Journal of Symbolic Computation 77 (2016) 175–188

Contents lists available at ScienceDirect

Journal of Symbolic Computation

www.elsevier.com/locate/jsc

Shortest division chains in unique factorization domains

Maksim Vaskouski [a], Nikita Kondratyonok [b]

[a] Department of Higher Mathematics, Belarusian State University, Minsk 220030, Belarus
[b] Faculty of Applied Mathematics and Computer Science, Belarusian State University, Minsk 220030, Belarus

ARTICLE INFO

Article history:
Received 6 October 2015
Accepted 30 January 2016
Available online 5 February 2016

Keywords:
Euclidean algorithm
Unique factorization domain
Euclidean domain
Continued fraction

ABSTRACT

We investigate the problem on the validity of the Lazard theorem analogue (or the Kronecker–Vahlen theorem), which states that the least remainder Euclidean Algorithm (EA) has the shortest length over any other versions of EA, in unique factorization domains. There is obtained the existence criterion to represent a fixed element of the fractions field of a unique factorization domain in the form of a continued fraction of a fixed length. This criterion enables to obtain a formula for the length of the least remainder (on norm) EA as a function of elements, with respect to which EA is applied. This result gives us the class $\mathcal{T}$ of unique factorization domains, for which the Lazard theorem analogue is valid. We propose algorithms to check whether the given unique factorization domain belongs to the class $\mathcal{T}$. We find the necessary and sufficient conditions under which the number of steps in the worst case of the least remainder EA grows not faster than logarithm. In particular, these results hold for the least remainder EA in any Euclidean quadratic domain. We provide counterexamples, which show the essentiality of the conditions in the obtained theorems.

E-mail addresses: vaskovskii@bsu.by (M. Vaskouski), nkondr2006@rambler.ru (N. Kondratyonok).

http://dx.doi.org/10.1016/j.jsc.2016.02.003
0747-7171/

1. Introduction

Let a and b be two nonzero elements of a unique factorization domain (UFD) $\mathbb{K}$. In this paper we investigate the problem on searching for shortest division chains (DC)

$$r_i = r_{i-2} - q_i r_{i-1},\ i = 1, 2, \ldots, k, \tag{1}$$

where $q_1, \ldots, q_k \in \mathbb{K}$, $r_{-1} = a$, $r_0 = b$, $r_1, \ldots, r_{k-1} \in \mathbb{K}$, $r_k = 0$. If there exists finite DC (1), then it may be considered as a version of the Euclidean Algorithm (EA) and $r_{k-1} = \gcd(a, b)$.

Vahlen (1895) and Kronecker (1901) (see Bach and Shallit, 1996, p. 80) have proved that the least remainder EA requires no more division steps than any other EA which chooses between a remainder of $(a \mod b)$ or $((a \mod b) - b)$ at each step. Lazard (1977) has extended the Kronecker–Vahlen theorem on the case where any remainder is chosen at each step and also has proved the analogue of this theorem for polynomials over a field. Kaltofen and Rolletschek (1985) and Rolletschek (1986) have established the Lazard theorem analogue for special cases of imaginary quadratic domain $\mathbb{Z}[\sqrt{d}]$, d is a negative integer. Rolletschek (1990) has given a complete solution to the problem on shortest Euclidean algorithm in arbitrary imaginary quadratic domains $\mathbb{Z}[\sqrt{d}]$: the Lazard theorem analogue is valid in $\mathbb{Z}[\sqrt{d}]$, $d < 0$, if and only if $d \neq -11c^2$, $c \in \mathbb{N}$. Up to present the question on the validity of the Lazard theorem analogue is still open for all rings $\mathbb{Z}[\sqrt{d}]$ with $d > 1$. Vaskouski and Kondratyonok (2013) have found a class of Euclidean domains, for which the Lazard theorem analogue holds. The main purpose of this paper is to enlarge the class of unique factorization domain, for which the Lazard theorem analogue is valid, and estimate the length of chain (1) for fixed a and b.

The present paper is organized by the following way. Section 2 contains basic definitions and statements of main results. In section 3 we give general methods of main results proofs. Detailed proofs are given in section 4. Methods for validation of conditions in main theorems are given in section 5. Finally, section 6 is devoted to discuss the results, more precisely we provide some counterexamples to show essentiality of the conditions in main theorems. Also there is given an application to optimization of algorithm for solution of linear Diophantine equation in general UFD.

2. Main results

In this section we introduce some definitions and notation and give statements of the main results.

Definition 1. A function $\upsilon : \mathbb{K} \to \mathbb{N} \cup \{0, -\infty\}$ is called a *norm* in a UFD $\mathbb{K}$, if the following conditions hold:

1. $\upsilon(x) = -\infty$ iff $x = 0$;
2. $\upsilon(xy) \geq \upsilon(y)$ for any $x, y \in \mathbb{K}_*$;
3. If $x, y \in \mathbb{K}_*$, then $\upsilon(xy) = \upsilon(x)$ iff $y \in \mathbb{I}$, where $\mathbb{I}$ is the set of all invertible elements of $\mathbb{K}$.

Remark 1. Let $\mathbb{K}$ be a UFD, take an arbitrary element $x \in \mathbb{K}_*$. There exists a unique (up to multiplying of p_i by invertible elements of the domain $\mathbb{K}$) representation $x = \varepsilon p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, where $\varepsilon \in \mathbb{I}$, $p_1, \ldots, p_k$ are prime elements of $\mathbb{K}$, $\alpha_1, \ldots, \alpha_k \in \mathbb{N}$, $k \geq 0$ (if $k = 0$, then $x = \varepsilon$). It's clear that the function $\upsilon : \mathbb{K} \to \mathbb{N} \cup \{0, -\infty\}$, defined as $\upsilon(x) = \sum_{i=1}^{k} \alpha_i$, $x = \varepsilon p_1^{\alpha_1} \ldots p_k^{\alpha_k} \in \mathbb{K}_*$, $\upsilon(0) = -\infty$, is a norm in the UFD $\mathbb{K}$, where $\sum_{i=1}^{k} \alpha_i = 0$ for $k = 0$.

Remark 2. It's easy to check that any Euclidean norm $\upsilon(\cdot)$ is also norm in the sense of Definition 1.

Definition 2. Let $\mathbb{F}$ be the field of fractions of a UFD $\mathbb{K}$ with a norm υ. A function $\mathrm{fr} : \mathbb{F} \to \mathbb{F}$ is called a *fractional part* in $\mathbb{F}$ if the following holds:

1. $\mathrm{fr}(\alpha + q) = \mathrm{fr}(\alpha)$ for any $\alpha \in \mathbb{F}$, $q \in \mathbb{K}$;
2. If $m/n \in \mathbb{F}$, $\gcd(m, n) = 1$, then $\mathrm{fr}(m/n) = r/n$, where $r \in \mathbb{K}$, $(m-r)/n \in \mathbb{K}$, and $\upsilon(r) = \min\{\upsilon(s) | s \in \mathbb{K}, (m-s)/n \in \mathbb{K}\}$.

If $\mathrm{fr}:\mathbb{F}\to\mathbb{F}$ is a fractional part, then the function $\mathrm{int}:\mathbb{F}\to\mathbb{K}$,

$$\mathrm{int}(\alpha)=\alpha-\mathrm{fr}(\alpha),\ \alpha\in\mathbb{F},$$

is called an *integer part* in $\mathbb{F}$.

For any $\mathbb{K}$ being a UFD with a norm υ one can define integer and fractional parts in the field of fractions $\mathbb{F}$ by the following. Consider an arbitrary element $X\in\mathbb{F}/\mathbb{K}$, $X=\{m/n+t|t\in\mathbb{K}\}$, where m, n are coprime elements of $\mathbb{K}$, $n\neq 0$. There exists $t_0\in\mathbb{K}$ such that $\upsilon(m+nt_0)=\min\{\upsilon(m+nt)|t\in\mathbb{K}\}$. Then for any $x\in\mathbb{K}$ we put $\mathrm{fr}(x)=m/n+t_0$. Let $\mathrm{int}(x)=x-\mathrm{fr}(x)$. It's clear that $\mathrm{fr}(\cdot)$ and $\mathrm{int}(\cdot)$ are fractional and integer parts in $\mathbb{F}$ with respect to the norm υ.

We shall assume that any UFD $\mathbb{K}$ is equipped with a norm $\upsilon(\cdot)$ and the field of fractions $\mathbb{F}$ of the domain $\mathbb{K}$ is equipped with a fractional part $\mathrm{fr}(\cdot)$ and an integer part $\mathrm{int}(\cdot)$.

Definition 3. Let $\mathbb{K}$ be a UFD, a and b be two nonzero elements of $\mathbb{K}$. For any $k\in\mathbb{N}$ and $q_1,\dots,q_k\in\mathbb{K}$ denote

$$\mathcal{D}_{a,b}(q_1,\dots,q_k)=(r_{-1},r_0,\dots,r_{k-1},r_k)\in\mathbb{K}^{k+2},$$

where $r_{-1}=a$, $r_0=b$, $r_i=r_{i-2}-q_ir_{i-1}$, $i=1,2,\dots,k$.

Denote by $\mathcal{E}_{a,b}$ the set

$$\{\mathcal{D}_{a,b}(q_1,\dots,q_k)=(r_{-1},\dots,r_k)|k\in\mathbb{N},q_1,\dots,q_k\in\mathbb{K},r_1,\dots,r_{k-1}\in\mathbb{K}_*,r_k=0\},$$

it is possible that $\mathcal{E}_{a,b}=\emptyset$.

Definition 4. The *Least Remainder DC* of a, b is DC

$$\mathcal{D}_{a,b}(q_1,\dots,q_k)=\mathcal{g}_{a,b}\in\mathcal{E}_{a,b}$$

such that $q_i=\mathrm{int}(r_{i-2}/r_{i-1})$ for any $i=1,\dots,k$. If there exists the Least Remainder DC for (a,b), then denote by $\mathcal{L}_{a,b}$ the length k of the Least Remainder DC, otherwise we set $\mathcal{L}_{a,b}=\infty$.

Let us give an example of UFD for which the Least Remainder DC may not exist.

Example 1. Let $\mathbb{K}=\mathbb{Z}[t]$. Define the fractional part in $\mathbb{F}=\mathbb{Z}(t)$ by the following. Let the map $\mathcal{A}:\mathbb{F}/\mathbb{K}\to\mathbb{F}$ be defined as $\mathcal{A}(\mathbb{A})=m(t)/n(t)$, where $\mathbb{A}=\{m(t)/n(t)+q(t)|q(t)\in\mathbb{Z}[t]\}$. For any $\mathbb{A}\in\mathbb{F}/\mathbb{K}$, $\alpha\in\mathbb{A}$ set $\mathrm{int}(\alpha)=r(t)$, $\mathrm{fr}(\alpha)=\mathcal{A}(\mathbb{A})-r(t)$, where $r(t)\in\mathbb{Z}[t]$, $\lim_{t\to+\infty}\left|\frac{\mathcal{A}(\mathbb{A})-r(t)}{\mathcal{A}(\mathbb{A})-p(t)}\right|\leq 1\ \forall p(t)\in\mathbb{Z}[t]$.

Take polynomials $a(t)=t$, $b(t)=2$. Suppose that there exists $\mathcal{g}_{a(t),b(t)}$. Then there exist polynomials $f(t)$, $g(t)$ such that

$$1=\gcd(a(t),b(t))=tf(t)+2g(t).$$

But this is impossible, since the equality $1=2g(0)$ fails for any $g(t)\in\mathbb{Z}[t]$. Hence, there doesn't exist $\mathcal{g}_{a(t),b(t)}$.

Definition 5. Denote by $\mathcal{l}_{a,b}$ the smallest positive integer k such that there exists $\mathcal{D}_{a,b}(q_1,\dots,q_k)\in\mathcal{E}_{a,b}$ if $\mathcal{E}_{a,b}\neq\emptyset$, and put $\mathcal{l}_{a,b}=\infty$ if $\mathcal{E}_{a,b}=\emptyset$. Let

$$\mathcal{O}_{a,b}=\{\mathcal{D}(q_1,\dots,q_k)\in\mathcal{E}_{a,b}|k=\mathcal{l}_{a,b}\}$$

for $\mathcal{E}_{a,b}\neq\emptyset$ and $\mathcal{O}_{a,b}=\emptyset$ for $\mathcal{E}_{a,b}=\emptyset$.

Definition 6. Define *number of steps* of the Least Remainder DC by the following:

$$l_n(\mathbb{K})=\max\{\mathcal{L}_{a,b}|(a,b)\in\mathbb{K}_*\times\mathbb{K}_*,n\geq\upsilon(a)\geq\upsilon(b)\},n\in\mathbb{N}.$$

Definition 7. Denote by $\mathbb{F}_1$ the set of all regular irreducible fractions of $\mathbb{F}$, i.e., $\mathbb{F}_1 = \{\alpha \in \mathbb{F} | \alpha = \mathrm{fr}(\alpha)\}$, $\mathbb{F}_1^* = \mathbb{F}_1 \backslash \{0\}$. Define the function $\omega : \mathbb{F}_1 \to \mathbb{F}_1$ by the following: $\omega(\alpha) = \mathrm{fr}(\alpha^{-1})$ for $\alpha \neq 0$, $\omega(0) = 0$.

Definition 8. A triple $(x_0, \alpha, n) \in \mathbb{K}_* \times \mathbb{F}_1^* \times \mathbb{N}$ is called *regular* if there exist natural numbers p and l, $p \leq n$, $l \leq p+1$, such that there exist $\varepsilon_i \in \mathbb{I}$, $b_i, c_i \in \mathbb{K}$, $i = \overline{1, l-1}$, satisfying the relations $\beta_1 = \omega^{(p)}(\mathrm{fr}((\alpha - x_0)^{-1}))$, $\beta_{i+1} = (\varepsilon_i \beta_i + c_i)^{-1} + b_i$, $i = \overline{1, l-1}$, $\beta_l = \alpha^{(-1)^\varepsilon}$, where $\varepsilon \in \{0, 1\}$, $\omega^{(p)}$ is the p-multiple composition of ω.

Definition 9. Let $\mathcal{T}$ be the set of all UFD $\mathbb{K}$ such that there exists $D_{\mathbb{K}} \in \mathbb{N}$ such that the following conditions hold:

1. For every $x_0 \in \mathbb{K}_*$, $\alpha \in \mathbb{F}_1^*$, the triple $(x_0, \alpha, D_{\mathbb{K}})$ is regular.
2. If $D_{\mathbb{K}} \geq 3$, then for any natural $k \in [3, D_{\mathbb{K}}]$ and $x_0 \in \mathbb{K}_*$, $\alpha \in \mathbb{F}_1^*$ the triple $(x_0, \alpha, k-2)$ is regular, assuming that $\omega^{(k-2)}(\mathrm{fr}((\alpha - x_0)^{-1})) = 0$.

Definition 10. Let $\Lambda_{\mathbb{K}} = \sup_{m/n \in \mathbb{F}_1} |m/n|$, where $|m/n| = \upsilon(m)/\upsilon(n)$ for $m/n \in \mathbb{F}_1^*$, $\gcd(m, n) = 1$, and $|0| = 0$.

Let $d \neq 1$ be an integer squarefree number. We recall that the quadratic domain $\mathbb{Z}[\sqrt{d}]$ is the domain of all integer algebraic elements of the quadratic field $\mathbb{Q}[\sqrt{d}]$. It is known (see, e.g., Rolletschek, 1986) that $\mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} | a, b \in \mathbb{Z}\}$ if $d \not\equiv 1 (\mathrm{mod}\ 4)$, and $\mathbb{Z}[\sqrt{d}] = \{(a + b\sqrt{d})/2 | a, b \in \mathbb{Z}, a \equiv b (\mathrm{mod}\ 2)\}$ if $d \equiv 1 (\mathrm{mod}\ 4)$. Let the norm in $\mathbb{Z}[\sqrt{d}]$ be defined as

$$\upsilon(a + b\sqrt{d}) = |a^2 - db^2| \text{ for } a + b\sqrt{d} \in \mathbb{Z}[\sqrt{d}] \setminus \{0\}, a, b \in \mathbb{Q}, \upsilon(0) = -\infty. \tag{2}$$

Let the fractional part in $\mathbb{Q}[\sqrt{d}]$ for $d < 0$ be defined by the following

$$\mathrm{fr}(q_1 + q_2\sqrt{d}) = q_1 - [q_1 + 1/2] + (q_2 - [q_2 + 1/2])\sqrt{d}, \tag{3}$$

where $q_1, q_2 \in \mathbb{Q}$, $[x] = \max\{k \in \mathbb{Z} | k \leq x\}$.

Now we are ready to state the main results.

Theorem 1. *Suppose that $\mathbb{K} \in \mathcal{T}$. Then the Least Remainder DC is Shortest DC, i.e. $\mathcal{L}_{a,b} = \ell_{a,b}$ for any $a, b \in \mathbb{K}_*$.*

Theorem 2. *The following statements are valid.*

1. *If $\mathbb{K}$ is a Euclidean domain with respect to the given norm υ, then $\Lambda_{\mathbb{K}} \in [0, 1]$.*
2. *If $\mathbb{K}$ is a UFD with a norm υ and $\Lambda_{\mathbb{K}} \in [0, 1)$, then the domain $(\mathbb{K}, \upsilon)$ is Euclidean, and the following inequality holds $l_n(\mathbb{K}) \leq [\log_{\Lambda_{\mathbb{K}}^{-1}} n] + 2$ for any $n \in \mathbb{N}$, where $\log_\infty n = 0$.*

Theorem 3. *Let $d \neq 1$ be an integer squarefree number. If the domain $\mathbb{Z}[\sqrt{d}]$ is Euclidean, then the following holds $l_n(\mathbb{Z}[\sqrt{d}]) = O(\log n)$.*

3. General strategy of proofs

Let's present main ideas of Theorem 1 proof.

For any DC $\mathcal{D}_{a,b}(q_1, \ldots, q_k) \in \mathcal{E}_{a,b}$ we consider reference finite continued fraction

$$\frac{a}{b} = x_1 + \cfrac{1}{x_2 + \cfrac{1}{x_3 + \cfrac{1}{\ddots + \cfrac{1}{x_k}}}} := [x_1 : x_2 : \ldots : x_k]. \tag{4}$$

It's clear that $x_i = q_i$, $i = 1, \ldots, k$.

Lemma 1 has key role in the proof of Theorem 1 and gives existence criterion to represent an element a/b of fraction field $\mathbb{F}$ in the form of continued fraction (4) of a fixed length. Next step is to express the length of the Least Remainder DC in terms of functions of fractional part (Proposition 2). The final step is to consider the length of the Shortest DC as minimal length of finite continued fraction such that Eq. (4) has a solution with respect to variables $x_1, \ldots, x_k$. We need to require the condition $\mathbb{K} \in \mathcal{T}$ to enable validity of Lemma 1. Induction on the length of finite continued fraction (4) is applied. Condition $\mathbb{K} \in \mathcal{T}$ gives the ability to reconstruct continued fraction (4) in proper way for validation of the inductive step. In further we'll prove that both Lemma 1 and Theorem 1 fail if we omit condition $\mathbb{K} \in \mathcal{T}$.

Let's proceed to the main ideas of Theorems 2 and 3 proofs.

Firstly, we give necessary and sufficient conditions for UFD $\mathbb{K}$ to be Euclidean in terms of characteristic $\Lambda_{\mathbb{K}}$ (see Definition 10). If $\Lambda_{\mathbb{K}} < 1$, then definition of Λ_K and basic properties of integer and fractional parts imply the logarithmic length $O(\log n)$ of the Least Remainder DC for any $a, b \in \mathbb{K}_*$ with $\upsilon(a) \le n$, $\upsilon(b) \le n$. In further we'll see that condition $\Lambda_{\mathbb{K}} < 1$ can't be replaced by weaker condition $\Lambda_{\mathbb{K}} \le 1$ without loss of logarithmic length $O(\log n)$ of the Least Remainder DC.

To obtain the logarithmic length $O(\log n)$ of the Least Remainder DC for any $a, b \in \mathbb{K}_*$ with $\upsilon(a) \le n$, $\upsilon(b) \le n$, in any Euclidean quadratic domain $\mathbb{Z}[\sqrt{d}]$ we use sufficient condition $\Lambda_{\mathbb{K}} < 1$ to have logarithmic length $O(\log n)$ of the Least Remainder DC and the following characterization of quadratic Euclidean domains, obtained in the paper Selfridge et al. (1992).

Proposition 1. *Let $d \neq 1$ be an integer squarefree number. The quadratic domain $\mathbb{Z}[\sqrt{d}]$ is Euclidean iff there exists $\lambda = \lambda_1 + \lambda_2\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$, $\lambda_1, \lambda_2 \in \mathbb{Q}$, such that the fundamental region $F(d)$ is contained in the unitary open ball $U(\lambda, 1)$ in $\mathbb{Q}[\sqrt{d}]$ with the center in λ, where $F(d) = ([0, 1/2] \times [0, 1/2]) \cap (\mathbb{Q} \times \mathbb{Q})$ if $d \not\equiv 1 (mod\ 4)$, and $F(d) = ([0, 1/2] \times [0, 1/4]) \cap (\mathbb{Q} \times \mathbb{Q})$ if $d \equiv 1 (mod\ 4)$, $U(\lambda, r) = \{q_1 + q_2\sqrt{d} \in \mathbb{Q}[\sqrt{d}] \,|\, q_1, q_2 \in \mathbb{Q}, |(q_1 - \lambda_1)^2 - d(q_2 - \lambda_2)^2| < r\}$, $r > 0$.*

4. Proofs of main results

4.1. Theorem 1

Lemma 1. *Let $\mathbb{K} \in \mathcal{T}$. If $\alpha \in \mathbb{F}_1$, $k \in \mathbb{N}$, then Eq. (4) is (α, k)-solvable, i.e., there exist $x_1, \ldots, x_k \in \mathbb{K}$ such that $\alpha = [x_1 : x_2 : \ldots : x_k]$, iff one has $\omega^{(k-1)}(\alpha) = 0$.*

Proof. Let $\alpha = m/n \in \mathbb{F}_1$, $\gcd(m, n) = 1$, $k \in \mathbb{N}$. If $\alpha = 0$ or $k = 1$, then the statement of the lemma is obvious. Suppose that $\alpha \neq 0$, $k \ge 2$. Consider the case $k = 2$. It's easy to see that Eq. (4) is $(\alpha, 2)$-solvable iff the following congruence holds $m \equiv \varepsilon (\mathrm{mod}\ n)$ for some $\varepsilon \in \mathbb{I}$. Let $m = qn + \varepsilon$, $q \in \mathbb{K}$, then $m/n = \mathrm{fr}(m/n) = \mathrm{fr}(q + \varepsilon/n) = \mathrm{fr}(\varepsilon/n)$. Since the norm υ takes the minimal finite value only at invertible elements of the domain $\mathbb{K}$, so $\mathrm{fr}(\varepsilon/n) = \delta/n$, where $\delta \in \mathbb{I} \cup \{0\}$.

Suppose that $D_{\mathbb{K}} \ge 3$. Let's prove the lemma for all $k \le D_{\mathbb{K}}$ by induction on k. The base of induction is validity of the lemma for $k = 1$ and $k = 2$. It's easy to see that Eq. (4) is (α, k)-solvable iff there exists $z \in \mathbb{K}$ such that Eq. (4) is $((\alpha - z)^{-1}, k - 1)$-solvable. That is why we need to prove that for any $k \in [3, D_{\mathbb{K}}]$ the following holds: $\omega^{(k-1)}(\alpha) = 0$ iff there exists $z \in \mathbb{K}$ such that $\omega^{(k-2)}(\mathrm{fr}((\alpha - z)^{-1})) = 0$.

Let $\omega^{(k-1)}(\alpha) = 0$. By the definition of ω, we get $\omega^{(k-2)}(\mathrm{fr}(\alpha^{-1})) = 0$.

Suppose that there exists $z \in \mathbb{K}$ such that $\omega^{(k-2)}(\mathrm{fr}((\alpha - z)^{-1})) = 0$. If $z = 0$, then the definition of the function ω implies the equality $\omega^{(k-1)}(\alpha) = 0$. Let $z \neq 0$. By assumption (2) in the definition of the class $\mathcal{T}$, we obtain that the triple $(z, \alpha, k - 2)$ is regular. Hence, there exist natural numbers p and l, $p \le k - 2$, $l \le p + 1$, such that there exist invertible elements $\varepsilon_i \in \mathbb{I}$ and elements $b_i, c_i \in \mathbb{K}$ $(i = 1, \ldots, l - 1)$, for which the following relations hold:

$$\beta_1 = \omega^{(p)}(\mathrm{fr}((\alpha - z)^{-1})),\ \beta_{i+1} = (\varepsilon_i\beta_i + c_i)^{-1} + b_i,\ i = \overline{1, l-1},\ \beta_l = \alpha^{(-1)^{\varepsilon}}, \tag{5}$$

where $\varepsilon \in \{0, 1\}$.

Since $\omega^{(k-p-2)}(\beta_1)=0$, so by the inductive assumption, Eq. (4) is $(\beta_1, k-p-1)$-solvable. It follows from (5) that for any $i=1,\dots,l-1$ and $j\in\mathbb{N}$ Eq. (4) is (β_i, j)-solvable iff Eq. (4) is $(\beta_{i+1}, j+1)$-solvable. Hence, Eq. (4) is $(\alpha^{(-1)^\varepsilon}, k-p+l-2)$-solvable. Since $k-p+l-2\le k-1$, so, by the inductive assumption, we receive that $\omega^{(k-p+l-3)}(\mathrm{fr}(\alpha^{(-1)^\varepsilon}))=0$. Consequently, $\omega^{(k-2)}(\mathrm{fr}(\alpha^{(-1)^\varepsilon}))=0$. The last equality and the definition of ω imply that $\omega^{(k-1)}(\alpha)=0$. So, the lemma is proved for all $k\le D_{\mathbb{K}}$.

Let's prove the lemma for any k by induction on k. The base of induction is validity of the lemma for all $k\le D_{\mathbb{K}}$. Let k be a natural number, $k>D_{\mathbb{K}}$. It is sufficiently to prove that $\omega^{(k-1)}(\alpha)=0$ iff there exists $z\in\mathbb{K}$ such that $\omega^{(k-2)}(\mathrm{fr}((\alpha-z)^{-1}))=0$.

The necessity is obvious. Let there exist $z\in\mathbb{K}$ such that the following holds

$$\omega^{(k-2)}(\mathrm{fr}((\alpha-z)^{-1}))=0.$$

If $z=0$, then, by the definition of ω, we get $\omega^{(k-1)}(\alpha)=0$.

Suppose that $z\neq 0$. By assumption (1) in the definition of the class $\mathcal{T}$, we receive that the triple $(z,\alpha,D_{\mathbb{K}})$ is regular, i.e., there exist natural numbers q and m, $q\le D_{\mathbb{K}}$, $m\le q+1$, such that there exist invertible elements $p_i\in\mathbb{I}$ and elements $f_i, g_i\in\mathbb{K}$ $(i=1,\dots,m-1)$, satisfying the relations

$$\gamma_1=\omega^{(q)}(\mathrm{fr}((\alpha-z)^{-1})),\ \gamma_{i+1}=(p_i\gamma_i+q_i)^{-1}+f_i,\quad i=\overline{1,m-1},\ \gamma_m=\alpha^{(-1)^\varepsilon}, \tag{6}$$

where $\varepsilon\in\{0,1\}$.

Since $\omega^{(k-q-2)}(\gamma_1)=0$, so the inductive assumption implies that Eq. (4) is $(\gamma_1, k-q-1)$-solvable.

Relations (6) imply that Eq. (4) is $(\alpha^{(-1)^\varepsilon}, k-q+m-2)$-solvable. Since $k-q+m-2\le k-1$, so, by the inductive assumption, we obtain that $\omega^{(k-q+m-3)}(\mathrm{fr}(\alpha^{(-1)^\varepsilon}))=0$. The definition of the function ω implies the equality $\omega^{(k-1)}(\alpha)=0$. The lemma is proved. □

Proposition 2. *Let $\mathbb{K}$ be a UFD. Then for any two elements $(a,b)\in\mathbb{K}_*\times\mathbb{K}_*$ the following equality holds*

$$\mathcal{L}_{a,b}=\min\{k\in\mathbb{N}\,|\,\omega^{(k-1)}(\mathrm{fr}(a/b))=0\},$$

where $\min\emptyset=\infty$.

Proof. Take arbitrary $a, b\in\mathbb{K}_*$. Suppose that $\mathcal{L}_{a,b}<\infty$. Let

$$\mathcal{g}_{a,b}=\mathcal{D}_{a,b}(q_1,\dots,q_k)=(r_{-1},r_0,r_1,\dots,r_{k-1},r_k),$$

where $r_{-1}=a$, $r_0=b$, $r_k=0$, $r_i\neq 0$ for any $i=\overline{1,k-1}$.

It follows from the relations

$$\frac{a}{b}=q_1+\frac{r_1}{b},\ \frac{b}{r_1}=q_2+\frac{r_2}{r_1},\dots,\ \frac{r_{k-3}}{r_{k-2}}=q_{k-1}+\frac{r_{k-1}}{r_{k-2}},\ \frac{r_{k-2}}{r_{k-1}}=q_k$$

and the definitions of the function ω and the Least Remainder DC that the following equalities hold

$$\omega\left(\mathrm{fr}\left(\frac{a}{b}\right)\right)=\mathrm{fr}\left(\frac{b}{r_1}\right),\omega^{(2)}\left(\mathrm{fr}\left(\frac{a}{b}\right)\right)=\mathrm{fr}\left(\frac{r_1}{r_2}\right),\dots,\omega^{(k-1)}\left(\mathrm{fr}\left(\frac{a}{b}\right)\right)=\mathrm{fr}\left(\frac{r_{k-2}}{r_{k-1}}\right)=0. \tag{7}$$

It follows from (7) that one has $\omega^{(k-1)}(\mathrm{fr}(a/b))=0$.

Since $\omega^{(j-1)}(\mathrm{fr}(a/b))=r_j/r_{j-1}\neq 0$ for any $j=1,\dots,k-1$, so

$$\mathcal{L}_{a,b}=k=\min\{n\in\mathbb{N}\,|\,\omega^{(n-1)}(\mathrm{fr}(a/b))=0\}.$$

Let $\mathcal{L}_{a,b}=\infty$. Suppose that there exists $k\in\mathbb{N}$ such that $\omega^{(k-1)}(\mathrm{fr}(a/b))=0$ (choose the smallest natural k with this property).

Let $\mathrm{int}(a/b)=q_1$, $\mathrm{fr}(a/b)=r_1/b$. If $r_1=0$, then $\mathcal{L}_{a,b}=1$, this is a contradiction. Hence $r_1\neq 0$. By the definition of ω, we obtain the equality $\omega^{(k-2)}(\mathrm{fr}(b/r_1))=0$. Let $\mathrm{int}(b/r_1)=q_2$, $\mathrm{fr}(b/r_1)=r_2/r_1$. If $r_2=0$, then $\mathcal{L}_{a,b}=2$, this is a contradiction. We deduce that $r_2\neq 0$ and $\omega^{(k-3)}(\mathrm{fr}(r_1/r_2))=0$.

Applying the analogous arguments, we construct the elements $r_3, \dots, r_k$, $q_3, \dots, q_k$ such that $\operatorname{int}(r_{i-2}/r_{i-1}) = q_i$, $\operatorname{fr}(r_{i-2}/r_{i-1}) = r_i/r_{i-1}$ for any $i = \overline{3,k}$ and $\omega^{(0)}(\operatorname{fr}(r_{k-2}/r_{k-1})) = r_k/r_{k-1} = 0$. Hence $r_k = 0$. The last one contradicts with $\mathcal{L}_{a,b} = \infty$. The proposition is proved. □

Let $(a,b) \in \mathbb{K}_* \times \mathbb{K}_*$. Suppose that $\mathcal{l}_{a,b} = k < \infty$. Let

$$\mathcal{D}_{a,b}(q_1, \dots, q_k) = (r_{-1}, r_0, r_1, \dots, r_{k-1}, r_k) \in \mathcal{O}_{a,b},$$

where $r_{-1} = a$, $r_0 = b$, $r_k = 0$, $r_i \neq 0$ for any $i = \overline{1, k-1}$.

Since $\imath(\mathcal{D}_{a,b}(q_1, \dots, q_k)) = [q_1 : q_2 : \dots : q_k]$, so, by Lemma 1, we get $\omega^{(k-1)}(\operatorname{fr}(a/b)) = 0$. It follows from Proposition 2 that

$$\mathcal{L}_{a,b} = \min\{r \in \mathbb{N} | \omega^{(r-1)}(\operatorname{fr}(a/b)) = 0\} \leq k = \mathcal{l}_{a,b}.$$

Hence, $\mathcal{L}_{a,b} = \mathcal{l}_{a,b}$.

If $\mathcal{l}_{a,b} = \infty$, then $\mathcal{E}_{a,b} = \emptyset$. Consequently, $\mathcal{L}_{a,b} = \infty$. This finishes the proof of Theorem 1.

4.2. Theorem 2

1. Let $(\mathbb{K}, \upsilon)$ be a Euclidean domain, then for any a and $b \in \mathbb{K}_*$ there exist q and $r \in \mathbb{K}$ such that $a = bq + r$ and $\upsilon(r) < \upsilon(b)$. Consider an arbitrary element $a/b \in \mathbb{F}_1^*$, $a, b \in \mathbb{K}$, $\gcd(a,b) = 1$. Let $a = bq + r$ and $\upsilon(r) < \upsilon(b)$, where $q, r \in \mathbb{K}$. Since $a/b = \operatorname{fr}(a/b)$, so $\upsilon(a) \leq \upsilon(r)$. Hence, $|a/b| = \upsilon(a)/\upsilon(b) \leq \upsilon(r)/\upsilon(b) < 1$. Consequently, $\Lambda_{\mathbb{K}} \in [0,1]$.

2. Let's fix an arbitrary natural number n.

Suppose that $\Lambda_{\mathbb{K}} \in [0,1)$. Then for any $a/b \in \mathbb{F}_1^*$, $a, b \in \mathbb{K}$, $\gcd(a,b) = 1$, we have $|a/b| = \upsilon(a)/\upsilon(b) < 1$. Take arbitrary $a, b \in \mathbb{K}$, $b \neq 0$. Let $q = \operatorname{int}(a/b)$, $r = b \operatorname{fr}(a/b)$, then $a = bq + r$ and $\upsilon(r) \leq \Lambda_{\mathbb{K}} \upsilon(b)$. If $\upsilon(b) > 0$, then $\upsilon(r) \leq \Lambda_{\mathbb{K}} \upsilon(b) < \upsilon(b)$. If $\upsilon(b) = 0$, then b is an invertible element of $\mathbb{K}$ and, consequently, $a = 0$ and $r = 0$. As $\upsilon(r) < \upsilon(b)$, so the domain $(\mathbb{K}, \upsilon)$ is Euclidean.

Consequently, for each $(a,b) \in \mathbb{K}_* \times \mathbb{K}_*$ with $n \geq \upsilon(a) \geq \upsilon(b)$ one has $\mathcal{E}_{a,b} \neq \emptyset$ and there exists $g_{a,b} = \mathcal{D}_{a,b}(q_1, \dots, q_k) = (r_{-1}, r_0, r_1, \dots, r_{k-1}, r_k)$, where $r_{-1} = a$, $r_0 = b$, $r_k = 0$, $r_i \neq 0$ for any $i = \overline{1, k-1}$.

Without loss of generality we may assume that $\gcd(a,b) = 1$. This assumption implies the equality $\gcd(r_{i-1}, r_i) = 1$ for any $i = 1, \dots, k$. Since $\operatorname{fr}(r_{i-2}/r_{i-1}) = r_i/r_{i-1} \neq 0$, $i = 1, \dots, k-1$, so

$$|r_i/r_{i-1}| = \upsilon(r_i)/\upsilon(r_{i-1}) \leq \Lambda_{\mathbb{K}}$$

for $i = 1, \dots, k-1$. Consequently,

$$\upsilon(r_i) \leq \upsilon(b)\Lambda_{\mathbb{K}}^i \leq n\Lambda_{\mathbb{K}}^i$$

for $i = 1, \dots, k-1$. Since $r_{k-2} \notin \mathbb{I} \cup \{0\}$, so $\upsilon(r_{k-1}) > \upsilon(1) \geq 0$. Hence, we get $1 \leq \upsilon(r_{k-2}) \leq n\Lambda_{\mathbb{K}}^{k-2}$. The last one implies the inequality $k \leq \log_{\Lambda_{\mathbb{K}}^{-1}} n + 2$. Consequently, $l_n(\mathbb{K}) \leq [\log_{\Lambda_{\mathbb{K}}^{-1}} n] + 2$. Theorem 2 is proved.

4.3. Theorem 3

By Proposition 1, there exists $\lambda = \lambda_1 + \lambda_2\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$, $\lambda_1, \lambda_2 \in \mathbb{Q}$, such that the following inclusion holds $F(d) \subset U(\lambda, 1)$, where the sets $F(d)$ and $U(\lambda, 1)$ are defined in Proposition 1.

Let $E(d) = [0, 1/2] \times [0, 1/4]$ if $d \equiv 1 (\operatorname{mod} 4)$ and $E(d) = [0, 1/2] \times [0, 1/2]$ if $d \not\equiv 1 (\operatorname{mod} 4)$. For any $r > 0$ define the set

$$V(\lambda, r) = \{(x, y) \in \mathbb{R} \times \mathbb{R} \big| |(x - \lambda_1)^2 - d(y - \lambda_2)^2| < r\}.$$

Let's prove validity of the inclusion $E(d) \subset V(\lambda, 1)$. Suppose that there exists $(x_0, y_0) \in E(d) \backslash V(\lambda, 1)$. Since $F(d) \backslash U(\lambda, 1) = \emptyset$, so $x_0 \notin \mathbb{Q}$ or $y_0 \notin \mathbb{Q}$. Let $x_0 \notin \mathbb{Q}$. Then there exists $\varepsilon > 0$ such that one has

$$\{(x, y_0) | x \in [x_0 - \varepsilon, x_0 + \varepsilon]\} \in E(d) \backslash V(\lambda, 1).$$

If $y_0 \in \mathbb{Q}$, then there exists $\varepsilon_0 \in (0, \varepsilon)$ such that the point $(x_0 + \varepsilon_0, y_0)$ has rational coordinates and belongs to $E(d)\backslash V(\lambda, 1)$, and hence

$$(x_0 + \varepsilon_0, y_0) \in F(d)\backslash U(\lambda, 1) = \emptyset,$$

that is impossible. If $y_0 \notin \mathbb{Q}$, then there exists $\varepsilon > 0$ such that

$$\{(x, y) | x \in [x_0 - \varepsilon, x_0 + \varepsilon], y \in [y_0 - \varepsilon, y_0 + \varepsilon]\} \in E(d)\backslash V(\lambda, 1).$$

Consequently, there exists a point $(x_1, y_1) \in E(d)\backslash V(\lambda, 1)$ with rational coordinates. Hence, $(x_1, y_1) \in F(d)\backslash U(\lambda, 1) = \emptyset$.

So, we have $E(d) \subset V(\lambda, 1)$.

Let's prove the existence of a number $r_0 < 1$ such that the inclusion $F(d) \subset U(\lambda, r_0)$ is valid. It is sufficient to prove that $E(d) \subset V(\lambda, r_0)$ for some $r_0 < 1$.

Suppose a contrary, i.e., for any $r \in (0, 1)$ the set $X_r = E(d)\backslash V(\lambda, r)$ is not empty. Take an arbitrary sequence $r_n \to 1 - 0$ as $n \to \infty$ and choose a point $q_{r_n} \in X_{r_n}$ for any natural number n. Since the sequence (q_{r_n}), $n \in \mathbb{N}$, is bounded, so there exists a convergence subsequence $q_{r_{n_m}} \to q$ if $m \to \infty$. As $V(\lambda, 1) = \bigcup_{m\in\mathbb{N}} V(\lambda, r_{n_m})$, so the following holds $E(d)\backslash V(\lambda, 1) = \bigcap_{m\in\mathbb{N}} X_{r_{n_m}}$. Since $q_{r_{n_m}} \in X_{r_{n_m}} \subset E(d)\backslash V(\lambda, 1)$ for any $m \in \mathbb{N}$ and the set $E(d)\backslash V(\lambda, 1)$ is closed in $\mathbb{R} \times \mathbb{R}$, so the inclusion $q \in E(d)\backslash V(\lambda, 1)$ is valid. But the last one contradicts with the inclusion $E(d) \subset V(\lambda, 1)$.

So, we have $F(d) \subset U(\lambda, r_0)$ for some $r_0 < 1$ and $\lambda \in \mathbb{Z}[\sqrt{d}]$. We deduce that for any $\gamma, \delta \in \mathbb{Z}[\sqrt{d}]$, $\delta \neq 0$ there exists an element $q \in \mathbb{Z}[\sqrt{d}]$, such that $N\left(\frac{\gamma}{\delta} - q\right) \leq r_0$, where $N\left(\frac{a+b\sqrt{d}}{c}\right) = \frac{|a^2-db^2|}{c^2}$, $a, b, c \in \mathbb{Z}$, $c \neq 0$. Since $N\left(\frac{\gamma}{\delta} - q\right) = \frac{N(\gamma-q\delta)}{N(\delta)}$, so for any $\delta, \gamma \in \mathbb{Z}[\sqrt{d}]$, $\delta \neq 0$, there exist $q, r \in \mathbb{Z}[\sqrt{d}]$ such that $\gamma = q\delta + r$ and $N(r) \leq r_0 N(\delta)$. Consequently, one has $\Lambda_{\mathbb{Z}[\sqrt{d}]} \leq r_0$.

So, by Theorem 2, we obtain the inequality $l_n(\mathbb{Z}[\sqrt{d}]) \leq [\log_{r_0^{-1}} n] + 2$ for any $n \in \mathbb{N}$. Theorem is proved.

5. Methods to prove the inclusion $\mathbb{K} \in \mathcal{T}$

Let us give the first method of checking of the inclusion $\mathbb{K} \in \mathcal{T}$.

Definition 11. Let $\mathcal{S}$ be the set of all UFD $\mathbb{K}$ such that for any $x \in \mathbb{K}_*$ and $\alpha \in \mathbb{F}_1^*$ one of the following conditions holds:

1. $\operatorname{int}((\alpha - x)^{-1}) \in \mathbb{I} \cup \{0\}$;
2. $x \operatorname{int}((\alpha - x)^{-1}) + 1 \in \mathbb{I}$.

Proposition 3. *The inclusion $\mathcal{S} \subseteq \mathcal{T}$ holds.*

Proof. Let a UFD $\mathbb{K}$ belong to $\mathcal{S}$. Take $D_{\mathbb{K}} = 1$. We need to prove that for any $x_0 \in \mathbb{K}_*$, $\alpha \in \mathbb{F}_1^*$ the triple $(x_0, \alpha, D_{\mathbb{K}})$ is regular. Choose $p = 1$ in the definition of regular triple. Denote $b = \operatorname{int}((\alpha - x)^{-1})$.

Suppose that $b \in \mathbb{I} \cup \{0\}$. We have $\beta_1 = \omega(\operatorname{fr}((\alpha - x)^{-1})) = \omega((\alpha - x)^{-1} - b) = \operatorname{fr}\left(\frac{\alpha-x}{1-b\alpha+bx}\right)$. There exists $c \in \mathbb{K}$ such that $\beta_1 = \frac{\alpha-x}{1-b\alpha+bx} - c$. If $b = 0$, then $\beta_2 = \alpha^{-1} = (\beta_1 + x + c)^{-1}$. If $b \in \mathbb{I}$, then $\beta_1 = \frac{b^{-1}}{1-b\alpha+bx} - b^{-1} - c$ and $\beta_2 = \alpha = (-b^2\beta_1 - b - b^2c)^{-1} + b^{-1} + x$.

Denote $xb + 1 = \varepsilon$. Suppose that $\varepsilon \in \mathbb{I}$. Analogously we receive $\beta_1 = \operatorname{fr}\left(\frac{\alpha-x}{1-b\alpha+bx}\right)$. Then $\beta_1 = \frac{\alpha-x}{1-b\alpha+bx} - c$ for some $c \in \mathbb{K}$. Hence,

$$\beta_2 = \alpha^{-1} = \frac{b\beta_1 + bc + 1}{\beta_1(1 + bx) + c(1 + bx) + x} = \frac{b\beta_1 + bc + 1}{\beta_1\varepsilon + c\varepsilon + x} =$$
$$= b\varepsilon^{-1} + \frac{1 - b\varepsilon^{-1}x}{\beta_1\varepsilon + c\varepsilon + x} = b\varepsilon^{-1} + \frac{\varepsilon^{-1}}{\beta_1\varepsilon + c\varepsilon + x} = (\beta_1\varepsilon^2 + c\varepsilon^2 + x\varepsilon)^{-1} + b\varepsilon^{-1}.$$

So, the triple $(x_0, \alpha, D_{\mathbb{K}})$ is regular and the proposition is proved. □

Now we are going to give a semi-decision algorithm to check the condition $\mathbb{K} \in \mathcal{S}$.

Algorithm 1.

Step 1. Construct the set $\mathbb{J} = \{x \in \mathbb{K}_* | \text{int}((\alpha - x)^{-1}) \in \mathbb{I} \cup \{0\}\ \forall \alpha \in \mathbb{F}_1^*\}$.
Step 2. For any $x_0 \in \mathbb{K}_* \backslash \mathbb{J}$ construct the value set $\mathbb{Y}(x_0)$ of the function $f_{x_0}(\alpha) = \text{int}((\alpha - x_0)^{-1})$, $\alpha \in \mathbb{F}_1^*$.
Step 3. For any $x_0 \in \mathbb{K}_* \backslash \mathbb{J}$ construct the set $\mathbb{U}(x_0) = \{\frac{\varepsilon - 1}{x_0} \in \mathbb{K} | \varepsilon \in \mathbb{I}\} \cup \mathbb{I}$.
Step 4. If the inclusion $\mathbb{Y}(x_0) \subseteq \mathbb{U}(x_0)$ holds for any $x_0 \in \mathbb{K}_* \backslash \mathbb{J}$, then the answer is "Yes", i.e. $\mathbb{K} \in \mathcal{S}$. Otherwise, the answer is "Unknown".

Correctness of Algorithm 1. Suppose that the answer of Algorithm 1 is "Yes". Take an arbitrary $x_0 \in \mathbb{K}$. If $x_0 \in \mathbb{J}$, then the first part of the definition holds. Suppose that $x_0 \notin \mathbb{J}$, then $x_0 \in \mathbb{K}_* \setminus \mathbb{J}$. Consider the sets $\mathbb{Y}(x_0)$ and $\mathbb{U}(x_0)$. Suppose that $y \in \mathbb{Y}(x_0)$, then $y = \text{int}((\alpha - x_0)^{-1})$. On the other hand $y \in \mathbb{U}(x_0)$, then either $y \in \mathbb{I}$ and the first item of class $\mathcal{S}$ definition holds or $y = \frac{\varepsilon - 1}{x_0}$. Then

$$\frac{\varepsilon - 1}{x_0} = \text{int}((\alpha - x_0)^{-1}).$$

So the second part of class $\mathcal{S}$ definition holds.

Applying Algorithm 1, we shall give examples of unique factorization domains $\mathbb{K}$ from the class $\mathcal{S}$ (assuming that $\mathbb{K}$ is equipped with proper norm and fractional part).

Example 2. Let $\mathbb{K} = \mathbb{Z}$, $\upsilon(a) = |a|\ \forall a \in \mathbb{Z}_*$, $\text{fr}(\alpha) = \alpha - [\alpha + 1/2]\ \forall \alpha \in \mathbb{Q}$.

1. $\mathbb{J} = \{x \in \mathbb{Z} \big| |x| > 1\}$;
2. $\mathbb{Y}(1) = \{-2, -1\}$, $\mathbb{Y}(-1) = \{1, 2\}$;
3. $\mathbb{U}(1) = \{-2, -1, 0, 1\}$, $\mathbb{U}(-1) = \{-1, 0, 1, 2\}$;
4. $\mathbb{Y}(1) \subseteq \mathbb{U}(1)$, $\mathbb{Y}(-1) \subseteq \mathbb{U}(-1)$. Hence, $\mathbb{Z} \in \mathcal{S}$.

Example 3. Let $\mathbb{K} = \mathbb{P}[t]$, $\mathbb{P}$ is a field, $\upsilon(f) = \deg f\ \ \forall f \in \mathbb{P}[t]$, $\text{fr}(m(t)/n(t)) = r(t)/n(t)$, $m(t) \equiv r(t) (\text{mod}\ n(t))$, $\deg r < \deg n$, for any $m(t)/n(t) \in \mathbb{P}(t)$.

1. $\mathbb{J} = \mathbb{K}_*$;
2. The set $\mathbb{K}_* \backslash \mathbb{J}$ is empty, so $\mathbb{P}[t] \in \mathcal{S}$.

Example 4. Let $\mathbb{K} = \mathbb{Z}[t]$, $\upsilon(f) = \deg f\ \ \forall f \in \mathbb{Z}[t]$. Define the fractional part in $\mathbb{F} = \mathbb{Z}(t)$ by the following. Let the map $\mathcal{A} : \mathbb{F}/\mathbb{K} \to \mathbb{F}$ be defined as $\mathcal{A}(\mathbb{A}) = m(t)/n(t)$, where $\mathbb{A} = \{m(t)/n(t) + q(t) | q(t) \in \mathbb{Z}[t]\}$. For any $\mathbb{A} \in \mathbb{F}/\mathbb{K}$, $\alpha \in \mathbb{A}$ set $\text{int}(\alpha) = r(t)$, $\text{fr}(\alpha) = \mathcal{A}(\mathbb{A}) - r(t)$, where $r(t) \in \mathbb{Z}[t]$, $\lim_{t \to +\infty} \left| \frac{\mathcal{A}(\mathbb{A}) - r(t)}{\mathcal{A}(\mathbb{A}) - p(t)} \right| \leq 1\ \forall p(t) \in \mathbb{Z}[t]$.

1. $\mathbb{J} \supseteq \{f \in \mathbb{Z}[t] | \deg f > 0 \text{ or } |f(t)| \equiv |x_0| > 2\}$.

Let's prove it. Take arbitrary $\mathbb{A} \in \mathbb{F}/\mathbb{K}$ and $\alpha = m(t)/n(t) \in \mathbb{A}$, $\alpha = \text{fr}(\alpha)$.

Firstly consider the case $\deg m > \deg n$. Let's show that $\text{int}((\alpha - x_0)^{-1}) = 0$ for any $x_0 \in \mathbb{Z}[t]$. Since $\alpha = \text{fr}(\alpha)$, so for any $x_0 \in \mathbb{Z}[t]$ the following holds $\deg m \leq \deg(m - nx_0)$. Suppose that $\text{int}((\alpha - x_0)^{-1}) = r(t) \not\equiv 0$ for some $x_0 \in \mathbb{Z}[t]$. Then $\text{fr}((\alpha - x_0)^{-1}) = \frac{n - r(m - nx_0)}{m - nx_0}$. Since $\deg n < \deg m \leq \deg(m - nx_0)$, so $\deg n < \deg(n - r(m - nx_0))$, but the last one contradicts with the definition of fractional part.

Let $\deg m \leq \deg n$. Let's show that $\text{int}((\alpha - x_0)^{-1}) = 0$ for any $x_0 \in \mathbb{Z}[t]$, $\deg x_0 > 0$. Suppose the contrary, i.e., $\text{int}((\alpha - x_0)^{-1}) = r(t) \not\equiv 0$ for some $x_0 \in \mathbb{Z}[t]$, $\deg x_0 > 0$. Since $\deg(m - nx_0) > \deg n$, so $\deg n < \deg(n - r(m - nx_0))$, that contradicts with the definition of fractional part.

Let's prove that $\text{int}((\alpha - x_0)^{-1}) = 0$ for any $x_0 \in \mathbb{Z}[t]$, $x_0(t) \equiv c \in \mathbb{Z} \backslash \{0, \pm 1, \pm 2\}$. Suppose that there exists $c \in \mathbb{Z}$, $|c| > 2$, such that $\text{int}((\alpha - x_0)^{-1}) = r(t) \not\equiv 0$. If $\deg m < \deg n$, then $\deg n <$

$\deg(n-r(m-nc))$ or $r=const.$, hence, $\lim_{t\to+\infty}\left|\frac{n(t)-r(m(t)-n(t)c)}{n(t)}\right|=|1+rc|\geq 2$, that contradicts with the definition of fractional part. So, we have $\deg m=\deg n$. In view of $\alpha=\mathrm{fr}(\alpha)$ and $\deg m=\deg n$ we obtain that $\lim_{t\to+\infty}\left|\frac{m(t)}{n(t)}\right|\leq 0.5$. If $\deg r>0$, then $\deg n<\deg(n-r(m-nc))$, a contradiction. So $r=const.$ and

$$\lim_{t\to+\infty}\left|\frac{n(t)-r(m(t)-n(t)c)}{n(t)}\right|\geq |1+rc|-|r|/2\geq |r|(|c|-1/2)-1\geq\frac{3}{2},$$

that contradicts with the definition of fractional part.

So $\mathbb{J}\supseteq\{f\in\mathbb{Z}[t]|\deg f>0 \text{ or } |f(t)|\equiv|x_0|>2\}$. If $x_0\equiv\pm 2$, then $\mathrm{int}((\alpha-x_0)^{-1})=r(t)\not\equiv 0$ iff $\deg m=\deg n$ and $r(t)\equiv\pm 1$, that implies $\pm 2\in\mathbb{J}$. It's easy to see that $0,\pm 1\notin\mathbb{J}$.

2. $\mathbb{K}_*\backslash\mathbb{J}\subseteq\{\pm 1\}$;

3. $\mathbb{Y}(1)=\{-2,-1\}$, $\mathbb{Y}(-1)=\{1,2\}$;

4. $\mathbb{U}(1)=\{-2,-1,0,1\}$, $\mathbb{U}(-1)=\{-1,0,1,2\}$. Hence, $\mathbb{Z}[t]\in\mathcal{S}$.

Example 5. Let $\mathbb{K}$ be a Euclidean domain such that for any $a,b\in\mathbb{K}$ the following holds $a|b$ or $b|a$ (e.g., $\mathbb{K}$ is one of the following domains: arbitrary field $\mathbb{P}$, the ring of formal power series $\mathbb{P}[[t]]$ over a field $\mathbb{P}$ or the ring $\mathbb{Q}_p$ of all rational numbers $p^k\frac{m}{n}$, where $k\in\mathbb{N}\cup\{0\}$, the numbers m, $n\in\mathbb{Z}$, p are pairwise coprime, p is a fixed prime number). In this case $\mathbb{F}=\mathbb{K}\cup\{1/a|a\in\mathbb{K}_*\backslash\mathbb{I}\}$.

1. Let's prove that $\mathbb{J}=\mathbb{K}_*$.

Take an arbitrary $\alpha\in\mathbb{F}_1^*$, then there exists $b\in\mathbb{K}_*\backslash\mathbb{I}$ such that $\alpha=1/b$. Let $x\in\mathbb{K}_*$. Let's prove that $\mathrm{int}((\alpha-x)^{-1})=(\alpha-x)^{-1}$. We have $(\alpha-x)^{-1}=\frac{b}{1-bx}$. Suppose that $\mathrm{fr}(\frac{b}{1-bx})\neq 0$, that is equivalent to $\frac{b}{1-bx}=\frac{1}{c}$ for some $c\in\mathbb{K}_*\backslash\mathbb{I}$. Since the elements b and $1-bx$ are coprime, so $b\in\mathbb{I}$. Hence, we have $\alpha-x=b^{-1}-x\in\mathbb{K}$, it means that $\alpha\in\mathbb{K}$, but this contradicts with the condition $\alpha\in\mathbb{F}_1^*$. So, we have $x\,\mathrm{int}((\alpha-x)^{-1})+1=\frac{1}{1-bx}$. Suppose that $1-bx\in\mathbb{K}_*\backslash\mathbb{I}$. Since the elements b and $1-bx$ are coprime, so $b|(1-bx)$. Hence, $b\in\mathbb{I}$. The last one implies $\alpha-x=b^{-1}-x\in\mathbb{K}$, but this contradicts with the condition $\alpha\in\mathbb{F}_1^*$. So, we get $1-bx\in\mathbb{I}$. That's why $x\,\mathrm{int}((\alpha-x)^{-1})+1\in\mathbb{I}$.

2. The set $\mathbb{K}_*\backslash\mathbb{J}$ is empty, so $\mathbb{K}\in\mathcal{S}$.

Let us give an example of UFD that does not belong to $\mathcal{S}$ but belongs to $\mathcal{T}$.

Example 6. Let $\mathbb{K}=\mathbb{Z}[i]$. Let the norm in $\mathbb{Z}[i]$ and the fractional part in $\mathbb{Q}[i]$ be defined by relations (2), (3). The domain $\mathbb{Z}[i]$ doesn't belong to the class $\mathcal{S}$. Indeed, choose $\alpha=\frac{9-4i}{20}$, $x=1$, then $\mathrm{int}((\alpha-x)^{-1})=-2+i\notin\mathbb{I}\cup\{0\}$ and $x\,\mathrm{int}((\alpha-x)^{-1})+1=-1+i\notin\mathbb{I}$.

Let us show that $\mathbb{K}\in\mathcal{T}$. It's easy to see that $\mathbb{F}_1=\{z\in\mathbb{C}|Re(z),Im(z)\in\mathbb{Q}\cap[-1/2,1/2[\}$. Take $D_{\mathbb{K}}=3$ in the definition of the set $\mathcal{T}$.

Let's check assumption (1) of the definition of the set $\mathcal{T}$. Take arbitrary $x_0\in\mathbb{Z}[i]\setminus\{0\}$ and $\alpha\in\mathbb{F}_1^*$. Denote $b=\mathrm{int}((\alpha-x_0)^{-1})$. Let p be a number from assumption (1) of the definition of the set $\mathcal{T}$. If $\upsilon(x_0)>5$, then for $p=1$ we have $\beta_1=\alpha$. If $b\in\mathbb{I}\cup\{0\}$, then for $p=1$ we have $\beta_1=\mathrm{fr}((\alpha-x_0)/(bx_0+1-\alpha))$, then $\beta_2=\alpha$. In further we suppose that $b\notin\mathbb{I}\cup\{0\}$ and $\upsilon(x_0)\leq 5$. It's easy to obtain that $\upsilon(x_0)\in\{1,2\}$. It is sufficient to consider only cases $x_0=1$ and $x_0=1+i$ (since for any x_0 with $\upsilon(x_0)\in\{1,2\}$ there exists an element $\varepsilon\in\mathbb{I}$ such that $x_0=\varepsilon$ or $x_0=(1+i)\varepsilon$).

Let $x_0=1+i$, then $b=-1+i$. If we set $p=1$, then we get

$$\beta_1=\mathrm{fr}((\alpha-(1+i))/(\alpha(1-i)-1)),\ \beta_2=\alpha^{-1}.$$

Let $x_0=1$. Then $b\in\{-2,-1\pm i,-2\pm i\}$.

If $b=-2$, then for $p=1$ we get

$$\beta_1=\mathrm{fr}((\alpha-1)/(2\alpha-1)),\ \beta_2=\alpha^{-1}.$$

Let $b=-1\pm i$, then for $p=1$ we have

$$\beta_1=\mathrm{fr}((\alpha-1)/(\alpha(1\mp i)\pm i)),\ \beta_2=\alpha^{-1}.$$

Let $b = -2 + i$. Consider the element

$$\beta = \omega(\mathrm{fr}((\alpha - 1)^{-1})) = \mathrm{fr}((\alpha - 1)/(\alpha(2 - i) - (1 - i))).$$

Note that

$$\gamma = \mathrm{int}((\alpha - 1)/(\alpha(2 - 1) - (1 - i))) \in \{1 + i, 1 + 2i, 2 + i, 2 + 2i\}.$$

If $\gamma = 1 + i$, then

$$\beta = (1 - \alpha(2 + i))/(\alpha(2 - i) - (1 - i)).$$

Take $p = 2$, then we have

$$\beta_1 = \omega^{(2)}(\mathrm{fr}((\alpha - 1)^{-1})) = \mathrm{fr}((\alpha(2 - i) - (1 - i))/(1 - \alpha(2 + i))),$$
$$\beta_2 = \alpha/(1 - \alpha(2 + i)),\ \beta_3 = \alpha^{-1}.$$

If $\gamma = 1 + 2i$, then

$$\beta = ((2 + i) - \alpha(3 + 3i))/(\alpha(2 - i) - (1 - i)).$$

Take $p = 2$, then we have

$$\beta_1 = \omega^{(2)}(\mathrm{fr}((\alpha - 1)^{-1})) = \mathrm{fr}((\alpha(2 - i) - (1 - i))/((2 + i) - \alpha(3 + 3i))),$$
$$\beta_2 = \alpha/(1 - \alpha(2 + i)),\ \beta_3 = \alpha^{-1}.$$

If $\gamma = 2 + i$, then

$$\beta = ((2 - i) - 4\alpha)/(\alpha(2 - i) - (1 - i)).$$

Take $p = 2$, then we get

$$\beta_1 = \omega^{(2)}(\mathrm{fr}((\alpha - 1)^{-1})) = \mathrm{fr}((\alpha(2 - i) - (1 - i))/((2 - i) - 4\alpha)),$$
$$\beta_2 = \alpha/(1 - \alpha(2 + i)),\ \beta_3 = \alpha^{-1}.$$

If $\gamma = 2 + 2i$, then

$$\beta = (3 - \alpha(5 + 2i))/(\alpha(2 - i) - (1 - i)).$$

Take $p = 3$, then we have

$$\beta_1 = \omega^{(3)}(\mathrm{fr}((\alpha - 1)^{-1})) = \mathrm{fr}((3 - \alpha(5 + 2i))/(2 - 2i - \alpha(5 - 2i))),$$
$$\beta_2 = \alpha/(1 - \alpha(2_i),\ \beta_3 = \alpha^{-1}.$$

The case $b = -2 - i$ is analogous to the case $b = -2 + i$.

Let's check assumption (2) of the definition of the set $\mathcal{T}$. Take arbitrary $x_0 \in \mathbb{Z}[i] \setminus \{0\}$ and $\alpha \in \mathbb{F}_1^*$ such that $\omega(\mathrm{fr}((\alpha - x_0)^{-1})) = 0$. Since at all cases, excepting $x_0 = 1$, $b = -2 \pm i$, it is possible to get $D_{\mathbb{K}} = 2$ instead of $D_{\mathbb{K}} = 3$, so it is sufficient to consider only the case $x_0 = 1$, $b = -2 \pm i$. Let $b = -2 + i$, then the condition $\omega(\mathrm{fr}((\alpha - x_0)^{-1})) = 0$ implies the inclusion $\alpha \in \{1/(2 + i), (2 + i)/(3 + 3i), (2 - i)/4, 3/(5 + 2i)\}$. For the first, second and third elements the following holds $\omega^{(2)}(\alpha) = 0$, for the fourth element the condition $\alpha = \mathrm{fr}(\alpha)$ fails. The case $b = -2 - i$ is analogous to the case $b = -2 + i$.

Let's give a general method (semi-decision algorithm) to prove that $\mathbb{K} \in \mathcal{T}$.

Algorithm 2.

Step 1. Choose positive integer $D_{\mathbb{K}}$ and M.

Step 2. Construct the set

$$\mathbb{J} = \left\{ x_0 \in \mathbb{K} \middle| \operatorname{int}\left(\frac{1}{\alpha - x_0}\right) \in \mathbb{I} \cup \{0\} \forall \alpha \in \mathbb{F}^* \right\}.$$

Step 3. Create a list $\mathbb{L}$ that will contain elements of $\mathbb{K}^r$ where $r \in \{1, \dots, D_{\mathbb{K}} - 1\}$.

Step 4. $\mathbb{L} = \mathbb{K}^* \setminus \mathbb{J}$. We will save all elements of $\mathbb{L}$ the number of elements of which is greater than 2 in list $\mathbb{L}_M$.

Step 5. Choose an element $(x_0, \dots, x_l) \in \mathbb{L}$ and delete it.

Step 6. Calculate $\delta = \left(\left(\dots \left((\alpha - x_0)^{-1} - x_1 \right)^{-1} - \dots \right)^{-1} - x_l \right)^{-1}$.

Step 7. Construct

$$\mathbb{A} = \left\{ b \in \mathbb{K} \middle| b = \operatorname{int}(\delta) \right\}.$$

Step 8. For every element x_{l+1} of $\mathbb{A}$ do the following steps.

Step 8.1. Calculate

$$\beta_1 = \omega^{(l+1)} \left(\operatorname{int}((\alpha - x_0)^{-1}) \right) = \operatorname{fr}((\delta - x_{l+1})^{-1}).$$

Step 8.2. Try to find $(\varepsilon_i) \in \mathbb{I}$ and $(a_i), (b_i) \in \mathbb{K}$, $\upsilon(a_i), \upsilon(b_i) \le M$ such that

$$\beta_{i+1} = \frac{1}{\varepsilon_i \beta_i + a_i} + b_i$$

and $\beta_{l+2} = \alpha$ or $\beta_{l+2} = \alpha^{-1}$.

Step 8.3. Switch

1) If such elements were not found and $l + 1 \ge D_{\mathbb{K}}$, then return **choose bigger** $D_{\mathbb{K}}$ **and** M.
2) If such elements were not found and $l + 1 < D_{\mathbb{K}}$, then add $(x_0, \dots, x_l, x_{l+1})$.
3) If such elements were found, then go to the next element in Step 8.

Step 9. Switch

1) If $\mathbb{L}$ is not empty, then go to Step 5.
2) If $\mathbb{L}$ is empty and $D_{\mathbb{K}} < 3$, then return **true**.
3) If $\mathbb{L}$ is empty and $D_{\mathbb{K}} \ge 3$, then go to Step 10.

Step 10. For every $k \in [3, D_{\mathbb{K}}]$ do Steps 11–13.

Step 11. Construct

$$\mathbb{B} = \left\{ \alpha \in \mathbb{F}^* \middle| \omega^{(k-2)} \left\{ \operatorname{fr}\left((\alpha - x_0)^{-1} \right) \right\} = 0 \right\},$$

where ω is calculated using the list $\mathbb{L}_M$.

Step 12. For every $\alpha_0 \in \mathbb{B}$ try to find $(\varepsilon_i) \in \mathbb{I}$ and $(a_i), (b_i) \in \mathbb{K}$, $\upsilon(a_i), \upsilon(b_i) \le M$ such that

$$\beta_{i+1} = \frac{1}{\varepsilon_i \beta_i + a_i} + b_i$$

and $\beta_{k-1} = \alpha$ or $\beta_{k-1} = \alpha^{-1}$, where $\beta_1 = 0$.

Step 13. Switch

1) If such elements were not found, then return **choose bigger** $D_{\mathbb{K}}$ **and** M.
3) If such elements were found and we checked every $x_0 \in \mathbb{L}^*$, then return **true**.

Correctness of Algorithm 2. Suppose that the answer of Algorithm 2 is "Yes". Take arbitrary $x_0 \in \mathbb{K}$. If $x_0 \in \mathbb{J}$, then the triple $(x_0, \alpha, D_{\mathbb{K}})$ is regular for any $\alpha \in \mathbb{F}^*$ and $D_{\mathbb{K}} \in \mathbb{N}$.

Then we want to show that the triple $(x_0, \alpha, D_{\mathbb{K}})$ is regular for any $x_0 \in \mathbb{K}^* \setminus \mathbb{J}$ and $\alpha \in \mathbb{F}^*$. Let us consider the set $\mathbb{L}_1$ of all elements that were put in $\mathbb{L}$. If $(x_0, \dots, x_k) \in \mathbb{L}_1$, $(y_0, \dots, y_l) \in \mathbb{L}_1$ and $x_i = y_i$ for any $i = \overline{1, k}$, $k \le l$, then we will delete $(x_0, \dots, x_k)$ from $\mathbb{L}_1$. Let us fix x_0 and show that

$(x_0, \alpha, D_{\mathbb{K}})$ is regular. It is easy to see that if (x_0, α, k) is regular, then $(x_0, \alpha, k+i)$ is regular for any $i \in \mathbb{N}$.

Let us consider an element $(x_0, \dots, x_l) \in \mathbb{L}_1$. This element generates the set of α such that

$$x_l = \left(\left(\dots \left((\alpha - x_0)^{-1} - x_1 \right)^{-1} - \dots \right)^{-1} - x_{l-1} \right)^{-1}.$$

It is obvious that all such elements of $\mathbb{L}_1$ with fixed x_0 generate $\mathbb{F}^*$. Since the answer of Algorithm 2 is "Yes" we can find sequences from the Algorithm for each element of $\mathbb{L}_1$ with fixed x_0. So the triple $(x_0, \alpha, D_{\mathbb{K}})$ is regular for any x_0, α. And the first part of the definition of the set $\mathcal{T}$ holds.

Suppose that $D_{\mathbb{K}} \geq 3$. Proof of correctness of Steps 10–13 is completely analogous to the proof of correctness of Steps 1–9.

6. Discussion of results

6.1. Theorem 1

Let us show that there exists UFD $\mathbb{K}$ such that $\mathbb{K} \notin \mathcal{T}$ and the Least Remainder DC may not have the minimal length.

Let $\mathbb{K} = \mathbb{Z}[\sqrt{-11}]$, where the norm and fractional part are defined by relations (2) and (3). It is easy to see that the set

$$\{6, -2i\sqrt{11}, 6, -3 + i\sqrt{11}, -1 - i\sqrt{11}, 2, 0\}$$

generates the Least Remainder DC for the pair $(a, b) = (6, -2i\sqrt{11})$. Then $\mathcal{L}_{a,b} = 5$. On the other hand, there exists another division chain for the pair (a, b):

$$\{6, -2i\sqrt{11}, -5 + i\sqrt{11}, 3 + i\sqrt{11}, 2, 0\},$$

hence, $\ell_{a,b} \leq 4 \leq \mathcal{L}_{a,b}$. Consequently, the statement of Theorem 1 fails. Suppose that $\mathbb{Z}[i\sqrt{11}] \in \mathcal{T}$, then, by Theorem 1, we obtain that for any $(c, d) \in \mathbb{K}_* \times \mathbb{K}_*$ the following holds $\ell_{c,d} = \mathcal{L}_{c,d}$, a contradiction. By analogous arguments, Lemma 1 also fails for UFD $\mathbb{Z}[\sqrt{-11}]$.

6.2. Theorem 2

Let us give an example of UFD for which Theorem 2 fails. Let $\mathbb{K} = \mathbb{P}[t]$ be equipped with the norm and fractional part as in Example 3.

Let n be an arbitrary natural number. Define the sequence

$$g_{k+2}(t) = t g_{k+1}(t) + g_k(t), k \geq 1, g_1(t) = 1, g_2(t) = t.$$

It's obvious that $\deg g_k = k - 1$. Let $a(t) = g_{n+1}(t)$, $b(t) = g_n(t)$, then $\mathcal{L}_{a(t),b(t)} = n$. Since $l_n(\mathbb{P}[t]) \leq n$, so we obtain that $l_n(\mathbb{P}[t]) = n$.

For any $n \in \mathbb{N}$ there exists an element $\alpha \in \mathbb{F}_1$ with $|\alpha| = n/(n+1)$, hence $\Lambda_{\mathbb{K}} \geq 1$. Since $\mathbb{P}[t]$ is a Euclidean domain, then, by Theorem 2, we have $\Lambda_{\mathbb{K}} \leq 1$ and $l_n(\mathbb{P}[t]) \leq n$. So $\Lambda_{\mathbb{K}} = 1$. Consequently, the condition $\Lambda_{\mathbb{K}} \in [0, 1)$ in Theorem 2 can't be replaced by the condition $\Lambda_{\mathbb{K}} \in [0, 1]$.

6.3. Theorem 3

It is possible to deduce from the proof of Proposition 1 the explicit upper bounds for characteristic $\Lambda_{\mathbb{K}}$ in case of imaginary quadratic Euclidean domains: $\Lambda_{\mathbb{Z}[i]} \leq 1/2$, $\Lambda_{\mathbb{Z}[i\sqrt{2}]} \leq 3/4$, $\Lambda_{\mathbb{Z}[i\sqrt{3}]} \leq 7/16$, $\Lambda_{\mathbb{Z}[i\sqrt{7}]} \leq 11/16$, $\Lambda_{\mathbb{Z}[i\sqrt{11}]} \leq 15/16$.

Remark 3. Dupre (1846) (see Bach and Shallit, 1996, p. 80) has showed that the maximal number of divisions of the Least Remainder DC over all pairs $(a, b) \in \mathbb{Z} \times \mathbb{Z}$ with $n \geq |a| \geq |b| > 0$ is equal to

$[\log_\theta n] + M_n$, where $\theta = 1 + \sqrt{2}$, $M_n \in \{0, 1\}$, and the maximal number of divisions is achieved for two largest numbers $f_k, f_{k+1} \in [1, n]$, where $f_1 = 0,\ f_2 = 1,\ f_{k+2} = 2f_{k+1} + f_k,\ k \geq 1$. Rolletschek (1986) has found the maximal number of divisions of the Least Remainder DC in the ring $\mathbb{Z}[i]$ of Gaussian integers over all pairs $(a, b) \in \mathbb{Z}[i] \times \mathbb{Z}[i]$ with $n \geq |a| \geq |b| > 0$, this number is equal to $[\log_\psi n^2] + T_n$, where $\psi = 2 + \sqrt{3},\ T_n \in \{0, 1, 2\}$.

6.4. Application to optimization of the algorithm for solving linear Diophantine equations

Consider a linear Diophantine equation

$$ax + by = c, \tag{8}$$

in variables $x, y \in \mathbb{K}$, $\mathbb{K}$ is a UFD with a norm υ, where $a, b, c \in \mathbb{K}$, $a, b \neq 0$. Suppose that there exists the Least Remainder DC

$$\mathcal{g}_{a,b} = \mathcal{D}_{a,b}(q_1, \ldots, q_k) = (r_{-1}, r_0, r_1, \ldots, r_{k-1}, r_k)$$

for the pair (a, b). We get $\gcd(a, b) = r_{k-1}$, $a/b = [q_1 : q_2 : \ldots : q_k]$. If r_{k-1} doesn't divide the right-hand side c of Eq. (8), then there are no solutions to Eq. (8). Let $r_{k-1} | c$. If

$$[q_1 : q_2 : \ldots : q_k] = P_k/Q_k, [q_1 : q_2 : \ldots : q_{k-1}] = P_{k-1}/Q_{k-1}$$

are the successive fractions for the continued fraction $[q_1 : q_2 : \ldots : q_k]$, then the following relation holds $P_k Q_{k-1} - Q_k P_{k-1} = (-1)^k$ (see, e.g., Davenport, 1965, p. 86). Using the last one, we get a formula for solutions to Eq. (8)

$$\begin{cases} x = (-1)^k Q_{k-1} P_k c/a + Q_k t, \\ y = (-1)^{k-1} P_{k-1} Q_k c/b - P_k t, \end{cases} \qquad t \in \mathbb{K}.$$

If $\mathbb{K} \in \mathcal{T}$, then the length k of the continued fraction $[q_1 : q_2 : \ldots : q_k]$ for a/b is minimal. If $\Lambda_{\mathbb{K}} < 1$, then $k \leq C \log(\upsilon(a) + \upsilon(b))$, where the constant C doesn't depend on the coefficients a and b.

Acknowledgement

Authors thank reviewers for careful reading of the paper and valuable remarks.

References

Bach, E., Shallit, J., 1996. Algorithmic Number Theory. MIT Press, Cambridge, MA.
Davenport, H., 1965. The Higher Arithmetic. An Introduction to the Theory of Numbers. Nauka, Moscow.
Kaltofen, E., Rolletschek, H., 1985. Arithmetic in quadratic fields with unique factorization. In: Proceedings of the EUROCAL'85 Conference on Computer Algebra. In: Lect. Notes Comput. Sci., vol. 204. Springer, pp. 279–288.
Lazard, D., 1977. Le meilleur algorithme d'euclide pour $k[x]$ et z. Computes Rendus Acad. Sci. Paris 284, 1–4.
Rolletschek, H., 1986. On the number of divisions of the euclidean algorithm applied to gaussian integers. J. Symb. Comput., 261–291.
Rolletschek, H., 1990. Shortest division chains in imaginary quadratic number fields. J. Symb. Comput., 321–354.
Selfridge, J., Lacampagne, C., Eggleton, R., 1992. Euclidean quadratic fields. Am. Math. Mon. 99, 829–837.
Vaskouski, M., Kondratyonok, N., 2013. Finite generalized continued fractions in euclidean domains. Vestnik BSU, 117–123.