CANONICAL NUMBER SYSTEMS OVER IMAGINARY QUADRATIC EUCLIDEAN DOMAINS

ATTILA PETHŐ AND PÉTER VARGA

Abstract. In this paper we investigate canonical number systems over imaginary quadratic Euclidean domains. We define canonical digit set in a uniform way. The linear ECNS polynomials are characterized completely. We prove that for every degree there are infinitely many ECNS polynomials. As a byproduct we give a sufficient condition that a polynomial being symmetric-CNS.

1. Introduction

Decimal representation of integers goes back to ancient time. The number 10 is only one out of infinitely many possibilities to be a base of the radix representation of integers. This concept has far reaching generalizations, see [1], [5], [14] and the references therein. One of the successful generalizations is the concept of canonical number system polynomials with integer coefficients, which will be called in the sequel CNS polynomials. It was introduced by the first author in [13]. Let $P(x) = x^d + p_{d-1}x^{d-1} + \cdots + p_0 \in \mathbb{Z}[x]$ and $\mathcal{N} = \{0, 1, \dots, |p_0| - 1\}$. The polynomial $P(x)$ is called CNS if for every $0 \neq A(x) \in \mathbb{Z}[x]$ there exist h and $a_0, \dots, a_h \in \mathcal{N}$ such that

$$A(x) \equiv a_0 + a_1x + \cdots + a_hx^h \pmod{P(x)}. \tag{1.1}$$

If $P(x)$ is irreducible one gets the concept of canonical number system in algebraic number fields, which was introduced by B. Kovács [10]. The canonical number systems were generalized for Gaussian integers by Jacob and Reveilles [9].

The shift radix systems, SRS, for real vectors were introduced in [1]. Generalizing SRS, Brunotte, Kirschenhofer and Thuswaldner [4] defined GSRS for Hermitian vector spaces. Analyzing the last paper we realized that the CNS concept has a meaningful generalization for Euclidean domains too.

In this paper we will define and investigate a specific canonical number system over imaginary quadratic Euclidean domains. This set has been chosen because by our knowledge this was the best to generalize the theorems

2010 *Mathematics Subject Classification.* Primary 11A63; Secondary 11K16.

Key words and phrases. canonical number systems, Euclidean domains, radix representation.

defined in the original CNS concept and the symmetric CNS concept, see [3]. It is clear that defining the Backward division process, cf. Section 4., it is necessary that the ring over which the polynomials are defined be Euclidean. However this is not sufficient, because we require the uniqueness of the remainder. We show (cf. Section 3) that this happens only if for any $r \in \mathbb{E}$ with $N(r) \geq 2$ there are only finitely many $x \in \mathbb{E}$ with $N(x) < N(r)$, i.e. for the ring of integers of the imaginary quadratic fields $\mathbb{Q}(\sqrt{-d})$ with $d = 1, 2, 3, 7, 11$ (see [8]). In these rings the norm is the square of the usual absolute value of complex numbers. Thus throughout this text we assume that $\mathbb{E}_d$ denotes one of these rings.

Section 3. defines the canonical digit set and describes its properties over the mentioned Euclidean domains. The next section describes the ECNS concept with some of its properties. In Section 5. we characterize completely the linear ECNS polynomials. The CNS case learns us that similar characterization result cannot be expected for higher degree polynomials. However we were able to do a small step for quadratic polynomials, see Theorem 7. It is not too hard to prove that there exist CNS polynomials of arbitrary degree. In the last section we concentrate to the analogous question for ECNS polynomials. It turned out that ECNS polynomials with rational integer coefficients are closely related to polynomials which admit both CNS and symmetric-CNS properties. Realizing this fact we prove the first sufficient condition for the symmetric-CNS property, which enables us to present for any degree infinitely many ECNS polynomials.

2. Basic concepts

Definition 2.1. Let $\mathbb{E}$ be an integral domain. The function $N : \mathbb{E} \mapsto \mathbb{N}$ with the following properties:

- $N(a) = 0$ for an $a \in \mathbb{E}$, if and only if $a = 0$.
- if $a \in \mathbb{E}$ and $b \in \mathbb{E} \setminus \{0\}$, then there are $q, r \in \mathbb{E}$ such that $a = bq + r$ and $N(r) < N(b)$
  is called **Euclidean function**.

Definition 2.2. The integral domain $\mathbb{E}$ is called **Euclidean domain** if it is endowed with a Euclidean function.

Remark 2.3. In these notes the following notations will be used:

$\mathbb{Q}$	field of rational numbers,
$\mathbb{Z}$	ring of integers,
$\mathbb{Z}_{\mathbb{F}[\beta]}$	algebraic integers of the extension $\mathbb{F}[\beta]$, where $\mathbb{F}$ is a field,
i	the imaginary unit $\sqrt{-1}$,
$\lvert z\rvert$	complex absolute value: $\lvert z\rvert := \sqrt{z_1^2+z_2^2}$, where $z \in \mathbb{C}, z_1, z_2 \in \mathbb{R}, z = z_1 + z_2 i$.

Remark 2.4. It was proved by L.E. Dickson [7] and O. Perron [12], see also Hua [8] (Theorem 15.3), that the ring of integers of an imaginary quadratic number field $\mathbb{Q}[\sqrt{-d}]$ is Euclidean iff $d \in \{1, 2, 3, 7, 11\}$. They will be called **imaginary quadratic Euclidean domains** and will be denoted by $\mathbb{E}_d$. Here the Euclidean function is the absolute value function:

$$N(z_1 + z_2 i) := |z_1 + z_2 i|^2 = z_1^2 + z_2^2, \text{ where } z_1, z_2 \in \mathbb{R}.$$

Definition 2.5. Let $\mathbb{E}_d$ be a Euclidean domain. Its **canonical integer basis** is: $\{1, \omega\}$, where $\omega \in \mathbb{E}_d$ and

$$\omega := \begin{cases} \sqrt{-d} & \text{, if } d \in \{1,2\}, \\ \frac{1+\sqrt{-d}}{2} & \text{, otherwise.} \end{cases}$$

(In the case of $d = 1$ for ω the imaginary unit i is used.)
For fixed d, the complex numbers $1, \omega$ form a basis of $\mathbb{C}$, as a two dimensional vector space over $\mathbb{R}$. Thus all $z \in \mathbb{C}$ can be uniquely written in the form $z = e_1 + e_2\omega$ with $e_1, e_2 \in \mathbb{R}$. This representation will be denoted by $(e_1, e_2)_d$. Plainly $z \in \mathbb{E}_d$ iff $e_1, e_2 \in \mathbb{Z}$. Let the functions $Re_d : \mathbb{C} \mapsto \mathbb{R}$ and $Im_d : \mathbb{C} \mapsto \mathbb{R}$ be defined as:

$$Re_d(z) := e_1, \ Im_d(z) := e_2.$$

$Re_d(z)$ and $Im_d(z)$ are called the **Euclidean real and Euclidean imaginary part of** z.

Remark 2.6. For all $z \in \mathbb{C}$,

$$\begin{aligned} Im_d(z) &= \frac{Im(z)}{Im(\omega)}, \\ Re_d(z) &= Re(z) - Im(z)\frac{Re(\omega)}{Im(\omega)}. \end{aligned}$$

Remark 2.7. Let $\mathbb{E}_d$ be a Euclidean domain. The norm of the elements $z \in \mathbb{E}_d$ is calculated as follows:
If $d \in \{1, 2\}$, $N(z) = N(e_1 + e_2\sqrt{-d}) = e_1^2 + de_2^2$, in the other cases $N(z) =$

$N(e_1 + e_2\frac{1+\sqrt{-d}}{2}) = e_1^2 + e_1e_2 + \frac{d+1}{4}e_2^2$. Thus we get

$$N(z) = \begin{cases} e_1^2 + e_2^2 & \text{, if } d = 1, \\ e_1^2 + 2e_2^2 & \text{, if } d = 2, \\ e_1^2 + e_1e_2 + e_2^2 & \text{, if } d = 3, \\ e_1^2 + e_1e_2 + 2e_2^2 & \text{, if } d = 7, \\ e_1^2 + e_1e_2 + 3e_2^2 & \text{, if } d = 11. \end{cases}$$

3. The canonical digit set

Assume that $a, b \in \mathbb{E}_d, b \neq 0$. Let $\mathbb{E}_d^*$ be the set of units in $\mathbb{E}_d$. Let $q, r \in \mathbb{E}_d$ be such that $a = bq+r$ and $N(r) < N(b)$. Then $a = b(q+\varepsilon)+(r-b\varepsilon)$ and $a = b(q + \varepsilon\omega) + (r - b\varepsilon\omega)$ hold for any $\varepsilon \in \mathbb{E}_d^*$. It is well known that

$$\mathbb{E}_d^* = \begin{cases} \{\pm 1\}, & \text{if d = 2, 7, 11;} \\ \{\pm 1, \pm i\}, & \text{if d = 1;} \\ \left\{\pm 1, \frac{\pm 1 \pm \sqrt{-3}}{2}\right\}, & \text{if d = 3.} \end{cases}$$

In some cases the remainder r is not uniquely defined, i.e., not only $N(r) < N(b)$, but also $N(r - b\varepsilon) < N(b)$ or $N(r - b\varepsilon\omega) < N(b)$ holds for some $\varepsilon \in \mathbb{E}_d^*$. This problem has already arisen in the case of rational integers, where the uniqueness of the remainder ensures such that the remainder is assumed to be non-negative. As $\mathbb{E}_d$ is a subset of the complex numbers, different solution has to be chosen. In the next definition we propose canonical digit sets, which depend only on b.

Definition 3.1. Let $\mathbb{E}_d$ be a Euclidean domain and $0 \neq b \in \mathbb{E}_d$. The set

$$\mathbb{D}_{d,b} := \left\{ z \in \mathbb{E}_d \;\middle|\; |z| < |b| \textit{ and } |z + b| \geq |b| \textit{ and } -\frac{1}{2} \leq Im_d\left(\frac{z}{b}\right) < \frac{1}{2} \right\}$$

be called the **(canonical) digit set** for b and $b \in \mathbb{E}_d$ the **base number**.

Remark 3.2. In the definition of the digit set there are three conditions. The first is to make sure that the norm of the digits are smaller than the norm of the base number. The second is to rule out the numbers which are ”negative” in a sense. The last one is to reach a complete residue system.

Remark 3.3. The assumptions ensure that if $b \in \mathbb{Z} \subseteq \mathbb{E}_d$ then $\{sgn(b)j \mid j = 0, \dots, |b| - 1\} \subseteq \mathbb{D}_{d,b}$.

Remark 3.4. The equation $Im_d\left(\frac{z}{b}\right) = s$ defines a line and $|z - a| = r$ defines a circle on the complex plane, where $a \in \mathbb{C}$ is the center of the circle, $b \in \mathbb{E}_d$ represents the direction vector of the line, $r \in \mathbb{R}$ is the radius of the circle and $s \in \mathbb{R}$.

Definition 3.5. For $0 \neq b \in \mathbb{E}_d$ the set

$$\mathbb{V}_{d,b} := \left\{ z \in \mathbb{E}_d \;\middle|\; -\frac{1}{2} \leq Im_d\left(\frac{z}{b}\right) < \frac{1}{2} \right\}$$

is called the **real band**.

Theorem 3.6. *Let $0 \neq b \in \mathbb{E}_d$. Then the set $\mathbb{D}_{d,b}$ is a complete residue system modulo b containing 0. Moreover for any $a \in \mathbb{E}_d$ there exist $q, r \in \mathbb{E}_d$ such that $a = bq + r$ and $r \in \mathbb{D}_{d,b}$, in particular $N(r) < N(b)$.*

Proof. As $a/b \in \mathbb{C}$ there exist $u_1, u_2 \in \mathbb{R}$ such that $\frac{a}{b} = u_1 + u_2\omega$. Write $u_i = q_i + r_i, i = 1, 2$ such that $q_1, q_2 \in \mathbb{Z}$ and $-\frac{1}{2} \leq r_i < \frac{1}{2}$ and put $q' = q_1 + q_2\omega, r' = r_1 + r_2\omega$ and $r'' = br'$. Then $a = bq' + r''$ and $q' \in \mathbb{E}_d$, thus $r'' \in \mathbb{E}_d$. Further $Im_d\left(\frac{r''}{b}\right) = Im_d(r')$. Thus $-\frac{1}{2} \leq Im_d\left(\frac{r''}{b}\right) < \frac{1}{2}$.

Further $N(r'') = N(b)N(r')$, and by Remark 2.7 $N(r') \leq \frac{3}{4}$, if $d \leq 3$ and $N(r') \leq \frac{5}{4}$ in the remaining two cases. If $N(r') < 1$, then we have also the inequality $N(r'') < N(b)$. Assume that $N(r') \geq 1$, which can happen only if $d = 7, 11$ and $r_1r_2 > 0$. Then redefine $r'' = b(r' + (-1)\frac{r_1}{|r_1|})$. Plainly we have $r'' \in \mathbb{E}_d$ such that $N(r'') < N(b)$ and $-\frac{1}{2} \leq Im_d\left(\frac{r''}{b}\right) < \frac{1}{2}$ hold.

Finally consider the sequence $r'' + mb, m = 0, 1, \ldots$. As the function $f(x) = N(r'' + xb)$ tends to infinity with $x \to \infty$ and $f(0) < N(b)$ there exists an $x_0 > 0$ such that $f(x_0) = N(b)$. Taking $m = \lfloor x_0 \rfloor$ we get $f(r'' + mb) < b$ and $f(r'' + (m+1)b) \geq b$. Putting $r = r'' + mb$ and $q = (a - r)/b$ we get $a = bq + r, q, r \in \mathbb{E}_d$ and $r \in \mathbb{D}_{d,b}$. As a was arbitrary $\mathbb{D}_{d,b}$ includes a complete residue system modulo b.

It remains to prove that the elements of $\mathbb{D}_{d,b}$ are incongruent modulo b. Assume that $a \in \mathbb{D}_{d,b}$ and $e := (e_1, e_2)_d \in \mathbb{E}_d \setminus \{0\}$ such that $a + eb \in \mathbb{D}_{d,b}$ holds too. Then both inequalities

$$-\frac{1}{2} \leq Im_d\frac{a}{b} < \frac{1}{2},\; -\frac{1}{2} \leq Im_d\frac{a+eb}{b} < \frac{1}{2}$$

hold. On the other hand $Im_d\frac{a+eb}{b} = Im_d\frac{a}{b} + e_2$, where e_2 is an integer. Thus both inequalities can hold only if $e_2 = 0$.

If $e_2 = 0$ then $eb = e_1b$ with an integer e_1. Assume that $e_1 \neq 0$. If $|e_1| \geq 2$ then using $|a| < |b|$ we obtain $|a + e_1b| \geq |e_1b| - |a| > 2|b| - |b| \geq |b|$, which contradicts $a + e_1b \in \mathbb{D}_{d,b}$. Hence $e_1 = \pm 1$.

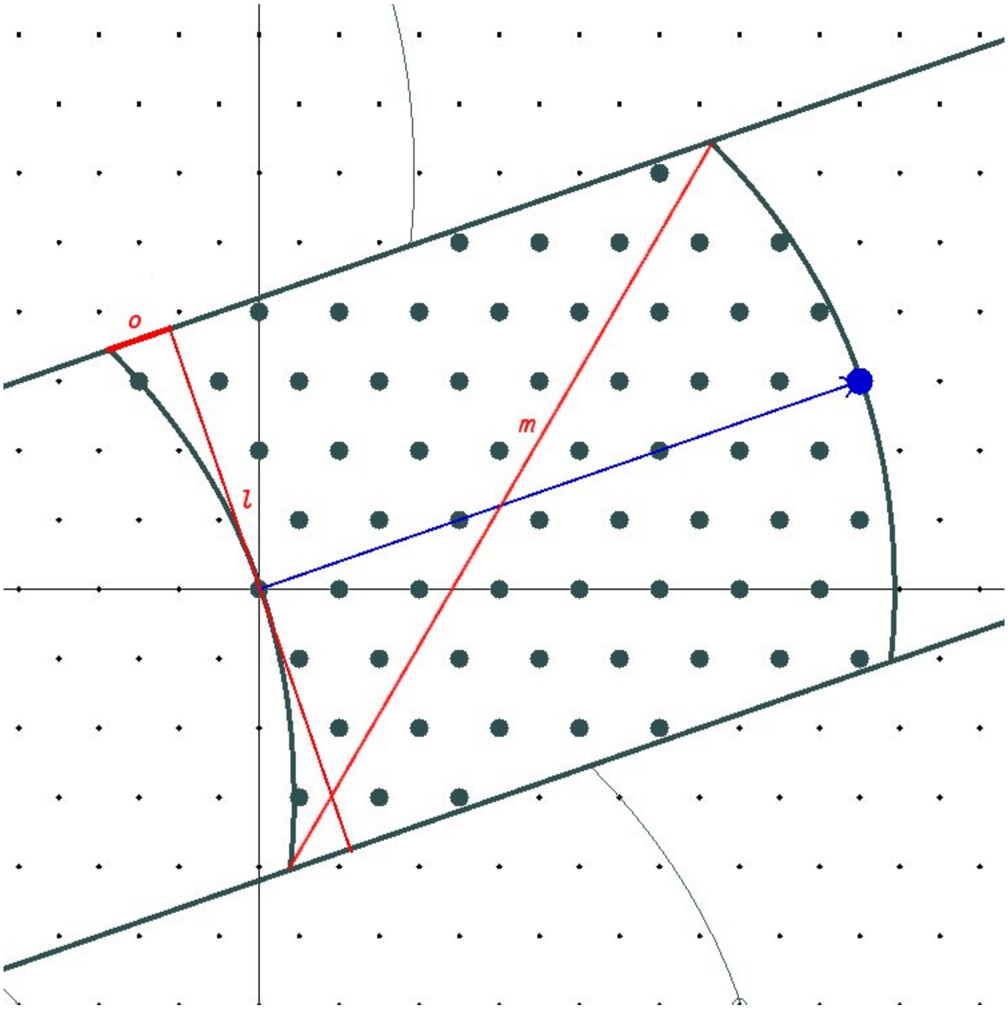
If $e_1 = -1$ then as $a - b \in \mathbb{D}_{d,b}$ we get $|a| = |(a - b) + b| \geq |b|$, which contradicts $a \in \mathbb{D}_{d,b}$. Finally if $e_1 = 1$ then as $a + b \in \mathbb{D}_{d,b}$ we have $|a + b| < |b|$, which again contradicts $a \in \mathbb{D}_{d,b}$. The proof is completed.

□

Let $a, b \in \mathbb{E}_d$ with $b \neq 0$. There exist by Theorem 3.6 uniquely defined $q \in \mathbb{E}_d$ and $r \in \mathbb{D}_{d,b}$ such that $a = bq + r$. In the sequel we will use the notation $q = \lfloor \frac{a}{b} \rfloor$.

Definition 3.7. Let $\mathbb{D}_{d,b}$ be a canonical digit set.
Let's define the followings for this digit set:
line distance: $l := Im(\omega)|b|$.
corner offset: $o := |b| - \sqrt{|b|^2 - \left(\frac{l}{2}\right)^2}$.
maximum distance between digits: $m := \sqrt{|b|^2 + l^2}$.

FIGURE 1. Digit set measures in $\mathbb{E}_3$, when the base of the digit set is $(6,3)_3$ (large dot). 'o': corner offset, 'l': line distance, 'm': maximum distance between digits



Remark 3.8. Let $\mathbb{E}_d$ be a Euclidean domain, and let $b \in \mathbb{E}_d$ be the base of the digit set $\mathbb{D}_{d,b}$.

d	Corner offset (o)	Line distance (l)	Maximum distance between digits (m)
1	$\lvert b\rvert \left(1-\frac{\sqrt{3}}{2}\right)$	$\lvert b\rvert$	$\lvert b\rvert\sqrt{2}$
2	$\lvert b\rvert \left(1-\frac{\sqrt{2}}{2}\right)$	$\lvert b\rvert\sqrt{2}$	$\lvert b\rvert\sqrt{3}$
3	$\lvert b\rvert \left(1-\frac{\sqrt{13}}{4}\right)$	$\lvert b\rvert\frac{\sqrt{3}}{2}$	$\lvert b\rvert\frac{\sqrt{7}}{2}$
7	$\lvert b\rvert\frac{1}{4}$	$\lvert b\rvert\frac{\sqrt{7}}{2}$	$\lvert b\rvert\frac{\sqrt{11}}{2}$
11	$\lvert b\rvert \left(1-\frac{\sqrt{5}}{4}\right)$	$\lvert b\rvert\frac{\sqrt{11}}{2}$	$\lvert b\rvert\frac{\sqrt{15}}{2}$

Lemma 3.9. *Let $a, b \in \mathbb{E}_d, b \neq 0$. If $|a| < \frac{Im(\omega)|b|}{2}$, then $a \in \mathbb{V}_{d,b}$.*

Proof. The assumption $|a| < \frac{Im(\omega)|b|}{2}$ implies $\left|\frac{a}{b}\right| < \frac{Im(\omega)}{2}$. As $|z| \geq |Im(z)|$ we get $\frac{|Im(a/b)|}{Im(\omega)} < \frac{1}{2}$, i.e. $a \in \mathbb{V}_{d,b}$. □

Lemma 3.10. *Let $a, b \in \mathbb{E}_d$ with $N(b) \geq 2$. If $|a| < \frac{l}{2}$ and $q = \left\lfloor \frac{a}{b} \right\rfloor$ then $q = 0, -1$.*

Proof. Let $a = bq + r$ with $q \in \mathbb{E}_d$ and $r \in \mathbb{D}_{d,b}$. Then

$$Im_d(q) = Im_d\left(\frac{a}{b}\right) + Im_d\left(\frac{-r}{b}\right).$$

By the assumption on a and as $r \in \mathbb{D}_{d,b}$ we get

$$|Im_d(q)| < \frac{1}{2} + \frac{1}{2} = 1,$$

i.e. $q \in \mathbb{Z}$. Further we have

$$|bq| \leq |a| + |r| < \frac{Im\,(\omega)\,|b|}{2} + |b|.$$

Dividing by $|b|$ we obtain $|q| < \frac{3}{2}$, thus $q \in \{0, \pm 1\}$. If $q = 1$ then $a = b + r$. The assumption $r \in \mathbb{D}_{d,b}$ implies $|a| = |b + r| \geq |b|$, which contradicts the assumption on a. □

Lemma 3.11. *If $z \in \mathbb{V}_{d,b}$ and $a \in \mathbb{Z}$, then $z + a \cdot b \in \mathbb{V}_{d,b}$.*

Proof. We have

$$Im_d\left(\frac{z + ab}{b}\right) = Im_d\left(\frac{z}{b}\right) + Im_d(a) = Im_d\left(\frac{z}{b}\right),$$

which proves the assertion. □

4. ECNS polynomials over imaginary quadratic Euclidean domains

In this section definitions and theorems will be about the CNS concept which needs only an imaginary quadratic Euclidean domain, a canonical digit set and a floor function over its quotient field. The digit set and the floor function are sufficient for an unambiguous definition of a number system over the Euclidean domain.

Definition 4.1. Let $\mathbb{E}_d$ be an imaginary quadratic Euclidean domain with a Euclidean function N, let $P(x) = x^n + p_{n-1}x^{n-1} + \cdots + p_0 \in \mathbb{E}_d[x]$ be a monic polynomial over $\mathbb{E}_d$ such that $N(p_0) \geq 2$, and let $\mathbb{D}_{d,p_0} \subset \mathbb{E}_d$ be the canonical digit set. The factor ring $\mathbb{E}_d[x]/\mathbb{E}_d[x]P(x)$ can be represented by polynomials over $\mathbb{E}_d$ of degree at most $n-1$. This set is denoted by $\mathbb{E}_d^{n-1}[x]$. If for an $a(x) \in \mathbb{D}_{d,p_0}[x]$ there exists $A(x) \in \mathbb{E}_d^{n-1}[x]$ such that

$$A(x) \equiv a(x) \pmod{P(x)},$$

then $A(x)$ has a **canonical expansion**. If all $A(x) \in \mathbb{E}_d^{n-1}[x]$ have canonical expansion, then the polynomial $P(x) \in \mathbb{E}_d[x]$ is called **ECNS polynomial**.

Remark 4.2. If K is a set we denote by $K[x]$ the set of polynomials with coefficients belonging to K.

Definition 4.3. Let the **length** of a polynomial $A = \sum_{i=0}^{n} a_i x^i$ be $l(A) := \sum_{i=0}^{n} |a_i|$.

Let $\mathbb{K}_d$ denote the quotient field of $\mathbb{E}_d$. With irreducible ECNS polynomials numeration systems can be defined in $\mathbb{E}_d$ and in some of its extensions. Indeed, let $P(x)$ be an irreducible ECNS polynomial over $\mathbb{E}_d$ and let γ denote one of its zeroes. Then $\mathbb{K}_d[x]/P(x)\mathbb{K}_d[x]$ is isomorphic to the field $\mathbb{K}_d(\gamma)$. Moreover $\mathbb{E}_d[x]/P(x)\mathbb{E}_d[x]$ is isomorphic to the ring $\mathbb{E}_d[\gamma]$. Thus every element $0 \neq \beta \in \mathbb{E}_d[\gamma]$ can be written uniquely in the form

$$\beta = \sum_{j=0}^{h} b_j \gamma^j, \quad b_j \in \mathbb{D}_{d,p_0}, b_h \neq 0.$$

Remark 4.4. The polynomial $P(x) = x + g, 0 \neq g \in \mathbb{E}_d$ is obviously irreducible. This implies that g with the digit set $\mathbb{D}_{d,g}$ defines a numeration system in $\mathbb{E}_d$ if and only if $x + g$ is a ECNS polynomial.

Definition 4.5. Let $P(x) = x^n + p_{n-1}x^{n-1} + \cdots + p_0 \in \mathbb{E}_d^n[x]$ be such that $N(p_0) \geq 2$. Let the mapping $T_P : \mathbb{E}_d^{n-1}[x] \mapsto \mathbb{E}_d^{n-1}[x]$ be defined as follows: for $A(x) = a_{n-1}x^{n-1} + \cdots + a_0 \in \mathbb{E}_d^{n-1}[x]$ let

$$T_P(A) = \frac{A - qP - r}{x},$$

where $q = \left\lfloor \frac{a_0}{p_0} \right\rfloor$ and $r = a_0 - qp_0 \in \mathbb{D}_{d,p_0}$. The mapping T_P is called **Backward division**.

The mapping backward division can be iterated, which means

$$T_P^k(A) = \begin{cases} A, & \text{if} \quad k = 0; \\ T_P(T_P^{k-1}(A)), & \text{if} \quad k > 0. \end{cases}$$

Let $q_k \in \mathbb{E}_d$ and $r_k \in \mathbb{D}_{d,p_0}$ be defined by the equation

$$T_P^{k+1}(A) = \frac{T_P^k(A) - q_k P - r_k}{x},$$

where $a_0^{(k)} = T_P^k(A)|_{x=0}, q_k = \left\lfloor \frac{a_0^{(k)}}{p_0} \right\rfloor$ and $r_k = a_0^{(k)} - q_k p_0, k \in \mathbb{N}$. Let $A_k := T_P^k(A)$.

The orbit of T_P starting with A will be denoted as follows:

$$A \underset{P}{\overset{(q_1,r_1)}{\Longrightarrow}} A_1 \underset{P}{\overset{(q_2,r_2)}{\Longrightarrow}} A_2 \underset{P}{\overset{(q_3,r_3)}{\Longrightarrow}} A_3 \ldots,$$

if it is not necessary to know the multipliers, it will simply be denoted:

$$A \underset{P}{\overset{r_1}{\Rightarrow}} A_1 \underset{P}{\overset{r_2}{\Rightarrow}} A_2 \underset{P}{\overset{r_3}{\Rightarrow}} A_3 \ldots,$$

or if it is not necessary to know even the remainders, it will simply be denoted:

$$A \underset{P}{\Rightarrow} A_1 \underset{P}{\Rightarrow} A_2 \underset{P}{\Rightarrow} A_3 \ldots.$$

If for $A, B \in \mathbb{E}_d^{n-1}[x]$ there exists $k \in \mathbb{N}$ such that $T_P^k(A) = B$ then we write:

$$A \underset{P}{\overset{*}{\Rightarrow}} B.$$

Plainly the orbits of T_P are either ultimately periodic or consist of infinitely many pairwise different elements and both cases may occur. Moreover in the first case the orbit is ultimately 0 or not. One of the basis aim of the investigations on CNS polynomials is the distinction between these possibilities.

Theorem 4.6. *$P(x) \in \mathbb{E}_d^n[x]$ is a ECNS polynomial if and only if for all $A(x) \in \mathbb{E}_d^{n-1}[x]$*

$$A \underset{P}{\overset{*}{\Rightarrow}} 0.$$

Proof. This theorem is a direct consequence of Definitions 4.1 and 4.5. □

Theorem 4.7. *Let $P(x) := p_0 + p_1x + \cdots + p_nx^n + p_{n+1}x^{n+1} \in \mathbb{E}_d^{n+1}[x]$ be such that $p_{n+1} = 1, N(p_0) \geq 2$. Assume that the orbit of T_P starting with $A(x) := a_0 + a_1x + \cdots + a_nx^n \in \mathbb{E}_d^n[x]$ is periodic of length $l > n$*

$$A = A_0 \underset{P}{\overset{(q_0,r_0)}{\Longrightarrow}} A_1 \underset{P}{\overset{(q_1,r_1)}{\Longrightarrow}} A_2 \underset{P}{\overset{(q_2,r_2)}{\Longrightarrow}} A_3 \ldots \underset{P}{\overset{(q_{l-2},r_{l-2})}{\Longrightarrow}} A_{l-1} \underset{P}{\overset{(q_{l-1},r_{l-1})}{\Longrightarrow}} A.$$

Then

$$-\sum_{m=0}^{n+1} q_{l+h-m}p_m \in \mathbb{D}_{d,p_0}$$

holds for $h = 0, 1, \ldots, l-1$.

Proof. Let $A_h(x) = \sum_{j=0}^{\infty} a_j^{(h)} x^j$, where $a_j^{(h)} = 0$ for all $h \geq 0$ and $j > n$. Similarly we write $P(x) = \sum_{j=0}^{\infty} p_jx^j$ with $p_j = 0$ for $j > n+1$. With these notation we have

$$a_j^{(h)} = a_{j+h}^{(0)} - \sum_{k=0}^{h-1} q_kp_{j+h-k}. \tag{4.1}$$

Indeed, the claim is true for $h = 0$ because the empty sum is 0. Assume that it is true for a $h \geq 0$. Then

$$A_{h+1} = T_P(A_h) = \frac{A_h - q_h P - r_h}{x}.$$

Comparing the coefficients and using the induction hypothesis we get

$$\begin{aligned} a_j^{(h+1)} &= a_{j+1}^{(h)} - q_h p_{j+1} \\ &= a_{j+h+1}^{(0)} - \sum_{k=0}^{h-1} q_k p_{j+1+h-k} - q_h p_{j+1} \\ &= a_{j+h+1}^{(0)} - \sum_{k=0}^{h} q_k p_{j+1+h-k}, \end{aligned}$$

which proves the claim.

Consider equation (4.1) for $j = 0$ and $h = l, \ldots, 2l-1$. By the assumption $A_h(x) = A_{h+l}(x), h = 0, \ldots, l-1$, especially $a_0^{(h+l)} = a_0^{(h)}, h = 0, \ldots, l-1$. Thus

$$q_{h+l} = \left\lfloor \frac{a_0^{(h+l)}}{p_0} \right\rfloor = \left\lfloor \frac{a_0^{(h)}}{p_0} \right\rfloor = q_h.$$

As $l > n$ we have $a_{l+h}^{(0)} = 0$ for $h \geq 0$. Summarizing (4.1) leads to

$$a_0^{(h)} = a_0^{(l+h)} = - \sum_{k=0}^{l+h-1} q_k p_{l+h-k}, \; h = 0, \ldots, l-1.$$

By the construction $a_0^{(l+h)} - q_{l+h} p_0 = r_{l+h} \in \mathbb{D}_{d,p_0}$, hence

$$- \sum_{k=0}^{l+h} q_k p_{l+h-k} \in \mathbb{D}_{d,p_0}, \; h = 0, \ldots, l-1.$$

Replacing the summation variable k by $m = l + h - k$ and taking into account that $p_m = 0$ for $m > n+1$ we obtain

$$- \sum_{m=0}^{n+1} q_{l+h-m} p_m \in \mathbb{D}_{d,p_0}, \; h = 0, \ldots, l-1,$$

as we stated. □

Remark 4.8. If we apply Theorem 4.7 with length 1, we get the following restriction for the coefficients of a ECNS polynomial:

$$-q \sum_{m=0}^{n+1} p_m \notin \mathbb{D}_{d,p_0},$$

where $q = \frac{a}{p_0}$, for all $a \in \mathbb{E}_d \setminus \{0\}$.

Remark 4.9. The assumption $l > n$ in Theorem 4.7 is not a serious restriction because any positive integer multiple of a period length is again a period length.

5. Linear ECNS polynomials over imaginary quadratic Euclidean domains

Investigating the linear case, Theorem 5.5 below shows that the ECNS property of linear polynomials is easily decidable over imaginary quadratic Euclidean domains.

In this section we will often refer to the real band $\mathbb{V}_{d,p}$, which will be called, for simplicity, band.

Lemma 5.1. *Let $P(x) := x + p$ be over $\mathbb{E}_d$ with $N(p) \geq 2$. If the Line distance $l = Im(\omega)|p|$ is greater than 2, a necessary condition for the ECNS property is $1 \in \mathbb{D}_{d,p}$.*

Proof. Assume that $1 \notin \mathbb{D}_{d,p}$.
The assumption $l > 2$ and Lemma 3.9 mean that $\mathbb{V}_{d,p}$ includes the closed unit disc, thus $1 \in \mathbb{V}_{d,p}$. Lemma 3.10, $|p| > 1$ and $1 \notin \mathbb{D}_{d,p}$ mean that $\left\lfloor \frac{1}{p} \right\rfloor = 1$, so

$$1 \underset{P}{\Rightarrow} 1,$$

which is a cycle, thus P cannot be a ECNS polynomial. □

Remark 5.2. It is easy to check that $1 \in \mathbb{D}_{d,p}$ is equivalent to $Re(p) \geq -1/2$ except when

$$p = \begin{cases} 1-i, -2i & : \quad d = 1 \\ -\sqrt{-2} & : \quad d = 2 \\ \pm\sqrt{-3}, 1-\sqrt{-3} & : \quad d = 3 \\ \frac{\pm 1 - \sqrt{-7}}{2} & : \quad d = 7. \end{cases}$$

Lemma 5.3. *Let $P(x) := x + p$ be over $\mathbb{E}_d$ with $N(p) \geq 2$. To decide the ECNS property those and only those polynomials have to be investigated, where*

$$\begin{aligned} A(x) &:= a \textit{ with } a \in \mathbb{E}_d \textit{ and} \\ |a| &\leq \sqrt{\frac{|p|+1}{|p|-1}}. \end{aligned}$$

Proof. Let $A \in \mathbb{E}_d[x]$. Consider the orbit of T_P, which starts at A. If $l(T_P(A)) < l(A)$ then iterate T_P. As $l(A)$ is a non-negative integer we have to reach an element B of the orbit such that $l(T_P(B)) \geq l(B)$. We may assume without loss of generality that this happens already at the beginning, i.e. with A. The length of $T_P(A)$ is

$$l(T_P(A)) = |q| = \left|\frac{a-r}{p}\right| \leq \frac{|a|+|r|}{|p|}.$$

Thus $l(A) \leq l(T_P(A))$ implies

$$|a| \leq \frac{|a|+|r|}{|p|},$$

which leads to

$$|a| \leq \sqrt{\frac{|p|+1}{|p|-1}}$$

since $N(r) < N(p)$, that is $|r|^2 \leq |p|^2 - 1$. □

Theorem 5.4. *Let* $P(x) := x + p$ *be a linear polynomial over* $\mathbb{E}_d$ *with* $N(p) \geq 2$*. If* $Im(\omega)|p| = l > 2\sqrt{\frac{|p|+1}{|p|-1}}$*, a sufficient and necessary condition for the ECNS property is* $1 \in \mathbb{D}_{d,p}$.

Proof. From Lemma 5.3, those and only those constant polynomials a have to be investigated for the ECNS property, where $|a| \leq \sqrt{\frac{|p|+1}{|p|-1}}$.
Since $\frac{l}{2} > \sqrt{\frac{|p|+1}{|p|-1}}$ we have $q = \left\lfloor \frac{a}{p} \right\rfloor \in \{0, -1\}$ by Lemma 3.10, thus all orbits of T_P terminate either at 0 or at -1. If $1 \in \mathbb{D}_{d,p}$ then P is a ECNS polynomial, and since $l > 2$ is also satisfied, from Lemma 5.1, this is not just sufficient but necessary condition as well. □

Theorem 5.5. *Let* $P(x) := x + p$ *be a linear polynomial over* $\mathbb{E}_d$ *and* $N(p) \geq 2$*.* $P(x)$ *is a ECNS polynomial if and only if* $1 \in \mathbb{D}_{d,p}$ *or* $p \in \left\{1-i, -2i, -\sqrt{-2}, \sqrt{-3}, -\sqrt{-3}, 1-\sqrt{-3}, \frac{1-\sqrt{-7}}{2}, \frac{-1-\sqrt{-7}}{2}\right\}$.

Proof. By Lemma 5.3 it is enough to check the representability only those constant polynomials $A(x) = a$ with

$$|a| \leq \sqrt{\frac{|p|+1}{|p|-1}},$$

which implies

$$N(a) \leq \frac{|p|+1}{|p|-1} = 1 + \frac{2}{|p|-1} = 1 + \frac{2}{\sqrt{N(p)}-1}.$$

Table 1 presents the possible values of $N(a)$ for each $N(p)$.

The necessary constant polynomials for the case $2 \leq N(p)$ will be investigated. By Theorem 5.4 if $\frac{l}{2} > \sqrt{\frac{|p|+1}{|p|-1}}$, a sufficient and necessary condition

$N(p)$	$1+\frac{2}{\sqrt{N(p)}-1}$	$N(a)$
2	≈ 5.8284	$\in \{0,1,2,3,4,5\}$
3	≈ 3.7321	$\in \{0,1,2,3\}$
4	$= 3.0000$	$\in \{0,1,2,3\}$
5	≈ 2.6180	$\in \{0,1,2\}$
6	≈ 2.3798	$\in \{0,1,2\}$
7	≈ 2.2153	$\in \{0,1,2\}$
8	≈ 2.0938	$\in \{0,1,2\}$
9	$= 2.0000$	$\in \{0,1,2\}$
≥ 10	< 2	$\in \{0,1\}$

TABLE 1

for the ECNS property is $1 \in \mathbb{D}_{d,p}$. Thus it is enough to check the case $\frac{l}{2} \leq \sqrt{\frac{|p|+1}{|p|-1}}$. Then

$$\begin{aligned}
\frac{l^2}{4} &\leq 1+\frac{2}{|p|-1}, \\
(l^2-4)(|p|-1) &\leq 8, \\
|p| &\leq \frac{l^2+4}{l^2-4}, \\
|p| &\leq \frac{(Im(\omega)|p|)^2+4}{(Im(\omega)|p|)^2-4}, \\
Im(\omega)^2|p|^3 - Im(\omega)^2|p|^2 - 4|p| - 4 &\leq 0, \\
Im(\omega)^2\sqrt{N(p)}^3 - Im(\omega)^2\sqrt{N(p)}^2 - 4\sqrt{N(p)} - 4 &\leq 0.
\end{aligned}$$

The cubic polynomial in $\sqrt{N(p)}$ staying on the left hand side of the last inequality has exactly one positive real root. The possible values of $N(p)$ lie between zero and this root. We present these in Table 2.

d	$N(p) <$	$N(p) \in$
1	8.2664	$\{2,3,4,5,6,7,8\}$
2	5.1508	$\{2,3,4,5\}$
3	10.1968	$\{2,3,4,5,6,7,8,9,10\}$
7	5.6206	$\{2,3,4,5\}$
11	4.2163	$\{2,3,4\}$

TABLE 2

For each triplets (d,p,a) with $d \in \{1,2,3,7,11\}$, $p,a \in \mathbb{E}_d$ such that $N(p)$ and $N(a)$ satisfy the conditions of Table 2 and Table 1 respectively we checked the representability of a. To summarize, if $1 \in \mathbb{D}_{d,p}$ then $x+p$ is a ECNS polynomial. If $1 \notin \mathbb{D}_{d,p}$ then $x+p$ is a ECNS polynomial, if and only if $p \in \left\{1-i, -2i, -\sqrt{-2}, \sqrt{-3}, -\sqrt{-3}, 1-\sqrt{-3}, \frac{1-\sqrt{-7}}{2}, \frac{-1-\sqrt{-7}}{2}\right\}$. □

6. Quadratic ECNS polynomials over imaginary quadratic Euclidean domains

The characterization of quadratic ECNS polynomials seems to be much more difficult than the characterization of the linear ones. In the present section this problem will be investigated. The first theorem is to decrease the possible quadratic CNS polynomials to a finite set for a fixed constant term p_0.

Theorem 6.1. *Let $P(x) := x^2 + p_1x + p_0$ be a quadratic polynomial over $\mathbb{E}_d$. If $P(x)$ is a ECNS polynomial then it is expanding.*

Proof. $\mathbb{E}_d[x]/P(x)\mathbb{E}_d[x]$ is isomorphic to the ring $\mathbb{E}[\gamma]$, where $P(\gamma) = 0$. This is true for both roots of the polynomial $P(x)$. If the norm of one of these is less then 1, then the representation of the elements $0 \neq \beta \in \mathbb{E}[\gamma]$ is bounded, so this cannot represent all elements β:

$$|\beta| = \left|\sum_{j=0}^{h} b_j\gamma^j\right| \leq \sum_{j=0}^{h} |b_j||\gamma^j| \leq |p_0|\sum_{j=0}^{h} |\gamma|^j \leq$$

$$\leq |p_0| \lim_{h\to\infty} \sum_{j=0}^{h} |\gamma|^j = |p_0|\frac{1}{1-|\gamma|} \quad (\text{if } |\gamma| < 1).$$

The case when $|\gamma| = 1$ has been proved by the first author in [13]. □

Theorem 6.2. *Let $P(x) := x^2 + p_1x + p_0$ be a quadratic polynomial over $\mathbb{E}_d$, $N(p_0) \geq 2$. It is expanding, if*

$$\frac{|\bar{p_1} - \bar{p_0}p_1|}{|p_0|^2 - 1} < 1,$$

where $\bar{x}$ is the complex conjugate of x.

Proof. This result comes from the Lehmer-Schur [11] algorithm. Let

$$P^*(x) = \bar{p_0}x^2 + \bar{p_1}x + 1, \text{ and}$$

$$g(x) = \bar{p_0}P(x) - P^*(x) = (\bar{p_0}p_1 - \bar{p_1})x + \bar{p_0}p_0 - 1.$$

The root of $g(x)$ is:

$$x_0 = \frac{1 - \bar{p_0}p_0}{\bar{p_0}p_1 - \bar{p_1}}.$$

Thus $P(x)$ is expanding iff $|x_0| > 1$, i.e.

$$1 < |x_0| = \left|\frac{1 - \bar{p_0}p_0}{\bar{p_0}p_1 - \bar{p_1}}\right| = \frac{||p_0|^2 - 1|}{|\bar{p_1} - \bar{p_0}p_1|} = \frac{|p_0|^2 - 1}{|\bar{p_1} - \bar{p_0}p_1|}.$$

□

Remark 6.3.
For a fixed p_0 the inequality of Theorem 6.2 determines a finite set of p_1. We have

$$\frac{|\bar{p_1} - \bar{p_0}p_1|}{|p_0|^2 - 1} \geq \frac{|p_0|\,|p_1| - |p_1|}{|p_0|^2 - 1} = \frac{|p_1|}{|p_0| + 1}.$$

Hence if $|p_1| \leq |p_0| + 1$, then the inequality of Theorem 6.2 follows.

Theorem 6.4. *Let $P(x) := x^2 + p_1 x + p_0$ be a quadratic polynomial over $\mathbb{E}_d$, $N(p_0) \geq 2$. If*

$$|p_1| \leq \left(1 - \frac{1}{\sqrt{2}}\right) |p_0| - 1,$$

then the orbits of T_P are periodic for all $A \in \mathbb{E}_d[x]$. Moreover there are only four possible periods, the trivial $\{0\}$ cycle and the following ones:

$$x + (p_1 + 1) \xrightarrow[P]{(-1,r_0)} x + (p_1 + 1), \quad r_0 \in \mathbb{D}_{d,p_0},$$

$$1 \xrightarrow[P]{(-1,r_0)} x + p_1 \xrightarrow[P]{(0,r_1)} 1, \quad r_0, r_1 \in \mathbb{D}_{d,p_0},$$

$$1 \xrightarrow[P]{(-1,r_0)} x + p_1 \xrightarrow[P]{(-1,r_1)} x + (p_1 + 1) \xrightarrow[P]{(0,r_2)} 1, \quad r_0, r_1, r_2 \in \mathbb{D}_{d,p_0}.$$

Proof. Assume that $A(x) = a_1 x + a_0 \in \mathbb{E}_d[x]$ with T_P leads to a period of length $n \geq 2$. Then by Theorem 4.7 the inclusions

$$-q_{j-2} - p_1 q_{j-1} - p_0 q_j \in \mathbb{D}_{d,p_0}$$

hold for $j = 0, 1, \ldots, n-1$, where we used $q_{-2} = q_{n-2}$ and $q_{-1} = q_{n-1}$. For a fixed p_0 these conditions can be transformed to a restriction for the linear term p_1. In fact if $q_j \neq 0$ then

$$p_1 \in \frac{\mathbb{D}_{d,p_0} + p_0 q_k + q_i}{-q_j},$$

and this is a conformal mapping of the digit set. If $q_j = 0$, then

$$q_k = \left\lfloor \frac{-q_i}{p_0} \right\rfloor,$$

which is a restriction for the position of p_0.

Let's check p_1's minimal absolute value in the intersection of the sets $\frac{\mathbb{D}_{d,p_0} + p_0 q_k + q_i}{-q_j}$. If the cycle does not contain 0 multiplier, let h be the index of the multiplier which has maximal absolute value: $|q_h| \geq |q_i|, i \in$

$\{0, 1, \ldots, n-1\}$.

$$\begin{aligned}
\min |p_1| &= \min \left\{ |t| \;:\; t \in \bigcap \frac{\mathbb{D}_{d,p_0} + p_0 q_k + q_i}{-q_j} \right\} \\
&\geq \min \left\{ |t| \;:\; t \in \frac{\mathbb{D}_{d,p_0} + p_0 q_h + q_{h-2}}{-q_{h-1}} \right\} \\
&= \min \left\{ \frac{|t + p_0 q_h + q_{h-2}|}{|q_{h-1}|} \;: t \in \mathbb{D}_{d,p_0} \right\} \\
&\geq \min \left\{ \frac{|p_0||q_h| - |q_{h-2}| - |t|}{|q_{h-1}|} \;:\; t \in \mathbb{D}_{d,p_0} \right\} \\
&> \frac{|p_0||q_h| - |q_{h-2}| - |p_0|}{|q_{h-1}|} \\
&\geq \frac{|p_0||q_h| - |q_h| - |p_0|}{|q_h|} \\
&= \left(1 - \frac{1}{|q_h|}\right) |p_0| - 1.
\end{aligned}$$

This value increases, if $|q_h|$ increases. If the period does not contain 0 and contains at least one element with absolute value greater than one then the smallest value of $|q_h|$ is $\sqrt{2}$, which implies

$$|p_1| > \left(1 - \frac{1}{\sqrt{2}}\right) |p_0| - 1.$$

If the period contains a 0 multiplier, the above inequality holds, except when $q_{h-1} = 0$. In such a case we have

$$q_h = \left\lfloor \frac{-q_{h-2}}{p_0} \right\rfloor,$$

thus $|q_h||p_0| = |-q_{h-2} - r| < |q_{h-2}| + |p_0|$. As $|q_{h-2}| \leq |q_h|$ we get

$$\frac{|q_h|}{|q_h| - 1} > |p_0|.$$

The expression $\frac{|q_h|}{|q_h|-1}$ decreases if $|q_h|$ increases. The lowest possible value of it is $|q_h| = \sqrt{2}$, whence

$$\sqrt{12} > \frac{\sqrt{2}}{\sqrt{2} - 1} > |p_0|.$$

If $|p_0| < \sqrt{12}$, then the disc $|p_1| \leq \left(1 - \frac{1}{\sqrt{2}}\right) |p_0| - 1 \leq \left(1 - \frac{1}{\sqrt{2}}\right) \sqrt{11} - 1 \approx -0.02858$ has no element. With our assumption the expression $\frac{|q_h|}{|q_h|-1} > |p_0|$ has no solution, so there is no period with $q_{h-1} = 0$.

So the periods in this region can contain elements only with absolute value 0 or 1.

Let's check the conditions $p_1 \in \frac{\mathbb{D}_{d,p_0} + p_0 q_k + q_i}{-q_j}$ and $q_k = \left\lfloor \frac{-q_i}{p_0} \right\rfloor$ $(q_j = 0)$ again.

If $|q_j| = 1$, then $q_k \in \{0, -1\}$, because in every other cases the minimum absolute value of p_1 will be outside the examined region:
(If $|q_k| = 1$, but $q_k \neq -1$)
From Theorem 3.10 elements of the set $\mathbb{D}_{d,p_0} + p_0 q_k$ have absolute value greater than $\frac{l}{2}$, and in every Euclidean domain $\frac{l}{2} \geq \left(1 - \frac{1}{\sqrt{2}}\right) |p_0|$.

$$\min |p_1| = \min \left\{ |t| \ : \ t \in \bigcap \frac{\mathbb{D}_{d,p_0} + p_0 q_n + q_l}{-q_m} \right\} \geq$$

$$\geq \min \left\{ |t| \ : \ t \in \frac{\mathbb{D}_{d,p_0} + p_0 q_k + q_i}{-q_j} \right\} = \min \left\{ \left| \frac{t + p_0 q_k + q_i}{-q_j} \right| \ : \ t \in \mathbb{D}_{d,p_0} \right\} \geq$$

$$\geq \min \left\{ |t + p_0 q_k| - |q_i| \ : \ t \in \mathbb{D}_{d,p_0} \right\} \geq \min \left\{ |t + p_0 q_k| - 1 \ : \ t \in \mathbb{D}_{d,p_0} \right\} \geq$$

$$\geq \left(1 - \frac{1}{\sqrt{2}}\right) |p_0| - 1.$$

If $|q_j| = 0$, then $q_k = -1$, because $q_k = \left\lfloor \frac{-q_i}{p_0} \right\rfloor$, q_i is a unit or zero, so in every Euclidean domain, for every canonical digit set $\left\lfloor \frac{-q_i}{p_0} \right\rfloor \in \{-1, 0\}$ (Theorem 3.10), but zero is not possible, because then two 0-s are there next to each other, which means $p_0 q_k \in \mathbb{D}_{d,p_0}$ and this is impossible.

If three equal values are next to each other in a cycle, then the whole period is constructed, because every multiplier is uniquely determined by the previous two values. So the periods with multipliers $(-1), (0, -1), (0, -1, -1)$ are the only possible periods in the examined region, these will be the witnesses for the ECNS property. □

7. Infinite sequences of CNS polynomials

Polynomials with rational integer coefficients can be considered also elements of $\mathbb{E}_d[x]$. In this section we prove a necessary and sufficient condition under which such a polynomial is ECNS. The second aim is to prove a simple sufficient condition in terms of the coefficient. The later result implies that there exist for any degree infinitely many ECNS polynomials.

To formulate our results we need some preparation. Let $P(x) \in \mathbb{Z}[x]$ with $P(0) = p_0$ and $I = \left[-\left\lfloor \frac{|p_0|-1}{2} \right\rfloor, |p_0| - 1 - \left\lfloor \frac{|p_0|-1}{2} \right\rfloor \right] \cap \mathbb{Z}$. Akiyama and Scheicher [3] called $P(x)$ symmetric-CNS if for any $A(x) \in \mathbb{Z}[x]$ there exists $a(x) \in I[x]$ such that $A(x) \equiv a(x) \pmod{P}$.

Theorem 7.1. *Let $P(x) \in \mathbb{Z}[x]$ with $p_0 > 0$. If $P(x)$ is a CNS and symmetric-CNS in $\mathbb{Z}[x]$ then it is ECNS in $\mathbb{E}_d[x]$. The conversion is true if $d = 1, 2$.*

Proof. Assume first that $P(x)$ is a CNS and symmetric-CNS in $\mathbb{Z}[x]$. Let $A(x) \in \mathbb{E}_d[x]$. There exist $A_1(x), A_2(x) \in \mathbb{Z}[x]$ such that $A(x) = A_1(x) + \omega A_2(x)$. As $P(x)$ is a symmetric-CNS there exist $a_2(x) \in I[x], q_2(x) \in \mathbb{Z}[x]$ such that $A_2(x) = a_2(x) + q_2(x)P(x)$. Let

$$a_2(x) = \sum_{j=0}^{m_2} a_{2j}x^j.$$

Assume that the first $j \geq -1$ coefficients of $A_1(x) + \omega a_2(x)$ belong to $\mathbb{D}_{d,p_0}$. This is obviously true for $j = -1$ because the coefficient of our polynomial with index -1 is zero, which belongs to $\mathbb{D}_{d,p_0}$. Let its $j+1$-th coefficient be $\beta = A_{1,j+1} + \omega a_{2,j+1}$. There exists by Theorem 3.1 a $\beta_1 \in \mathbb{D}_{d,p_0}$ such that $\beta_1 \equiv \beta \pmod{p_0}$. We have $\beta_1 - \beta \in \mathbb{Z}$ because $a_{2,j+1} \in I$ and $p_0 \in \mathbb{Z}$. Thus $(\beta_1 - \beta)/p_0 \in \mathbb{Z}$. Denote it by q and set $A(x) \leftarrow A(x) + qP(x)x^{j+1}$. This transformation does not affect $a_2(x)$, but the first $j+1$ coefficients of $A(x)$ belong to $\mathbb{D}_{d,p_0}$.

Performing the transformation of the last paragraph $m_2 + 1$-times we obtain a polynomial $a_1^{(1)}(x) + a_1^{(2)}(x)x^{m_2+1} + \omega a_2(x) \equiv A(x) \pmod{P(x)}$ such that $a_1^{(1)}(x) + \omega a_2(x) \in \mathbb{D}_{d,p_0}[x]$ and $a_1^{(2)}(x) \in \mathbb{Z}[x]$. As $P(x)$ is a CNS polynomial in $\mathbb{Z}[x]$ there exists $a_1^{(3)}(x)$ with coefficients in $\{0, 1, \dots, p_0 - 1\}$, which is a subset of $\mathbb{D}_{d,p_0}$, such that $a_1^{(2)}(x) \equiv a_1^{(3)}(x) \pmod{P(x)}$. Setting $a_1(x) = a_1^{(1)}(x) + a_1^{(3)}(x)x^{m_2+1}$ and $a(x) = a_1(x) + \omega a_2(x)$ we have that $A(x) \equiv a(x) \pmod{P(x)}$ and the coefficients of $a(x)$ belong to $\mathbb{D}_{d,p_0}$. Thus the conditions are sufficient.

Assume that $P(x)$ is ECNS in $\mathbb{E}_d[x]$. Then for any $A(x) \in \mathbb{E}_d[x]$ there exists $a(x) \in \mathbb{D}_{d,p_0}[x]$ such that $A(x) \equiv a(x) \pmod{P(x)}$. Write $a(x) = a_1(x) + \omega a_2(x)$. Then the coefficients of a_2 belong obviously to I. If $d = 1, 2$ then the coefficients of $a(x)$ have the form $e_1 + e_2\sqrt{-d}$, which absolute value is $\sqrt{e_1^2 + de_2^2} < p_0$. Thus $|e_1| < p_0$ and $e_1 \geq 0$ because $|(e_1 + p_0) + e_2\sqrt{-d}| > p_0$. □

To characterize the CNS polynomials in $\mathbb{Z}[x]$ is a hard problem, see Akiyama et al. [1]. However there is a simple sufficient criterion proved by Béla Kovács [10], which we cite now.

Theorem 7.2. *Let $P(x) = p_0 + p_1x + \cdots + p_{n-1}x^{n-1} + x^n \in \mathbb{Z}[x]$. If $p_0 \geq 2$ and $p_i > p_{i+1}, i = 0, \dots, n-1$, then $P(x)$ is a CNS polynomial.*

By our best knowledge similar simple condition is not available for symmetric-CNS. We cannot expect such a nice sufficient condition. Indeed the polynomials $x^2 + ax + a, 3 \leq a \in \mathbb{Z}$ are by Theorem 7.2 CNS, but they are not symmetric-CNS. In the next lemma we prove a condition, which depends only on the coefficients of $P(x)$. In its proof we borrowed ideas from [2]. In the sequel set $M = \left\lfloor \frac{p_0-1}{2} \right\rfloor$ and $I = \left[-\left\lfloor \frac{p_0-1}{2} \right\rfloor, p_0 - 1 - \left\lfloor \frac{p_0-1}{2} \right\rfloor \right] \cap \mathbb{Z}$.

Lemma 7.3. *Let $P(x) = p_0 + p_1 x + \cdots + p_{n-1}x^{n-1} + p_n x^n \in \mathbb{Z}[x]$ be a polynomial such that $M \geq p_1 \geq p_2 \geq \cdots \geq p_n = 1$ and*

$$\sum_{j=2}^{n} p_j \leq M.$$

Then $P(x)$ is a symmetric-CNS.

Proof. By Theorem 7.2 we may assume that $a_j \in [0, p_0 - 1], j = 0, \ldots, k$. Let $J = [-p_0, p_0 + M - 1] \cap \mathbb{Z}$. For polynomials $a(x) \in \mathbb{Z}[x]$ with constant term a_0 define the mapping $U(a) = U_P(a) \; : \; \mathbb{Z}[x] \mapsto \mathbb{Z}[x]$ as

$$U(a) = \frac{a - \varepsilon P - (a_0 - \varepsilon p_0)}{x},$$

where ε denotes the unique integer with

$$\varepsilon p_0 \leq a_0 + M < (\varepsilon + 1)p_0.$$

Notice that if the coefficients of a belong to J then

$$a = r + xU(a) + \varepsilon P, \tag{7.1}$$

where $r = a_0 - \varepsilon p_0$ and $\varepsilon \in \{0, \pm 1\}$ is the coefficient of P in the definition of $U(a)$. Further it is clear that if $a_0 \in J$ then $r \in I$. Thus the lemma will be proved when we are able to show that for all $a \in J[x]$ there exists $m > 0$ such that $U^m(a) \equiv 0 \pmod{P}$.

We claim that if the coefficients of $a(x) \in \mathbb{Z}[x]$ belong to $[0, p_0 - 1]$ then $U^\ell(a) \in J[x]$ hold for $\ell \geq 0$. To prove the claim we have to examine the coefficients of $U^\ell(a)$ carefully.

Let $U^\ell(a) = \sum_{j=0}^{\infty} a_j^{(\ell)} x^\ell$. (Of course the number of non-zero coefficients of $U^\ell(a)$ is finite, thus there exists $j_0 = j_0()\ell$ such that $a_j^{(\ell)} = 0$ for all $j > j_0$. We use the same convention for $U^0(a) = a$ and for P too, i.e. we set $p_j = 0$ for $j > n$. Then we have

$$a_j^{(\ell)} = a_{\ell+j} - \sum_{h=1}^{\ell} \varepsilon^{(h)} p_{\ell+j-h+1}, \; j, \ell \geq 0, \tag{7.2}$$

where $\varepsilon^{(s)} = 0$, if $s < 0$ and for $s \geq 0$ it is defined by the equation

$$U^{(s-1)}(a) = r_s + xU^{(s)} + \varepsilon^{(s)} P,$$

with $r_s \in I$.

Equation (7.2) is obviously true for $\ell = 0$. Assume that it is true for all $s \le \ell$. Set $\varepsilon^{(\ell+1)}$ according to the size of $a_0^{(\ell)}$. Then we have

$$\begin{aligned} U^{(\ell+1)}(a) &= \frac{U^{(\ell)}(a) - a_0^{(\ell)} - \varepsilon^{(\ell+1)}(P - p_0)}{x} \\ &= \sum_{j=1}^{\infty} a_j^{(\ell)} x^{j-1} - \varepsilon^{(\ell+1)} \sum_{j=1}^{\infty} p_j x^{j-1} \\ &= \sum_{j=0}^{\infty} (a_{j+1}^{(\ell)} - \varepsilon^{(\ell+1)} p_{j+1}) x^j. \end{aligned}$$

Comparing coefficients and using (7.2) we obtain

$$\begin{aligned} a_j^{(\ell+1)} &= a_{\ell+j+1} - \sum_{h=1}^{\ell} \varepsilon^{(h)} p_{\ell+j+2-h} - \varepsilon^{(\ell+1)} p_{j+1} \\ &= a_{j+\ell+1} - \sum_{h=1}^{\ell+1} \varepsilon^{(h)} p_{\ell+j+2-h}, \end{aligned}$$

which is (7.2) for $\ell + 1$, i.e. (7.2) is true for all $\ell, j \ge 0$.

Now we are in the position to prove the claim. Assume that the coefficients of $a(x) \in \mathbb{Z}[x]$ belong to $[0, p_0 - 1]$, i.e. $0 \le a_j = a_j^{(0)} < p_0$. Thus the claim is true for $\ell = 0$ and $\varepsilon^{(1)} \in \{0, \pm 1\}$. Let $\ell \ge 1$ and assume that the claim and $\varepsilon^{(j)} \in \{0, \pm 1\}$ hold for $1 \le j < \ell$. Then

$$\varepsilon^{(\ell)} = \left\lfloor \frac{a_0^{(\ell-1)} - p_0/2}{p_0} \right\rfloor,$$

which belongs to he set $\{0, \pm 1\}$ because by the induction hypothesis $-p_0 \le a_0^{(\ell-1)} \le p_0 + M - 1$. By (7.2) we have

$$a_j^{(\ell)} = a_{\ell+j} - \sum_{h=1}^{\ell} \varepsilon^{(h)} p_{\ell+j-h+1}.$$

Plainly the sum of the right hand side is at least

$$0 - \sum_{h=1}^{n} p_h = -(p_1 + \sum_{h=2}^{n} p_h) \ge -2M > -p_0.$$

To finish the induction we have to prove the upper bound for $a_j^{(\ell)}$. Assume that $\varepsilon^{(m)} = -1$ for some $m \le \ell$. Then $a_0^{(m-1)} < M$. We have

$$\begin{aligned} a_0^{(m-1)} &= a_{m-1} - \sum_{h=1}^{m-1} \varepsilon^{(h)} p_{m-h} \\ &\ge 0 - \varepsilon^{(m-1)} p_1 - \sum_{h=2}^{n} p_h \\ &\ge -\varepsilon^{(m-1)} p_1 - M. \end{aligned}$$

Thus $a_0^{(m-1)} < -M$ can hold only if $\varepsilon^{(m-1)} = 1$. Applying again (7.2) and using the induction hypothesis and this observation we get

$$a_j^{(\ell)} \leq p_0 - 1 + \sum_{h=1}^{n} (-1)^{h+1} p_h = p_0 - 1 + p_1 - (p_2 - p_3) - \cdots \leq p_0 + M - 1. \tag{7.3}$$

Here we used the monotonicity of the coefficients as well. The claim is proved completely.

If $U^{(k+1)}(a) = 0$ then the Lemma is proved. Assume in the sequel $U^{(k+1)}(a) \neq 0$. Then the inequality in (7.3) can be considerably improved. Indeed as $a_\ell = 0, \ell > k$ we get

$$a_j^{(\ell)} \leq M$$

for all $j \geq 0$. The degree of the polynomial $U^{(k+1)}(a)$ is at most n and its coefficients belong to $[-2M, M]$. Thus $U^{n+k+2}(a) \in I[x]$ and the lemma is proved. □

Theorem 7.4. *Let $P(x) := \sum_{i=0}^{n} p_i x^i \in \mathbb{Z}[x]$ be a monic polynomial of degree n. Put $M = \left\lfloor \frac{p_0 - 1}{2} \right\rfloor$ and assume $p_0 \geq M \geq p_1 \geq p_2 \geq \cdots \geq p_n = 1$ and*

$$\sum_{j=2}^{n} p_j \leq M.$$

Then $P(x)$ is a ECNS polynomial with the digit set $\mathbb{D}_{d,p_0}$.

Proof. By Lemma 7.3, starting from a general polynomial one can determine a polynomial which is equivalent to the original modulo $P(x)$, and the imaginary part of the coefficients of the new polynomial belong to the interval $\left]-\left\lfloor \frac{p_0-1}{2} \right\rfloor, p_0 - 1 - \left\lfloor \frac{p_0-1}{2} \right\rfloor\right]$ (coefficients on the real band property).

For the real part an iteration can be started using the following transformation. In every step the investigated polynomial $A(x)$ will be changed, such that

$$A := T_P(A) := \frac{A - q \cdot P - r}{x},$$

where $q := \left\lfloor \frac{a_0}{p_0} \right\rfloor$. It is easy to see that $q \in \mathbb{Z}$, because of the coefficients on the real band property, this means that if one wants to move a coefficient to the digit set an integer times p_0 has to be added. After some iteration of this transformation all of the original coefficients of the polynomial $A(x)$ will be moved into the digit set, in every step the newly created coefficients are rational integers. So after finitely many steps $A(x)$ becomes a polynomial with rational integer coefficients. Polynomial $P(x)$ satisfies the assumptions of Theorem 7.2, thus it is CNS. From this point on we can use Theorem 7.2 to get an $A(x) \in \mathbb{D}_{d,p_0}[x]$ because the integer canonical digit set of the integer CNS polynomial $P(x)$ is a subset of $\mathbb{D}_{d,p_0}$ (Remark 3.3).

□

8. Conclusion and further work

In this paper CNS polynomials have been defined over imaginary quadratic Euclidean domains (Definition 4.1). Proved that for linear polynomials it is easy to decide whether it is a CNS or not (Theorem 5.5). For quadratic polynomials a set of CNS polynomials has been found where the linear term's absolute value is small (Theorem 6.4). Infinite sequences of CNS polynomials over imaginary quadratic Euclidean domains has been found (Theorem 7.4). This can be continued to investigate polynomials and vectors with greater degree, or other Euclidean domains can be investigated as well.

Acknowledgements. This research was partly supported by the OTKA grants NK104208, NK101680.

The authors are very much grateful to the referee for the careful reading and for the many helpful suggestions, which helped to improve the quality of the presentation considerably.

References

[1] Sh. Akiyama, T. Borbély, H. Brunotte, A. Pethő and J. M. Thuswaldner, *Generalized radix representations and dynamical systems I.*, Acta Math. Hungar., **108** (2005), 207–238.

[2] Sh. Akiyama and A. Pethő, *On canonical number systems*, Theor. Comp. Sci., **270** (2002), 921–933.

[3] Sh. Akiyama and K. Scheicher, *Symmetric shift radix systems and finite expansions*, Math. Pannon. **18** (2007), 101–124.

[4] H. Brunotte, P. Kirschenhofer and J. M. Thuswaldner, *Shift radix systems for Gaussian integers and Pethő's loudspeaker*, Publ. Math. Debrecen, **79** (2011), 341–356.

[5] G. Barat, V. Berthé, P. Liardet and J. Thuswaldner, *Dynamical directions in numeration*, Ann. Inst. Fourier (Grenoble) **56** (2006), no. 7, 1987–2092.

[6] H. Davenport, *Indefinite binary quadratic forms and Euclid's algorithm in real quadratic fields*, Proc. London Math. Soc. **53**, 75–82 (1951).

[7] L.E. Dickson, *Algebren und ihre Zahlentheorie*, Zürich und Leipzig, 1927, S. 150f.

[8] Hua Loo Keng, *Introduction to number theory*, Springer Verlag Berlin Heidelberg New York, 1982.

[9] M.-A. Jacob and J.-P. Reveilles, *Gaussian numeration systems*, Actes du colloque de Géométrie Discrète DGCI, (1995).

[10] B. Kovács, *Canonical number systems in algebraic number fields*, Acta Math. Acad. Sci. Hungar., **37** (1981), 405–407.

[11] Lehmer D.H., *A machine method for solving polynomial equations*, Journal of the ACM, **2** (1961), 151–162.

[12] O. Perron, *Quadratische Zahlkörper mit Euklidischem Algorithmus*, Math. Annalen, **107** (1933) 489–495.

[13] A. Pethő, *On a polynomial transformation and its application to the construction of a public key cryptosystem*, Computational number theory (Debrecen, 1989), de Gruyter, Berlin, 1991, pp. 31–43.

[14] K. Scheicher, P. Surer, J.M. Thuswaldner and C.E. van de Woestijne, *Digit systems over commutative rings*, Int. J. Number Theory, **10** (2014) 1459 - 1483.

(Attila Pethő)
Department of Computer Science, University of Debrecen,
H-4010 Debrecen, P.O. Box 12, HUNGARY, and
University of Ostrava, Faculty of Science,
Dvořákova 7, 70103 Ostrava, Czech Republik
E-mail address: petho.attila@inf.unideb.hu

(Péter Varga)
H–1052 Budapest,
Semmelweis utca 23. 3/23., HUNGARY
E-mail address: vapeti@gmail.com