac{1}{2}(1 + \sqrt{-3})$ and obtain the matrix $A_2 = A_1E(q_2)^{-1} = \left[\begin{smallmatrix} -2 & -1+\frac{1}{2}(1+\sqrt{-3}) \end{smallmatrix}\right]$. If we apply the procedure again for A_2, we obtain only one reduction element $q_3 = (1 + \sqrt{-3})$ and the matrix $A_3 = A_2E(q_3)^{-1} = \left[\begin{smallmatrix} -1+\frac{1}{2}(1+\sqrt{-3}) & 0 \end{smallmatrix}\right]$. Now, $B = A_3$ is a non-reducible matrix and $A = BE(q_3)E(q_2)E(q_1)$ is one of nearly standard forms for the matrix A.

So, if we consider the matrix $M = \left[\begin{smallmatrix} 4+\frac{1}{2}(1+\sqrt{-3}) & 1-\frac{3}{2}(1+\sqrt{-3}) \\ 29 & 3-9(1+\sqrt{-3}) \end{smallmatrix}\right] \in \mathrm{GL}_2(\mathbb{Z}[C\theta])$ ($\det M = 1$), then $M = \left[\begin{smallmatrix} B \end{smallmatrix}\right] E(q_3)E(q_2)E(q_1)$. It follows $M \in \mathrm{GE}_2(\mathbb{Z}[C\theta])$ because of Remark 2.

7. The zone of non-reductionability and some examples

We start this section with the study of areas of zones of non-reductionability. It leads to reflections on a "probability" that a matrix over $\mathbb{Z}[C\theta]$ is non-reducible. We denote the area in question by $P(\mathcal{Z}_{\mathrm{nonred}})$ and use standard integral calculus.

Proposition 19. *In the case (I) and $C^2D \geq 5$, the area of the zone of non-reductionability $\mathcal{Z}_{\mathrm{nonred}}$ is*

$$P(\mathcal{Z}_{\mathrm{nonred}}) = 1 - \frac{1}{C\sqrt{-d}}\left(\frac{2\sqrt{3}}{1-d} + \frac{\alpha_1\beta_1 + \alpha_2\beta_2}{2(1-d)} + 2\left(\arctan\frac{\alpha_1}{\beta_1} + \arctan\frac{\alpha_2}{\beta_2}\right)\right),$$

where

$$\alpha_1 = \sqrt{3} + \sqrt{-d},$$
$$\alpha_2 = -\sqrt{3} + \sqrt{-d},$$
$$\beta_1 = \sqrt{1 - 3d - 2\sqrt{-3d}},$$
$$\beta_2 = \sqrt{1 - 3d + 2\sqrt{-3d}}.$$

Proof. We have proved that the line $y = \frac{1}{2}$ has not any common point with ellipses $\mathcal{E}_i$, $1 \leq i \leq 6$ (Proposition 10). In consideration of Proposition 14, we compute the area $\bar{P}$ bordered by the ellipse $\mathcal{E}_5$ and by the lines p, $x = 0$, $x = \frac{1}{2} + \frac{1}{2}\sqrt{\frac{3}{-d}}$ and the area $\bar{\bar{P}}$ bordered by the ellipse $\mathcal{E}_6$ and by the lines p, $x = \frac{1}{2} + \frac{1}{2}\sqrt{\frac{3}{-d}}$, $x = 1$; then it remains to multiply the sum $\bar{P} + \bar{\bar{P}}$ by 2. (Of course, we have easily found points of intersection of $\mathcal{E}_5$ and $\mathcal{E}_6$: $\left[\frac{1}{2} + \frac{1}{2}\sqrt{\frac{3}{-d}}, 1 - \frac{1}{C}\sqrt{\frac{3}{-d}}\right]$ and $\left[\frac{1}{2} - \frac{1}{2}\sqrt{\frac{3}{-d}}, 1 + \frac{1}{C}\sqrt{\frac{3}{-d}}\right]$.) So, we have

$$P(\mathcal{Z}_{\mathrm{nonred}}) = 2\int_0^{\frac{1}{2}+\frac{1}{2}\sqrt{\frac{3}{4D-1}}} \left(1 + \frac{-Cx - \sqrt{C^2x^2 - 4C^2D(x^2-1)}}{2C^2D}\right) \mathrm{d}x$$
$$+ 2\int_{\frac{1}{2}+\frac{1}{2}\sqrt{\frac{3}{4D-1}}}^{1} \left(1 + \frac{-C(x-1) - \sqrt{C^2(x-1)^2 - 4C^2D((x-1)^2-1)}}{2C^2D}\right) \mathrm{d}x - 1$$

and the result is obtained by a technical simplifying process. □

Proposition 20. *In the case (II) and $C^2D \geq 4$, the area of the zone of non-reductionability $\mathcal{Z}_{\text{nonred}}$ is*

$$P(\mathcal{Z}_{\text{nonred}}) = 1 - \frac{3\sqrt{3} + 2\pi}{6C\sqrt{-d}}$$

Proof. The proof leans on the same reasons as the proof of the previous proposition, but the calculation is considerably easier. We compute the area $\bar{P}$ bordered by the ellipse $\mathcal{E}_5$ and by the lines p, $x = 0$, $x = \frac{1}{2}$ (points of intersection of $\mathcal{E}_5$ and $\mathcal{E}_6$ are $\left[\frac{1}{2}, 1 - \frac{\sqrt{3}}{2C\sqrt{-d}}\right]$ and $\left[\frac{1}{2}, 1 + \frac{\sqrt{3}}{2C\sqrt{-d}}\right]$) and multiply $\bar{P}$ by 4. So, we have

$$P(\mathcal{Z}_{\text{nonred}}) = 4\int_0^{\frac{1}{2}} 1 - \frac{\sqrt{1-x^2}}{C\sqrt{D}}\mathrm{d}x - 1$$

and the result is obtained quickly. □

Thus, the main observation can be formulated as the following result.

Theorem 13. *In the case (I) and $C^2D \geq 5$ as well as in the case (II) and $C^2D \geq 4$, for areas of zones of non-reductionability*

$$\lim_{C \to \infty} P(\mathcal{Z}_{\text{nonred}}) = 1 \quad \textit{and} \quad \lim_{d \to -\infty} P(\mathcal{Z}_{\text{nonred}}) = 1$$

hold.

Proof. The evaluation of limits follows directly from the expressions of areas in Proposition 19 and Proposition 20. □

Now, we return to some examples known from earlier studies of several authors about non-elementary second order matrices over rings, introducing them in Figs. 4 and 5 below.

Example 2 (*Cohn's example* [3]). Let $d = -19$, $C = 1$, $A = [\, 3-\theta \;\; 2+\theta \,]$. We have $P(\mathcal{Z}_{\text{nonred}}) = 1 - \sqrt{\frac{3}{19}} - \frac{2\pi}{3\sqrt{19}} \approx 0.122153$. We find $\Sigma = \left[\frac{4}{11}, \frac{6}{11}\right] \in \mathcal{Z}_{\text{nonred}}$. Before now, there has been proved by Cohn in [3] that $\begin{bmatrix} 3-\theta & 2+\theta \\ -3-2\theta & 5-2\theta \end{bmatrix} \notin \mathrm{GE}_2(\mathbb{Z}[C\theta])$.

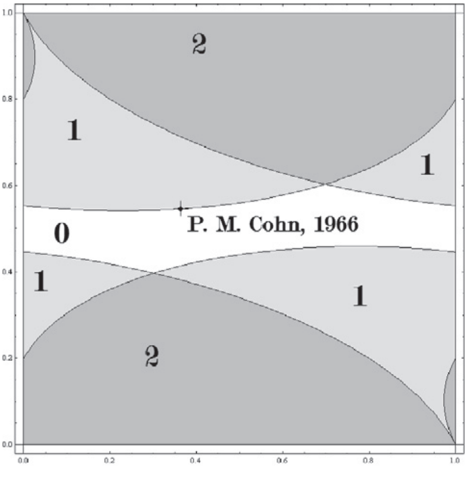

Fig. 4. The marked point represents Cohn's example. The number of reductions is presented, the white zone with 0 is $\mathcal{Z}_{\text{nonred}}$.

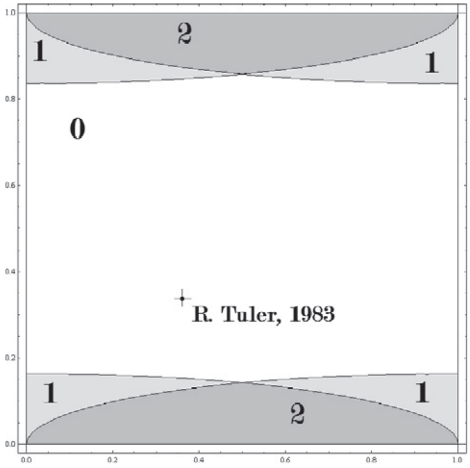

Fig. 5. The marked point represents Tuler's example. The number of reductions is presented, the white zone with 0 is $\mathcal{Z}_{\text{nonred}}$.

Example 3 (*Tuler's example* [5]). Let $d = -37$, $C = 1$, $A = [\,29\ 7-\theta\,]$. We have $P(\mathcal{Z}_{\text{nonred}}) = 1 - \frac{1}{2}\sqrt{\frac{3}{37}} - \frac{\pi}{3\sqrt{37}} \approx 0.685468$. We find $\Sigma = \left[\frac{31}{86}, \frac{29}{86}\right] \in \mathcal{Z}_{\text{nonred}}$. Before now, there has be proved by R. Tuler in [5] that $\begin{bmatrix} 29 & 7-\theta \\ 7+\theta & 3 \end{bmatrix} \notin \mathrm{GE}_2(\mathbb{Z}[C\theta])$.

References

[1] Z.I. Borevich, I.R. Shafarevich, Number Theory, Academic Press Inc., New York, 1966. (translation from Russian).
[2] W.C. Brown, Matrices over Commutative Rings, Marcel Dekker, 1993.
[3] P.M. Cohn, On the structure of GL_2 of a ring, Publ. Math. de l'I.H.É.S. 30 (1966) 5–53.
[4] W. Narkiewicz, Elementary and Analytic Theory of Algebraic Numbers, second ed., PWN – Polish Scientific Publishers, Springer-Verlag, 1990.
[5] R. Tuler, Detecting products of elementary matrices in $GL_2(\mathbb{Z}[\sqrt{d}])$, Proc. Amer. Math. Soc. 89 (1) (1983) 45–48.