On canonical expansions of integers in imaginary quadratic fields

Attila Kovács

Abstract

In [6] a complete description was given for the location, number and structural properties of attractors generated by the discrete dynamic of the system $(\theta, \mathcal{A})$, where θ is an arbitrary Gaussian integer with norm N greater than one and canonical digit set $\mathcal{A} = \{0, 1, \ldots, N-1\}$. In this paper we shall extend this result to the integers in imaginary quadratic fields. On the other hand it is also an extension of the result of Kátai, B. Kovács ([4]) and of Gilbert ([1]).
AMS classif.:11A63, 11Y55

1 Introduction

Let $\mathbb{Q}$ be the field of rational numbers, $\mathbb{Q}(\vartheta)$ its extension generated by ϑ. Let $\mathbb{Q}[\vartheta]$ denote the integers of $\mathbb{Q}(\vartheta)$. Let $\theta \in \mathbb{Q}[\vartheta]$ be an algebraic integer for which θ and all its conjugates have moduli greater than one. Let $N = \mid \mathrm{Norm}(\theta) \mid \geq 2$ and let $\mathcal{A}$ be a complete residue system modulo θ. The pair $(\theta, \mathcal{A})$, $\mathcal{A} = \{0, a_1, \ldots, a_{N-1}\}$ is called a number system in $\mathbb{Q}[\vartheta]$ if for each $\gamma \in \mathbb{Q}[\vartheta]$ there exist an $m \in \mathbb{N}_0$ and $a_j \in \mathcal{A}$ $(j = 0, 1, \ldots, m)$ such that

$$\gamma = a_0 + a_1\theta + \ldots + a_m\theta^m.$$

The uniqueness of the expansion follows from the assumption that any two elements of $\mathcal{A}$ are incongruent modulo θ. The problem of characterizing number systems in various rings in general seems to be hard. In this note we shall always consider the canonical digit set $\mathcal{A} = \{0, 1, \ldots, N-1\}$ as it appears to be the obvious generalization of the traditional number systems. In this case all those integers θ in quadratic number fields can be given for which $(\theta, \mathcal{A})$ are number systems.

Theorem 1.1 (Kátai and B. Kovács [3, 4], Gilbert [1]): Let θ be a quadratic integer with minimal polynomial $x^2 + Ex + F$ and $\mathcal{A} = \{0, 1, \dots, \mid F \mid -1\}$. Then $(\theta, \mathcal{A})$ is a number system if and only if $F \geq 2$ and $-1 \leq E \leq F$.

The system $(\theta, \mathcal{A})$ can be used to represent all the integers $\gamma \in \mathbb{Q}[\vartheta]$ even if it is not a number system. Clearly, for each γ there exist a unique $a_j \in \mathcal{A}$ such that $\theta \mid \gamma - a_j$. Let $\gamma_1 = \frac{\gamma - a_j}{\theta}$ and let us define the function $\Phi : \mathbb{Q}[\vartheta] \to \mathbb{Q}[\vartheta]$ by $\Phi(\gamma) = \gamma_1$. Let Φ^l denote the l-fold iterate of Φ, $\Phi^0(\gamma) = \gamma_0$. The sequence of integer vectors $\Phi^j(\gamma_0) = \gamma_j$ $(j = 1, 2, \dots)$ is called the path of the dynamical system generated by Φ. The concept of this kind of dynamic in algebraic number fields can be extended to the lattices of the k-dimensional Euclidean space. It was examined from algorithmical point of view in [5].

In the following we restrict our attention to the ring of integers in imaginary quadratic fields.

Let $D \geq 2$ be a square-free integer. Let $\mathbb{Q}(i\sqrt{D})$ be an imaginary quadratic extension of $\mathbb{Q}$, I be the set of integers in $\mathbb{Q}(i\sqrt{D})$. It is known, that if $D \not\equiv 3 \pmod 4$ then $\{1, \delta\}$, while for $D \equiv 3 \pmod 4$ $\{1, \omega\}$ is an integer basis in I, where $\delta = i\sqrt{D}$, $\omega = \frac{1+i\sqrt{D}}{2}$. The lattice generated by the basis $\{1, \delta\}$ will be called δ-lattice and the other one is ω-lattice.

A set of vectors $\mathcal{V}_{M,j} \subset \mathbb{Z}^k$ is called j-canonical with respect to the integer matrix M $(1 \leq j \leq k)$ if all of its elements have the form $\nu \underline{e}_j$, where $\underline{e}_j$ denotes the j-th unit vector, $\nu = 0, 1, \dots, t-1$ and $t = \mid \det(M) \mid$. In [5] the following theorem was proved.

Theorem 1.2 Let M be an invertible expanding linear operator of $\mathbb{R}^k$ mapping $\mathbb{Z}^k$ into itself and let $\underline{c} = [c_1, c_2, \dots, c_k]^T \in \mathbb{Z}^k$ be the j-th column of the adjoint of M. (Here adjoint means the integer matrix, for which the elements are the adjoints of the appropriate subdeterminants.) Let $\kappa_l = (c_l, t)$ $(l = 1, \dots, k)$. Let furthermore $\tau_l = t/\kappa_l$. Then the set $\mathcal{V}_{M,j}$ forms a complete residue system (CRS) modulo M if and only if $\operatorname{lcm}(\tau_1, \dots, \tau_k) = t$.

Let $\alpha_1 = a + b\delta$ and $\alpha_2 = a + b\omega$, $a, b \in \mathbb{Z}$, $b \neq 0$, $E = \frac{D+1}{4}$. In these cases the corresponding linear operators in $\mathbb{Z}^2$ are

$$M_1 = \begin{bmatrix} a & -Db \\ b & a \end{bmatrix} \text{ and } M_2 = \begin{bmatrix} a & -Eb \\ b & a+b \end{bmatrix}.$$

Clearly, $\det(M_1) = a^2 + Db^2$ and $\det(M_2) = a^2 + ab + Eb^2$; the first column of the adjoint of the matrices M_1 and M_2 are $[a, -b]^T$ and $[a + b, -b]^T$, accordingly. Suppose that $(a, b) > 1$. Theorem 1.2 immediately shows that in these cases the sets $\{0,1,\ldots,a^2+Db^2-1\}$ and $\{0,1,\ldots,a^2+ab+Eb^2-1\}$ can not be complete residue systems modulo M_1 and M_2, accordingly. Hence the following lemma holds.

Lemma 1 For a given $\alpha \in \mathbb{Q}[i\sqrt{D}]$ ($\alpha = a + b\delta$ or $\alpha = a + b\omega$) there exist a canonical digit set $\mathcal{A} = \{0,1,\ldots,\mathrm{Norm}(\alpha)-1\}$ if and only if $(a,b) = 1$.

Throughout this article we shall always assume that $(a,b) = 1$. Let α $(= \alpha_1$ or $\alpha_2) \in I, (a,b) = 1, N = \mathrm{Norm}(\alpha), L = \frac{N-1}{|\alpha|-1} = |\alpha| + 1$. Then $\mathcal{A} = \{0,1,\ldots,N-1\}$ is a complete residue system modulo α. Obviously, if $\mid \gamma \mid \leq L$ then $\mid \Phi(\gamma) \mid \leq \frac{L+N-1}{|\alpha|} = L$, if $\mid \gamma \mid > L$ then $\mid \Phi(\gamma) \mid \leq \frac{|\gamma|+N-1}{|\alpha|} < \mid \gamma \mid$ for every $\gamma \in I$. Since the inequality $\mid \kappa \mid \leq L$ holds only for finitely many integers $\kappa \in I$, therefore the path $\gamma, \Phi(\gamma), \Phi^2(\gamma), \ldots$ is ultimately periodic for all $\gamma \in I$. An element $\pi \in I$ is called periodic if there exist a $j \in \mathbb{N}$ such that $\Phi^j(\pi) = \pi$. The smallest such j is the length of the period of π generated by Φ. Let $\mathcal{P}$ denote the set of all periodic elements. The basin of attraction of $\pi \in \mathcal{P}$ consists of all $\gamma \in I$ for which there exists a $j \in \mathbb{N}_0$ such that $\Phi^j(\gamma) = \pi$ and is denoted by $\mathcal{B}(\pi)$. It is also clear that $\pi \in \mathcal{P}$ if and only if there is an $l > 0$ such that

$$\pi = a_0 + a_1\alpha + \ldots + a_{l-1}\alpha^{l-1} + \pi\alpha^l, \quad a_j \in \mathcal{A}, \tag{1}$$

Let $\mathcal{G}(\mathcal{P})$ be the directed graph defined on $\mathcal{P}$ by drawing an edge from $\pi \in \mathcal{P}$ to $\Phi(\pi)$. Then $\mathcal{G}(\mathcal{P})$ is a disjoint union of directed cycles, where loops are allowed. $\mathcal{G}(\mathcal{P})$ is also called the attractor of I generated by Φ. In this paper we give a complete description of the location, number and structural properties of the attractors generated by the discrete dynamic of the system $(\alpha, \mathcal{A})$, where $\alpha \in I$.

2 Periodic elements of period length one

Consider the δ-lattice and let $\alpha = a + b\delta,\ a, b \neq 0,\ (a,b) = 1$.

Lemma 2.1 The loops in the system $(\alpha, \mathcal{A})$ are $\pi_j = \frac{1-a+b\delta}{(1-a,b)}j,\ j = 0,\ldots,k$, where $k = \lfloor (1-a,b)(1 + 2\frac{a-1}{(1-a)^2+b^2D}) \rfloor$.
Proof: It follows from (1) that $\pi \in \mathcal{P}$ is a loop if and only if $\pi = d + \alpha\pi$ for some $d \in \mathcal{A}$. It means that $(1-\alpha)\pi = d \in \mathcal{A}$, hence $\pi = \frac{d}{1-\alpha} = \frac{d(1-a)}{(1-a)^2+b^2D} + \delta\frac{db}{(1-a)^2+b^2D}$. Since $\pi \in I$ therefore $(1-a)^2 + b^2D \mid d(1-a,b)$. On the other hand $0 \leq d \leq a^2 + b^2D - 1$ by which the proof is completed.$\square$

Consider now the ω-lattice. Let $\alpha = a + b\omega,\ b \neq 0,\ (a,b) = 1,\ N = \mathrm{Norm}(\alpha) = a^2 + ab + b^2E,\ E = \frac{D+1}{4}$. If $E = 1$, $a = 0, b = \pm 1$ or $E = 1, a = -b = \pm 1$ then $\mid \alpha \mid= 1$, so in the following we always excude these cases. Using the same idea as before the next lemma can be easily proved. We leave it to the reader.

Lemma 2.2 The loops in the system $(\alpha, \mathcal{A})$ are $\pi_j = \frac{1-a-b+b\omega}{(1-a-b,b)} j,\ j = 0, \ldots, k$, where $k = \lfloor (1-a-b,b)(1 + \frac{2a+b-2}{(1-a)^2-(1-a)b+b^2E}) \rfloor$. □

Remarks

(1) Let $b > 0$ be fixed. From these lemmas we can calculate the maximal number of loops. In the δ-lattice this can be achieved by $b \mid a-1,\ a \geq 1$, in which case it is $b+1$. In the ω-lattice we have two cases depending on the value of E. If $E \geq 2$ then the maximal number of loops is $b+1$ by $b \mid a-1, 2a+b \geq 2$. If $E = 1$ then this value is $b+2$, by $a = 1$ or by $b \geq 1, a = b+1$.

(2) If a is positive then the element $1 - a + b\delta \in \mathcal{P}$ of period length one. In the ω-lattice, if $2a+b \geq 2$ then the element $1-a-b+b\omega \in \mathcal{P}$ of period length one. Moreover, if $E = 1, \#\mathcal{P} = b+2$ then $(1-a-b)(b+1)/b + (b+1)\omega \in \mathcal{P}$ of period length one.

3 Location of periodic elements

Before we continue our analysis, we have some useful observations.

(1) Let $\gamma \in I,\ \gamma \equiv 0 \bmod \alpha, \gamma_1 = \gamma + x,\ \gamma_2 = \gamma + y,\ x, y \in \mathcal{A}$. Then

$$\Phi(\gamma_1) = \Phi(\gamma_2). \tag{2}$$

(2) Let $\alpha \in I, \pi \in \mathcal{P}$, that is, $\pi = a_0 + a_1\alpha + \ldots + a_{l-1}\alpha^{l-1} + \pi\alpha^l,\ a_j \in \mathcal{A}$. Then

$$\overline{\pi} = a_0 + a_1\overline{\alpha} + \ldots + a_{l-1}\overline{\alpha}^{l-1} + \overline{\pi}\overline{\alpha}^l, \quad a_j \in \mathcal{A}. \tag{3}$$

It means that if $\pi \in \mathcal{P}$ in $(\alpha, \mathcal{A})$ then $\overline{\pi} \in \mathcal{P}$ in $(\overline{\alpha}, \mathcal{A})$. If $\alpha = a + b\delta$ then $\overline{\alpha} = a - b\delta$, if $\alpha = a + b\omega$ then $\overline{\alpha} = a + b - b\omega$, so it is enough to examine the cases $b \geq 1$.

(3) It is known (see e.g. [5]) that if $\pi \in \mathcal{P}$ then

$$-\pi = \frac{d_1}{\alpha} + \frac{d_2}{\alpha^2} + \frac{d_3}{\alpha^3} + \cdots$$

for some $d_i \in \mathcal{A}$. It means that

$$\Big| -\pi - \frac{d_1}{\alpha}\Big| \le \sum_{i=2}^{\infty} \frac{\mid d_i \mid}{\mid \alpha \mid^i} \le \frac{(N-1)}{\mid \alpha \mid^2} \frac{1}{1-\frac{1}{|\alpha|}} = \frac{\mid \alpha \mid +1}{\mid \alpha \mid} = 1 + \frac{1}{\mid \alpha \mid}.$$

Hence

$$\Big| -\pi - \frac{d_1\overline{\alpha}}{N}\Big| \le 1 + \frac{1}{\mid \alpha \mid}. \tag{4}$$

Statement 1 Let $\alpha \in I$ $(\alpha = a + b\delta$ or $\alpha = a + b\omega)$, $(a, b) = 1$, $e \in \mathbb{Z}$. If $\alpha \mid e$ then $N = \alpha\overline{\alpha} \mid e$.
Proof If $a + b\delta = \alpha \mid e$ then $(a + b\delta)(c + d\delta) = ac - bdD + (ad + bc)\delta = e$ for some $c, d \in \mathbb{Z}$. Since $(a, b) = 1$ therefore $c = ap$ and $d = -bp$ for some $p \in \mathbb{Z}$. Hence $a^2p + b^2Dp = e$, which means that $a^2 + b^2D \mid e$. If $a + b\omega = \alpha \mid e$ then $(a + b\omega)(c + d\omega) = ac - bdE + (ad + bc + bd)\omega = e$ for some $c, d \in \mathbb{Z}$. Again, since $(a, b) = 1$ therefore $c = (a + b)p$ and $d = -bp$ for some $p \in \mathbb{Z}$. It means that $a(a + b)p + Eb^2p = e$, by which the proof is finished. □

3.1 Case $\alpha = a + ib\sqrt{D}$

Let $\pi = U + V\delta \in \mathcal{P}$ and let $\Phi(\pi) = U_1 + V_1\delta$. By the definition of Φ we have the following equations:

$$\begin{aligned} U &= d + aU_1 - bDV_1 & (5)\\ V &= bU_1 + aV_1, & (6) \end{aligned}$$

for some $d \in \mathcal{A}$. On the other hand using (4) we have that

$$\Big|\Big(-U - \frac{d_1a}{N}\Big) + \Big(-V + \frac{d_1b}{N}\Big)\delta\Big| \le 1 + \frac{1}{\mid \alpha \mid}. \tag{7}$$

Theorem 3.1 Let $\alpha = a + b\delta$, $f = -a$, $b \ge 1$, $S_1 = \{U + V\delta,\ -a + 1 \le U \le 0,\ 0 \le V \le b\}$, $S_2 = \{U + V\delta,\ 0 \le U \le f,\ 0 \le V \le b - 1\}$. Let $\pi = U + V\delta \in \mathcal{P}$. If $a \ge 1$ then $\pi \in S_1$, if $-a \ge 1$ then $\pi \in S_2$.
Proof Let $\mid \alpha \mid \ge 2$. Suppose that $\mid U \mid \ge \mid a \mid +2$. Then using (7) we get that

$$\mid a \mid +2 \le \mid U \mid \le \frac{3}{2} + \frac{\mid d_1a \mid}{N} \le \frac{3}{2} + \frac{N-1}{N} \mid a \mid,$$

which is a contradiction. Therefore $| U | \leq | a | +1$. Now suppose that $D \geq 4$ and $| V | \geq | b | +1$. Then

$$b+1 \leq | V | \leq \frac{3}{2 | \delta |} + \frac{| d_1 | b}{N} \leq \frac{3}{2\sqrt{D}} + \frac{N-1}{N} b,$$

which is a contradiction again. Hence, if $D \geq 4$ then $| V | \leq b$. In the same way, if $D = 2$ then it is easy to see that $| V | \leq b+1$. On the other hand it follows from (7) that

$$\left| -U - \frac{d_1 a}{N} \right| \leq \frac{3}{2},$$

therefore if $a > 0$ then $U \leq 1$, if $a < 0$ then $U \geq -1$. It is obvious as well that

$$\left| -V + \frac{d_1 b}{N} \right| \leq \frac{3}{2 | \delta |},$$

hence if $D > 2$ then $V \geq 0$, if $D = 2$ then $V \geq -1$.

Case $a \geq 1$. Let $D = 2$. Consider equation (6) and suppose that $V_1 = b+1$. Then we have that $V = b(a+U_1) + a \leq b+1$, therefore either $U_1 = 0, a = 1$ or $U_1 \leq -a$. In the first case, if $a = 1$ then $b > 1$ and by (5) we get that $U \leq -bD(b+1) + N - 1 = -bD < -2 = -(a+1)$ which is a contradiction. It means that $(b+1)\delta$ can not be periodic. On the other hand, if $U_1 = -a$ then $a \leq b+1$, therefore if $a \geq 3$ then $U \leq -a^2 - bD(b+1) + N - 1 = -bD - 1 \leq (-a+1)D - 1 = -2a + 1 < -(a+1)$ which is not possible as well. If $a = 2$ then $a = b+1$, therefore $b = 1$ and it is easy to check that in this case $\mathcal{G}(\mathcal{P}) = \{-1+\delta \to -1+\delta, 0 \to 0\}$. If $a = 1, b \geq 2$ then $U \leq -2b - 1 \leq -5$ which is a contradiction again. If $U_1 = -a-1$ then $U \leq -a^2 - a - bD(b+1) + N - 1 = -a - bD - 1 < -(a+1)$. We conclude that $-(a+c) + (b+1)\delta$ $(c = 0, 1)$ can not be periodic. Hence if $U + V\delta \in \mathcal{P}$ then $V \leq b$. Suppose now that $D = 2$ and $V_1 = -1$. Then by (6) we get that $-1 \leq V = bU_1 - a$, therefore $U_1 \geq 0$. It is easy to see that in this case $U \geq aU_1 + bD \geq 2$ which is a contradiction. We have that if $U + V\delta \in \mathcal{P}$ then $0 \leq V \leq b$. Let $D \geq 2$ and suppose that $U_1 = 1$. Then by (6) we have that $V = b + aV_1 \leq b$. Hence $V_1 = 0$, but obviously 1 can not be periodic. Suppose that $U_1 = -a-1$. Then (6) shows that $V \leq -b$ which is impossible. If $U_1 = -a$ then we have that $V_1 = b$. Then, it follows from Statement 1, (2) and from Remark 2.2 that if $x \in \mathcal{A}$ then $-x - 1 + \alpha \in \mathcal{B}(1 - \overline{\alpha})$. Finally, since $2a + 1 \leq a^2 + b^2 D$, therefore $-a + b\delta$ can not be periodic.

Case $-a = f \geq 1$. Suppose that $D = 2$ and $V_1 = b + 1$. Then $-1 \leq V = bU_1 - f(b+1) = b(U_1 - f) - f$, therefore $f - 1 \leq b(U_1 - f)$, so $U_1 = f = 1$ or $U_1 \geq f + 1$. In the first case it follows from (5) that $U \leq -1 - bD(b+1) + N - 1 = -bD - 1 < -1$ which is a contradiction. In the second case, if $U_1 = f+1$ then $U \leq -f^2 - f - bD(b+1) + N - 1 = -f - bD - 1 < -1$ which is not possible as well. Hence if $U + V\delta \in \mathcal{P}$ then $V \leq b$. Now suppose that $D = 2$ and $V_1 = -1$. Then by (6) we get that $V = bU_1 + f \leq b$, therefore $U_1 \leq 0$ and if $U_1 = 0$ then $f \leq b$, if $U_1 = -1$ then $f \leq 2b$. Hence, it follows from (5) that $f + 1 \geq U \geq -fU_1 + bD \geq 2f$. Since $(f, b) = 1$ therefore it is a contradiction. It is also clear that $a + x + b\delta \in \mathcal{B}(0)$ $(x \in \mathcal{A})$ and $2f + 2 \leq f^2 + b^2D$, therefore by (2) we have that $V_1 \leq b - 1$. Hence, if $U + V\delta \in \mathcal{P}$ then $0 \leq V \leq b - 1$. If $U_1 = -1$ then $0 \leq V = -b - fV_1$, therefore $V_1 < 0$, which is a contradiction. Suppose that $U_1 = f + 1$. Then using (6) we get that $V = b(f+1) - fV_1 \leq b - 1$, therefore $V_1 > b$, which is a contradiction as well.

If $\mid \alpha \mid < 2$ then keeping in mind Theorem 1.1 we have to check only the case $a = 1, b = 1, D = 2$. It is easy to see that in this case $\mathcal{G}(\mathcal{P}) = \{\delta \to \delta, 0 \to 0\}$. The proof is complete. □

Lemma 3.1 If $a \geq 1$ then $\#\mathcal{P} \leq b + 1$, if $-a \geq 1$ then $\#\mathcal{P} \leq b$.
Proof We have seen that if $a \geq 1$ and $\pi = U + b\delta \in \mathcal{P}$ then $\pi = 1 - \overline{\alpha}$. It is obvious that $d \in \mathcal{B}(0)$ for each $d \in \mathcal{A}$. Now we shall examine the expansion of -1. Clearly, $-1 = -1 + N - \alpha\overline{\alpha}$ and $-\overline{\alpha} = -2a + \alpha$. Since $a \geq 1$ therefore $-2a + \alpha = -2a + N - \alpha\overline{\alpha} + \alpha$. Moreover, $0 < N - 2a < N - 1$ and $1 - \overline{\alpha} \in \mathcal{P}$ therefore $-1 \in \mathcal{B}(1 - \overline{\alpha})$. Hence the only rational integer periodic element is 0. Now, Theorem 3.1 and Statement 1 show that there does not exist any $\rho \in S_1 \cup S_2$, $(\rho \neq 0)$ for which $\rho \equiv 0$ (α). In virtue of (2) and Statement 1 it is easy to see that if $U + V\delta \in \mathcal{P}$ then there is not any $Z, (Z \neq U)$ for which $Z + V\delta \in \mathcal{P}$. The proof is finished. □

3.2 Case $\alpha = a + b\omega$

Let $\pi = U + V\omega \in \mathcal{P}$ and let $\Phi(\pi) = U_1 + V_1\omega$. By the definition of Φ we have the equations

$$U = d + aU_1 - bEV_1 \tag{8}$$
$$V = b(U_1 + V_1) + aV_1, \tag{9}$$

for some $d \in \mathcal{A}$. On the other hand using (4) we have that

$$\Big|\Big(-U-\frac{d_1(a+b)}{N}\Big)+\Big(-V+\frac{d_1 b}{N}\Big)\omega\Big| \leq 1+\frac{1}{\mid \alpha \mid}. \tag{10}$$

Theorem 3.2 Let $\alpha = a+b\omega, f=-a, b\geq 1, T_1=\{U+V\omega,\ -a-b+1\leq U\leq 0,\ 0\leq V\leq b-1\}, T_2=\{U+V\omega, 0\leq U\leq f-b,\ 0\leq V\leq b-1\}$. Let $\pi = U+V\omega \in \mathcal{P}$.
If $E=1, a=1$ then $\pi \in T_1 \cup \{1-\overline{\alpha}, -b-1+(b+1)\omega\}$,
if $E=1, a=b+1$ then $\pi \in T_1 \cup \{1-\overline{\alpha}, -a-b-1+(b+1)\omega\}$,
if $E\geq 2$ or $E=1, a>1$ and $a\neq b+1$ then $\pi \in T_1\cup\{1-\overline{\alpha}\}$,
if $1\leq f<b$ and $2a+b\geq 2$ then $\pi\in T_1\cup\{1-\overline{\alpha}\}$,
if $1\leq f<b$ and $2a+b<2$ then $\pi\in T_1$,
if $f>b$ then $\pi\in T_2$.
Proof Let $\mid \alpha \mid \geq 3$. Suppose that $\mid U\mid\geq\mid a+b\mid +2$. Then using (10) we get that

$$\mid a+b\mid +2 \leq \mid U\mid \leq \frac{4}{3}+\frac{\mid d_1(a+b)\mid}{N}\leq \frac{4}{3}+\frac{N-1}{N}\mid a+b\mid,$$

which is a contradiction. Therefore $\mid U\mid\leq\mid a+b\mid +1$. Suppose that $E\geq 2$ and $\mid V\mid\geq\mid b\mid +1$. Then

$$b+1\leq\mid V\mid\leq\frac{4}{3\mid\omega\mid}+\frac{\mid d_1\mid b}{N}\leq\frac{4}{3\sqrt{E}}+\frac{N-1}{N}b,$$

which is a contradiction again. Hence, if $E\geq 2$ then $\mid V\mid\leq b$. In the same way, if $E=1$ then it is easy to see that $\mid V\mid\leq b+1$. On the other hand it follows from (10) that

$$\Big|-U-\frac{d_1(a+b)}{N}\Big|\leq\frac{4}{3},$$

therefore if $a+b>0$ then $U\leq 1$, if $a+b<0$ then $U\geq -1$. It is obvious as well that

$$\Big|-V+\frac{d_1 b}{N}\Big|\leq\frac{4}{3\mid\omega\mid},$$

hence if $E\geq 2$ then $V\geq 0$, if $E=1$ then $V\geq -1$.

Case $a\geq 1$. Let $E=1$. Consider equation (9) and suppose that $V_1=b+1$. Then we have that $V=b(U_1+a+b+1)+a\leq b+1$. Hence either

$a = 1, U_1 = -b-1$ or $U_1 = -a-b-1, 1 \le a \le b+1$. If $a = 1, U_1 = -b-1$ then by Lemma 2.2 we have that $-b-1+(b+1)\omega \in \mathcal{P}$ of period length one. If $U_1 = -a-b-1$ then by (8),(9) we get that $1 \le V = a \le b+1$ and $U = -a-b-1$. Now, suppose that $U_1 = -a-b-1, V_1 = a$. In virtue of (9) we have that $-1 \le V = -b^2-b+a^2$. It means that $b(b+1) \le a^2+1$, therefore $a = b+1$. Hence, if $a = 1$ then $-b-1+(b+1)\omega \in \mathcal{P}$, if $a \ge 2$ and $a = b+1$ then $-a-b-1+(b+1)\omega \in \mathcal{P}$ of period length one and does not exist any other periodic element $X+Y\omega$ with $Y = b+1$. Let $E = 1$ and $V_1 = -1$. Then by (9) we have that $-1 \le V = b(U_1-1)-a$, therefore $U_1 = 1, a = 1$. Using (8) we get that $U \ge b+1 \ge 2$ which is a contradiction. Let furthermore $E \ge 1$. Since $2a+b \ge 2$ always holds, therefore by Remark 2.2 the element $1-a-b+b\omega \in \mathcal{P}$ of period length one. Clearly, $a^2+ab+b^2E > 2a+b+1$ therefore there is not any other element $X+Y\omega \in \mathcal{P}$ with $Y = b$. Suppose that $U_1 = 1$ Then by (9) we have that $0 \le V = V_1(a+b)+b \le b-1$ which is a contradiction. Suppose that $U_1 = -a-b-c, (c = -1, 0, 1)$ and $0 \le V_1 \le b-1$. Then by (9) we get that $V = b(-a-b-c+V_1)+aV_1 \le b(-a-1-c)+ab-a = -a-b-bc < 0$ which is a contradiction again.

Case $-a = f \ge 1$. Let $E = 1$. Suppose that $V_1 = b+1$. Then by (9) we have that $-1 \le V = b(U_1+b-f+1)-f \le b+1$, therefore either $f = 1, U_1 = -b \le -4, V = -1$ or $U_1 \ge f-b$. In the first case using (8) we get that $U \le b-b(b+1)+N-1 = -b$. Suppose that $U_1 = -b, V_1 = -1, f = 1$. It follows from (9) that $V = -b^2-b+1 < -1$ which is a contradiction. In the second case, by (8) we get that $U \le -fU_1-b(b+1)+N-1 \le -b-1 < -b$ which is a contradiction as well. Hence if $U+V\omega \in \mathcal{P}$ then $V \le b$. Suppose that $V_1 = -1$. Then using (9) we have that $-1 \le V = b(U_1-1)+f \le b$ therefore $U_1 \le 1$. Since $U \ge -fU_1+b$ therefore $U_1 \ge 0$. If $U_1 = 0$ then $b-1 \le f \le 2b$ and by (9) we get that $V = f-b$. Suppose that $U_1 \ge b, V_1 = f-b$. Then by (9) we have that $V = b(U_1+f-b)-f(f-b) = 2fb-f^2+bc \le b$ $(c \ge 0)$. It means that $c = 0$ or 1. Moreover, in both cases the only solution is $2b = f$, which contradicts either to $(f, b) = 1$ or to $\mid \alpha \mid \ge 3$. Suppose that $U_1 = 1, V_1 = -1$. It follows from (8), (9) that $U \ge b-f$ and $V = f \le b$. This can happen iff $b = f+1$. Now, suppose that $U_1 = 1, V_1 = b-1$. Then using (9) we get that $V = b^2-f(b-1) = b+f$, which is not possible. It means that if $U+V\omega \in \mathcal{P}$ then $0 \le V \le b$. Let furthermore $E \ge 1$. Suppose that $V_1 = 0$. Clearly, it is enough to consider the expansion of -1. Since $-1 = -1+N-\alpha\overline{\alpha}$, $-\overline{\alpha} = \alpha-2a-b$ therefore if $2a+b \le 0$ then $-1 \in \mathcal{B}(0)$, if $2a+b > 0$ then $-\overline{\alpha} = \alpha-2a-b+N-\alpha\overline{\alpha}$. Obviously $2a+b \le N-1$

and $1-\overline{\alpha}=\alpha-2a-b+1$ therefore we can conclude that if $2a+b\geq 2$ then $-1\in\mathcal{B}(1-\overline{\alpha})$ else $-1\in\mathcal{B}(0)$. Suppose that $V_1=b$. It follows from (9) that $V=b(U_1+b-f)\leq b$. Clearly, it is enough to consider the case $U_1=f-b+1$. The previous deduction shows that $U_1+V_1\omega\in\mathcal{P}$ iff $2a+b\geq 2$. We can also notice that there is not other periodic element with $V_1=b$.

Subcase $f<b$. Suppose that $U_1=1$. Then by (9) we have that $V=V_1(b-f)+b\leq b$, therefore $V_1=0$ which is a known case. Suppose that $U_1=f-b-c$ $(c=0,1)$. Now $0\leq V=V_1(b-f)+b(f-b-c)\leq b$, therefore $V_1=b, c=0$ which is known as well. It means that if $f<b$ and $U+V\omega\in\mathcal{P}$ then $f-b+1\leq U\leq 0$.

Subcase $b<f$. Suppose that $U_1=-1$. Then using (9) we have that $0\leq V=V_1(b-f)-b\leq b$ therefore $V_1<0$ which is a contradiction. Suppose that $U_1=f-b+1$. Then $0\leq V=V_1(b-f)+b(f-b+1)\leq b$, hence $V_1=b$ which is a known case.

If $\mid\alpha\mid<3$ then by Lemma 1 and by Theorem 1.1 the following cases remain. If $a=2, b=1, E=1$ then $-4+2\omega, -2+\omega, 0\in\mathcal{P}$ of period length one, if $a=2, b=1, E=2$ then $-2+\omega, 0\in\mathcal{P}$ of period length one, if $a=1, b=1, E=1$ then $-2+2\omega, -1+\omega, 0\in\mathcal{P}$ of period length one, if $a=1, b=1, E=2,\ldots,6$ then $-1+\omega, 0\in\mathcal{P}$ of period length one, if $a=1, b=2, E=1$ then $-3+3\omega, -2+2\omega, -1+\omega, 0\in\mathcal{P}$ of period length one, if $a=-1, b=2, E=1,2$ then $\omega, 0\in\mathcal{P}$ of period length one, if $a=-1, b=3, E=1$ then $\mathcal{G}(\mathcal{P})=\{\omega\rightarrow -1+2\omega\rightarrow\omega, 0\rightarrow 0\}$, if $a=-2, b=3, E=1$ then $2\omega, \omega, 0\in\mathcal{P}$ of period length one, if $a=-3, b=2, E=1$ then $1+\omega, 0\in\mathcal{P}$ of period length one. The proof is completed. $\square$

Lemma 3.2 If $E=1, a=1$ or if $E=1, a=b+1$ then $\#\mathcal{P}\leq b+2$, if $E\geq 2$ or $E=1, a>1, a\neq b+1$ or $1\leq f<b$ and $2a+b\geq 2$ then $\#\mathcal{P}\leq b+1$, else $\#\mathcal{P}\leq b$.

Proof Since there does not exist any $\rho\in T_1$ (resp. T_2), $(\rho\neq 0)$ for which $\rho\equiv 0\ (\alpha)$ therefore by Statement 1, (2) and by Theorem 3.2 we have that if $U+V\omega\in\mathcal{P}$ then there is not any $Z, (Z\neq U)$ for which $Z+V\omega\in\mathcal{P}$. $\square$

4 Structure of periodic elements

Let $b\geq 2$ and let $\mathcal{L}_\mu=\{P+Q\delta\in I,\ (b,Q)=\mu\}$. Obviously, $I=\bigcup_{\mu\mid b}\mathcal{L}_\mu$. Now, we shall examine the case $\mu<b$. In virtue of (6) and (9) it is easy to see that if $(V,b)=\mu$ then $(V_1,b)=\mu$. Hence the function Φ maps $\mathcal{L}_\mu$ to $\mathcal{L}_\mu$ for each $\mu\mid b$. Let $b_\mu=b/\mu$.

Theorem 4 There is a finite decomposition of $\mathcal{L}_\mu$ into $\mathcal{L}_\mu^{(j)}$, $(j = 0, \dots, l_\mu - 1)$ for which if $\pi \in \mathcal{L}_\mu^{(j)}$ then $\Phi(\pi) \in \mathcal{L}_\mu^{(j)}$ for every $\pi \in \mathcal{P}$. The length of period of $\pi \in \mathcal{P}$ is $\varphi(b_\mu)/l_\mu$, where φ denotes the Euler totient function.
Proof Let $X = V/\mu$, $X_1 = V_1/\mu$. Then from (6) we have that $X = b_\mu U_1 + aX_1$ and from (9) we get that $X = b_\mu(U_1 + V_1) + aX_1$. Clearly, in both cases $X \equiv aX_1 \pmod{b_\mu}$, $(X, b_\mu) = (X_1, b_\mu) = 1$. Let us denote by $\mathbb{Z}_{b_\mu}^*$ the set of reduced residue classes modulo b_μ, i.e., $\mathbb{Z}_{b_\mu}^* = \{m \pmod{b_\mu},\ (m, b_\mu) = 1\}$. Let T_μ denotes the cyclic subgroup $< a >$ in $\mathbb{Z}_{b_\mu}^*$ and let $t_\mu = \operatorname{ord}(a)$. By Lagrange theorem, $\varphi(b_\mu) = l_\mu t_\mu$, hence the order of the factor group $\mathbb{Z}_{b_\mu}^*/T_\mu$ is l_μ. So we have a decomposition $\mathbb{Z}_{b_\mu}^* = H_0 \cup H_1 \cup \ldots \cup H_{l_\mu - 1}$, where $H_0 = T_\mu$. Let $\mathcal{L}_\mu^{(j)} = \{\gamma = P + Q\delta,\ \gamma \in \mathcal{L}_\mu,\ Q/\mu \pmod{b_\mu} \in H_j\}$. Finally, we have the decomposition by $\mathcal{L}_\mu = \mathcal{L}_\mu^{(0)} \cup \mathcal{L}_\mu^{(1)} \cup \ldots \cup \mathcal{L}_\mu^{(l_\mu - 1)}$. The proof is completed. $\square$

Remark
Consider the graph $\mathcal{G}(\mathcal{P})$. Theorem 4 states that for a fixed a and b $(b \geq 2)$ there are $\tau(b)$ different sets $\mathcal{L}_\mu$, in each there exist $l_\mu = \varphi(b_\mu)/\operatorname{ord}_{b_\mu} a$ cycles with period length $t_\mu = \operatorname{ord}_{b_\mu}$. If b_μ is prime then there is only one cycle in $\mathcal{L}_\mu$ with period length $b_\mu - 1$. If $a \equiv 1 \pmod{b_\mu}$ then there are only loops in $\mathcal{L}_\mu$ and the number of them is $\varphi(b_\mu)$.

5 Number of periodic elements

We have seen in the previous section that for each $\mu \mid b$ and for each $j = 0, 1, \dots, l_\mu - 1$ there exist at least one period-cycle in $\mathcal{L}_\mu^{(j)}$. The length of a period in $\mathcal{L}_\mu^{(j)}$ is a multiple of t_μ, so it is at least t_μ. This means that $\#\mathcal{P} \geq \sum_{\mu|b} t_\mu l_\mu$. Since $t_\mu l_\mu = \varphi(b_\mu)$ therefore $\#\mathcal{P} \geq \sum_{\mu|b} \varphi(b/\mu) = b$. Keeping in mind the theorems and lemmas proved in this paper we have the following result.

Theorem 5 Let $b \geq 1$. Let $\alpha = a + b\delta$. If $a \geq 1$ then $\#\mathcal{P} = b + 1$, if $-a \geq 1$ then $\#\mathcal{P} = b$. Let $\alpha = a + b\omega$. If $E = 1, a = 1$ or if $E = 1, a = b + 1$ then $\#\mathcal{P} = b + 2$, if $E \geq 2$ or $E = 1, a > 1, a \neq b + 1$ or $1 \leq f < b$ and $2a + b \geq 2$ then $\#\mathcal{P} = b + 1$, else $\#\mathcal{P} = b$. If $b \leq -1$ then apply (3).

References

[1] Gilbert, W.J., *Radix representation of quadratic fields*, J. Math. Anal. Appl.

83, 1991. 264–274.

[2] Kátai, I., *Number systems in imaginary quadratic fields*, Annales Univ. Sci. Budapest, Sect. Comp. **14**, 1994. 91–103.

[3] Kátai, I., Kovács B., *Kanonische Zahlensysteme bei reelen quadratischen algebraischen Zahlen*, Acta Sci. Math. **42**, 1980, 99–107.

[4] Kátai, I., Kovács, B., *Canonical number systems in imaginary quadratic fields*, Acta Math. Hung. **37**, 1981. 159–164.

[5] Kovács, A., *On computation of attractors for invertible expanding linear operators in* $\mathbb{Z}^k$, Publ. Math. Debrecen, to appear

[6] Kovács, A., *On expansions of Gaussian integers with non-negative digits*, Mathematica Pannonica, **10 (2)**, 1999. 177–191.

Attila Kovács
Department of Computer Algebra
Eötvös Loránd University, Budapest, Hungary
attila@compalg.inf.elte.hu