On diophantine properties of radix representations in algebraic number fields

Attila Pethő

Abstract. In these notes we investigate elements with special patterns in their representations in number systems in algebraic number fields. We concentrate on periodicity and on the representation of rational integers. We prove under natural assumptions that there are only finitely many S-integers whose representation is periodic with a fixed period. We prove that the same holds for the set of values of polynomials at rational integers.

1. Introduction

Let $\mathbb{K}$ denote an algebraic number field with ring of integers $\mathbb{Z}_\mathbb{K}$. Let $\gamma \in \mathbb{Z}_\mathbb{K}$ and $\mathcal{D} \subset \mathbb{Z}$ be a complete residue system modulo γ containing zero. Then the pair $(\gamma, \mathcal{D})$ is called a *number system in* $\mathbb{Z}_\mathbb{K}$. With the special choice $\mathcal{D}_\gamma = \{0, 1, , \dots, |N(\gamma)| - 1\}$, which is a complete residue system modulo γ, $(\gamma, \mathcal{D}_\gamma)$ will be called *canonical number system.*

The element $\beta \in \mathbb{Z}_\mathbb{K}$ is representable in $(\gamma, \mathcal{D})$ if either $\beta = 0$ or there exist $L = L(\gamma) \in \mathbb{Z}$ and $b_0, b_1, \dots, b_L \in \mathcal{D}, b_L \neq 0$ such that

$$\beta = \sum_{i=0}^{L} b_i \gamma^i. \tag{1.1}$$

To fix the terminology γ will be called the *basis*, $\mathcal{D}$ the *digit set* of the number system, while $L+1$ the *length* of the representation. Plainly, if such a representation exists then it is unique. The set of representable elements will be denoted by $R(\gamma, \mathcal{D})$. If $R(\gamma, \mathcal{D}) = \mathbb{Z}_\mathbb{K}$ then we say that $(\gamma, \mathcal{D})$ has the *finiteness property.* For $\beta = 0$ we set $(0)_{(\gamma,\mathcal{D})} = 0$, and if β admits the representation (1.1) then we put $(\beta)_{(\gamma,\mathcal{D})} = b_0 b_1 \dots b_L$, which are finite words over the alphabet $\mathcal{D}$. If the number system is fixed then we will simply write $(\beta)_\gamma$ instead of $(\beta)_{(\gamma,\mathcal{D})}$.

With the choices $\mathbb{K} = \mathbb{Q}, \gamma = 10$ and $\mathcal{D}_{10} = \{0, 1, \dots, 9\}$ we obtain our familiar decimal system. In this number system only the non-negative integers are representable; to represent the negative integers we need the sign, i.e. $\mathbb{Z} = R(10, \mathcal{D}_{10}) \cup (-R(10, \mathcal{D}_{10}))$, hence the decimal system does not admit the finiteness

2010 *Mathematics Subject Classification.* 11A63, 11D57, 11J72.

Key words and phrases. Number system, radix representation, periodic words, repunit, unit equations.

property. In 1885 Grünwald [6] showed among others that $\mathbb{Z} = R(-10, \mathcal{D}_{10})$, i.e, with the application of negative basis one could forget the sign. (In return the algorithms for addition, multiplication and division with rest become more complicated.)

Since the middle of the last century many generalization appeared, see Knuth [10], Penney [12], B. Kovács [11], Pethő [13], Pethő and Thuswaldner [16] and Evertse, Győry, Pethő and Thuswaldner [4]. Because of space limitation we cannot detail the rich and expanding theory of number systems, but refer to the good overview of Kirschenhofer and Thuswaldner [9].

The investigation of integers with simple or special decimal expansion fascinate people, and lead often to hard diophantine problems. For example it is still an unsolved problem to determine all integers, which are repunits in two different bases. An integer n is called repunit in the integer base $g \geq 2$, if $(n)_g = 1^\ell$ for some $\ell \geq 1$. For details see Section 5.

In these notes we concentrate on elements with special patterns in their representations in number systems. We concentrate on periodicity and on the representation of rational integers. In Section 2 we investigate the representations of S-integers. We prove under natural assumptions that there are only finitely many S-integers whose $(\gamma, \mathcal{D})$-representation is periodic with a fixed period, see Theorem 2.2. In the next section we prove that the same holds for the set of values of polynomials at rational integers. Moreover the corresponding Theorem 3.1 is effective. In Section 4 we fix a word $w \in \mathbb{Z}^*$ and $k \geq 2$ and present a procedure, which finds all essentially different number systems $(\gamma, \mathcal{D})$ of number fields of degree k and all rational integers n such that $(n)_{(\gamma,\mathcal{D})} = w$. We show that if $k = L(w), L(w) - 1$ then, under natural assumptions, there are infinitely many such number systems and integers. Otherwise our procedure indicates that there are only finitely many such objects. Finally, in Section 5 we specialize our former results to repunits.

Our results mirrors, the intuitive fact that both S-integers and rational integers are minorities among the integers of an algebraic number field. In contrast the asymptotic formula of Dumont, Grabner and Thomas [2] for the frequency of occurrences of finite words in the representation of rational integers in number systems of algebraic number fields shows some regularity.

In the sequel we will use frequently that if the number system $(\gamma, \mathcal{D})$ in $\mathbb{Z}_\mathbb{K}$ admits the finiteness property then $|\gamma^{(j)}| > 1$ holds for all conjugates of γ. This fact was proved first by Vince [20], and rediscovered several times, see e.g. Kovács [11] and Pethő [13].

2. Periodic S-integers

For an alphabet (set) A denote A^* the set of finite words on A including the empty word λ. The set A^* is equipped with the *concatenation* operation. For $w \in \mathcal{A}^*$ and $k \geq 1$ we write $w^k = w \dots w$, the k-times concatenation of w. This definition is extended to $k = 0$ by setting $w^0 = \lambda$ for all $w \in A^*$. If a word can be written as $w_1 w^k$ then it is called *periodic*, furthermore w_1 is called its *preperiod* and w its *period*. In this section we are dealing with elements having periodic representation in a number system $(\gamma, \mathcal{D})$. For any given $w, w_1 \in \mathcal{D}^*$ there are infinitely many elements whose representation has preperiod w_1 and period w. They are the elements with $(\beta)_\gamma = w_1 w^k$ for some $k \geq 0$. We prove that some sets have finite intersection with this set.

S-unit equations play a vital role in our proofs. Now we define them. For an algebraic number field $\mathbb{K}$ denote $M_{\mathbb{K}}$ its set of places. Let $S \subset M_{\mathbb{K}}$ be finite including all archimedean places, and denote $\mathbb{Z}_S$ the set of *S-integers* of $\mathbb{K}$, i.e., the set of those elements $\alpha \in \mathbb{K}$ with $|\alpha|_v \leq 1$ for all $v \in M_{\mathbb{K}} \setminus S$. The set $\mathbb{Z}_S$ forms a ring, its group of units is denoted by $\mathbb{Z}_S^*$.

Consider the *weighted S-unit equation*

$$\alpha_1 X_1 + \cdots + \alpha_s X_s = 1, \tag{2.1}$$

where $s \geq 2$, $\alpha_1, \ldots, \alpha_s$ are non-zero elements of $\mathbb{K}$ and the solutions $x_1, \ldots, x_s$ belong to $\mathbb{Z}_S^*$. A solution $x_1, \ldots, x_s$ of (2.1) is called *degenerate* if there exists a proper subset I of $\{1, \ldots, s\}$ such that $\sum_{i \in I} \alpha_i x_i = 0$. The next theorem was proved by Evertse [**3**] and independently by van der Poorten and Schlickewei [**19**], see also [**5**].

Theorem 2.1. *Equation* (2.1) *has only finitely many non-degenerate solutions in $x_1, \ldots, x_s \in \mathbb{Z}_S^*$.*

For a finite set $S \subset \mathbb{Z}_K$ we will denote by $\Gamma(S), \Gamma^*(S)$ the multiplicative semigroup, the multiplicative group generated by S respectively. Let $0 \notin \mathcal{A}, \mathcal{B} \subset \mathbb{Z}_{\mathbb{K}}$ be finite. Put

$$S(\mathcal{A}, \mathcal{B}, s) = \{\alpha_1\mu_1 + \cdots + \alpha_s\mu_s \ : \ \alpha_j \in \mathcal{A}, \mu_j \in \Gamma(\mathcal{B})\}.$$

For example, if $\mathbb{K} = \mathbb{Q}, \mathcal{A} = \{1\}, \mathcal{B} = \{2, 3\}$ then

$$S(\mathcal{A}, \mathcal{B}, 2) = \{2^a 3^b + 2^c 3^d \ : \ a, b, c, d \geq 0\}.$$

The elements $\alpha_1, \ldots, \alpha_s \in \mathbb{K}$ are called *multiplicatively dependent* if there exist $u_1, \ldots, u_s \in \mathbb{Z}, u_1 \neq 0$ such that $\alpha_1^{u_1} \cdots \alpha_s^{u_s} = 1$. Otherwise they are called *multiplicatively independent.*

Now we are in the position to formulate our first result.

Theorem 2.2. *Let $(\gamma, \mathcal{D})$ be a number system with finiteness property in $\mathbb{Z}_{\mathbb{K}}$, and $w, w_1 \in \mathcal{D}^*$. Let $0 \notin \mathcal{A}, \mathcal{B} \subset \mathbb{Z}_{\mathbb{K}}$ be finite such that the elements of $\{\gamma\} \cup \mathcal{B}$ are multiplicatively independent. Then there are only finitely many $U \in S(\mathcal{A}, \mathcal{B}, s)$ such that $(U)_\gamma = w_1 w^k$.*

Remark 2.3. *This is the finite version of Corollary 2.3 of* [**15**]. *More precisely we derived Corollary 2.3 of* [**15**] *from Theorem 2.2 without explicitly stating it. We realized this fact only after the publication of* [**15**]. *Because, by our opinion, Theorem 2.2 is interesting itself we decided to formulate it here.*

Proof. Let $w_1 \in \mathcal{D}^*$ be given. By unicity of expansions there is at most one U with $(U)_\gamma = w_1$. Thus our statement is true if $w = \lambda$. From here on we assume $w \neq \lambda$.

Let $w = d_0 \ldots d_{h-1}$ and $q = d_0 + d_1\gamma + \ldots + d_{h-1}\gamma^{h-1}$. Set $q_0 = 0$ if $w_1 = \lambda$, and $q_0 = f_0 + f_1\gamma + \ldots + f_{g-1}\gamma^{g-1}$ provided $w_1 = f_0 \ldots f_{g-1}$. Finally let $U = \alpha_1\mu_1 + \cdots + \alpha_s\mu_s$, $\alpha_j \in \mathcal{A}, \mu_j \in \Gamma(\mathcal{B})$. It is enough to show that if $(U)_\gamma = w_1 w^k$ then k is bounded. Indeed, if k is bounded then $w_1 w^k$ can take finitely many values, but by our first claim $(U)_\gamma = v$, $v \in \mathcal{D}^*$ holds for at most one $U \in S(\mathcal{A}, \mathcal{B}, s)$.

Now assume that $(U)_\gamma = w_1 w^k$ holds for some $k > 0$. It means nothing else then

$$\begin{aligned}
\alpha_1\mu_1 + \cdots + \alpha_s\mu_s &= q_0 + \gamma^g \sum_{i=0}^{k-1} \gamma^{ih} \sum_{j=0}^{h-1} d_j \gamma^j \\
&= q_0 + \gamma^g \sum_{i=0}^{k-1} q\gamma^{ih} \\
&= q_0 + q\gamma^g \frac{\gamma^{hk}-1}{\gamma^h - 1} \\
&= \frac{q\gamma^g}{\gamma^h-1}\gamma^{hk} + q_0 - \frac{q\gamma^g}{\gamma^h-1}.
\end{aligned}$$

Setting

$$\alpha_{s+1} = \frac{q\gamma^g}{\gamma^h-1}, \qquad \alpha_{s+2} = q_0 - \frac{q\gamma^g}{\gamma^h-1}$$

we get the equation

$$\alpha_1\mu_1 + \cdots + \alpha_s\mu_s = \alpha_{s+1}\gamma^{hk} + \alpha_{s+2}.$$

By the fact mentioned at the end of the Introduction $|\gamma| > 1$, hence $\gamma^h \neq 1$ and $\alpha_{s+1}, \alpha_{s+2}$ are well defined. Plainly $\alpha_j \in \mathbb{K}, j = 1, \ldots, s+2$ and $\alpha_j \neq 0, k = 1, \ldots, s$ by assumption. It is easy to see that $\alpha_{s+1} \neq 0$ holds too.

In the sequel we have to distinguish the cases $\alpha_{s+2} = 0$ and $\alpha_{s+2} \neq 0$. As the argumentation is similar in both cases we detail here only the case $\alpha_{s+2} \neq 0$. Dividing by $\alpha_{s+2} \neq 0$ and letting $\hat{\alpha}_j = \alpha_j/\alpha_{s+2},\ j = 1, \ldots, s$ and $\hat{\alpha}_{s+1} = -\alpha_{s+1}/\alpha_{s+2}, \mu_{s+1} = \gamma^{hk}$ we get

$$\hat{\alpha}_1\mu_1 + \cdots + \hat{\alpha}_{s+1}\mu_{s+1} = 1. \tag{2.2}$$

Let S be the set of places of $\mathbb{K}$, which includes the archimedean ones, and those which correspond to prime ideal divisors of γ or some element of $\mathcal{B}$. Plainly S is a finite set. Set $\Gamma_1 = \Gamma^*(\gamma, \mathcal{B})$, Then the elements of Γ_1 are S-units and, hence, (2.2) an S-unit equation. If there are infinitely many $U \in S(\mathcal{A}, \mathcal{B}, s)$ such that $(U)_\gamma = w_1 w^k$ then k has to take arbitrary large values and, hence, (2.2) has infinitely many solutions in $(\mu_1, \ldots, \mu_{s+1}) \in \Gamma^*(\mathcal{B})^s \times \Gamma_1 \subset \Gamma_1^{s+1}$, which means that γ appears solely in μ_{s+1} and its exponents in the solutions are not bounded. In the sequel we derive from (2.2) new equations in less unknowns such that all but one coordinate of the solution vectors belong to $\Gamma^*(\mathcal{B})$, only one - μ_{s+1} - belongs to Γ_1.

As (2.2) has infinitely many solutions in Γ_1^{s+1}, i.e. in S-units, Theorem 2.1 implies that there is a proper subset $I \subset \{1, \ldots, s+1\}$ such that the equation

$$\sum_{i \in I} \hat{\alpha}_i \mu_i = 0 \tag{2.3}$$

has infinitely many solutions $(\mu_i)_{i \in I} \in \Gamma_1^{|I|}$, where $|I|$ denotes the size of I. We show that there is such a subset which contains $s+1$.

Indeed, assume that $s+1 \notin I$ for all $I \subset \{1, \ldots, s+1\}$ such that the equation (2.3) admits infinitely many solutions $(\mu_i)_{i \in I} \in \Gamma_1^{|I|}$. As the number of such sets is at most 2^s, there is an $\emptyset \neq I \subseteq \{1,\dots,s\}$ such that the equation

$$\sum_{i\in\{1,\dots,s+1\}\setminus I} \hat{\alpha}_i\mu_i = 1 \tag{2.4}$$

is again a S-unit equation of the shape (2.2), but in less summands. Moreover if $(\mu_1,\dots,\mu_{s+1}) \in \Gamma^*(\mathcal{B})\times\Gamma_1$ is a solution of (2.2) such that $\mu_i, i\in I$ satisfy (2.3) then $\mu_i, i\in\{1,\dots,s+1\}\setminus I$ satisfy (2.4), thus it has infinitely many solutions in $(\mu_i)_{i\in\{1,\dots,s+1\}\setminus I} \in \Gamma^*(\mathcal{B})^{s-|I|}\times\Gamma_1$. Assume that I is maximal in the sense that if $I\subset I'\subseteq\{1,\dots,s\}$ then $\sum_{i\in\{1,\dots,s+1\}\setminus I'}\hat{\alpha}_i\mu_i = 1$ has only finitely many solutions in $\mu_i\in\Gamma^*(\mathcal{B})$, $i\in\{1,\dots,s\}\setminus I'$ and $\mu_{s+1}\in\Gamma_1$.

As (2.4) admits infinitely many S-unit solutions $\mu_i\in\Gamma_1, i\in\{1,\dots,s+1\}\setminus I$, Theorem 2.1 implies the existence of $I_1\subset\{1,\dots,s+1\}\setminus I$ such that $\sum_{i\in I_1}\hat{\alpha}_i\mu_i = 0$ has infinitely many solutions $\mu_i\in\Gamma_1,\ i\in I_1$. Thus, by our assumption $s+1\notin I_1$, and as $\mu_{s+1}=\gamma^{hk}$, the equation $\sum_{i\in(\{1,\dots,s+1\}\setminus I)\setminus I_1}\hat{\alpha}_i\mu_i = 1$ has to have infinitely many solutions $\mu_i\in\Gamma_1,\ i\in(\{1,\dots,s+1\}\setminus I)\setminus I_1$. Set $I' = I\cup I_1$. Then $I\subset I'\subseteq\{1,\dots,s\}$ and $(\{1,\dots,s+1\}\setminus I)\setminus I_1 = \{1,\dots,s+1\}\setminus I'$, which contradicts the maximality of I, i.e. $I=\{1,\dots,s\}$.

Hence $\alpha_{s+1}\mu_{s+1} = 1$ holds for infinitely many $\mu_{s+1}=\gamma^{hk}\in\Gamma_1$. This means that $\alpha_{s+1}\gamma^{hk}=1$ holds for infinitely many k. Thus γ is a root of unity, which is impossible because $|\gamma|>1$.

In the sequel we assume $s+1\in I$. By possible renumbering we may assume $I=\{1,\dots,s_1,s+1\}$ with some $1\le s_1<s$. (The case $I=\{s+1\}$ is impossible.) Hence

$$\sum_{i=1}^{s_1}\hat{\alpha}_i\mu_i + \hat{\alpha}_{s+1}\mu_{s+1} = 0$$

has infinitely many solutions in $\mu_i\in\Gamma^*(\mathcal{B}),\ i=1,\dots,s_1,\ \mu_{s+1}\in\Gamma_1$. As the elements of $\mathcal{B}\cup\{\gamma\}$ is multiplicatively independent there is a prime ideal $\wp$ of $\mathbb{Z}_K$, which divides γ, but no elements of $\mathcal{B}$. Dividing this equation by $-\hat{\alpha}_{s_1}\mu_{s_1}$ and setting $\hat{\alpha}_j\leftarrow-\hat{\alpha}_j/\hat{\alpha}_{s_1}, \mu_j\leftarrow\mu_j/\mu_{s_1}, j=1,\dots,s_1-1$ and $\hat{\alpha}_{s_1}\leftarrow-\hat{\alpha}_{s+1}/\hat{\alpha}_{s_1}, \mu_{s_1}\leftarrow\mu_{s+1}/\mu_{s_1}$ we see that $\wp^{hk}$ divides μ_{s_1}, further the obtained equation has the shape (2.2), but with $s_1<s+1$ summands. Moreover it has infinitely many solutions in $(\mu_1,\dots,\mu_{s_1})\in\Gamma^*(\mathcal{B})^{s_1-1}\times\Gamma_1$.

After repeated application of this argument we arrive at $s_1=1$, i.e., an equation $\hat{\alpha}_1\mu_1+\hat{\alpha}_2\mu_2=0$, which has infinitely many solutions in $\mu_1\in\Gamma^*(\mathcal{B})$ and $\mu_2\in\Gamma_1$ such that $\wp^{hk}$ divides μ_2, i.e. the exponent of $\wp$ in μ_2 is not bounded. Dividing by $\hat{\alpha}_1\mu_1$ we obtain an equation of shape $\alpha\mu=1$, which has infinitely many solutions in $\mu\in\Gamma_1$ such that the exponent of $\wp$ in μ is still at least hk, which is not bounded. Fixing one of the solutions, say μ_0, we have that $\mu/\mu_0=1$ holds for infinitely many $\mu\in\Gamma_1$, which is impossible because the elements of $\{\gamma\}\cup\mathcal{B}$, which generate Γ_1 are multiplicatively independent. □

3. Periodic rational integers

The elements of $(\mathcal{A},\mathcal{B},s)$ are sums of powerproduct, thus, by a theorem of van der Poorten and Schlickewei [**19**] are growing exponentially. In this section we prove that under certain assumptions the set of values of polynomials at rational integers behave similarly, i.e., cannot have arbitrary long periodic expansions, provided the preperiod and the period are given. More precisely we prove

Theorem 3.1. *Let $\mathbb{K}$ be an algebraic number field of degree $k \geq 2$, $(\gamma, \mathcal{D})$ be a number system with finiteness property in $\mathbb{Z}_{\mathbb{K}}$, and $w, w_1 \in \mathcal{D}^*$. Let $t(X) \in \mathbb{Z}_{\mathbb{K}}[X]$ be of degree $v \geq 0$. Assume that γ has two conjugates whose quotient is not a root of unity. Then there exist only finitely many effectively computable rational integers n such that $(t(n))_\gamma = w_1 w^u$.*

Remark 3.2. *You may find a characterization of algebraic integers whose conjugates lie on a circle in Robinson* [**17**]. *Assume that $\gamma^\ell = m$ for some integers $\ell \geq 1$, and m. As $(\gamma, \mathcal{D})$ is a number system with finiteness property in $\mathbb{Z}_{\mathbb{K}}$ we have $\mathbb{K} = \mathbb{Q}(\gamma)$, i.e., the degree of γ is exactly k. Thus γ can be a zero of an integer polynomial only if its degree is at least k. Hence $\ell \geq k$. Let $0 \neq d \in \mathcal{D}$. Then the rational integers $\sum_{i=0}^{j} d\gamma^{\ell i}$ admit the periodic representation $w^j, j \geq 1$ with the word $w = d0^\ell$. On the other hand, if $\gamma^\ell = m$ then the quotients of different conjugates of γ are roots of unity. Thus our assumption is necessary.*

Proof. We showed $\mathbb{K} = \mathbb{Q}(\gamma)$ in the remark above. Denote $\alpha^{(j)},\ j = 1, \dots, k$ the conjugates of $\alpha \in \mathbb{K}$.

Using the same notation as in the proof of Theorem 2.2 and following the same line we obtain the equation

$$t(n) = \alpha\gamma^{hu} + \beta, \tag{3.1}$$

with

$$\alpha = \frac{q\gamma^g}{\gamma^h - 1} \neq 0, \quad \beta = q_0 - \alpha.$$

Taking conjugates we obtain the system of equations

$$\begin{aligned} t^{(1)}(n) &= \alpha^{(1)}(\gamma^{(1)h})^u + \beta^{(1)}, \\ t^{(2)}(n) &= \alpha^{(2)}(\gamma^{(2)h})^u + \beta^{(2)} \end{aligned}$$

in the unknown integers n, u. This is a system of polynomial equations for any fixed u, hence it has a common solution if and only if its resultant with respect to n is zero. Let $t(X) = t_v X^v + \ldots + t_0$. Putting $Y_i = t_0^{(i)} - \alpha^{(i)}(\gamma^{(i)h})^u - \beta^{(i)}, i = 1, 2$ our resultant is the determinant of the $2v \times 2v$ matrix

$$\begin{pmatrix} t_v^{(1)} & t_{v-1}^{(1)} & \cdots & t_1^{(1)} & Y_1 & 0 & \cdots & 0 \\ 0 & t_v^{(1)} & t_{v-1}^{(1)} & \cdots & t_1^{(1)} & Y_1 & 0 & \cdots \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & \cdots & 0 & t_v^{(1)} & t_{v-1}^{(1)} & \cdots & t_1^{(1)} & Y_1 \\ t_v^{(2)} & t_{v-1}^{(2)} & \cdots & t_1^{(2)} & Y_2 & 0 & \cdots & 0 \\ 0 & t_v^{(2)} & t_{v-1}^{(2)} & \cdots & t_1^{(2)} & Y_2 & 0 & \cdots \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & \cdots & 0 & t_v^{(2)} & t_{v-1}^{(2)} & \cdots & t_1^{(2)} & Y_2 \end{pmatrix}.$$

Subtracting the $t_v^{(1)}/t_v^{(2)}$-times the $v+j$-th row from the j-t one, $j=1,\dots,v$ our matrix is equivalent to

$$\begin{pmatrix} 0 & t_{v-1,1} & \cdots & t_{1,1} & Y_{1,1} & 0 & \cdots & 0 \\ 0 & 0 & t_{v-1,1} & \cdots & t_{1,1} & Y_{1,1} & 0 & \cdots \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & \cdots & 0 & 0 & t_{v-1,1} & \cdots & t_{1,1} & Y_{1,1} \\ t_v^{(2)} & t_{v-1}^{(2)} & \cdots & t_1^{(2)} & Y_2 & 0 & \cdots & 0 \\ 0 & t_v^{(2)} & t_{v-1}^{(2)} & \cdots & t_1^{(2)} & Y_2 & 0 & \cdots \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & \cdots & 0 & t_v^{(2)} & t_{v-1}^{(2)} & \cdots & t_1^{(2)} & Y_2 \end{pmatrix}$$

where $t_{j,1} = t_j^{(1)} - t_j^{(2)} \cdot t_v^{(1)}/t_v^{(2)}, j = 1,\dots,v-1; Y_{1,1} = Y_1 - Y_2 \cdot t_v^{(1)}/t_v^{(2)}$. Subtracting the $t_{v-1,1}/t_v^{(2)}$-times the $v+j+1$-th row from the j-t one, $j=2,\dots,v$ and so one, finally we get the matrix

$$\begin{pmatrix} 0 & 0 & \cdots & 0 & Y_{1,v+1} & Y_{1,v+2} & \cdots & Y_{1,2v} \\ 0 & 0 & 0 & \cdots & t_{2,v+1} & Y_{2,v+2} & Y_{2,v+3} & \cdots \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & \cdots & 0 & 0 & t_{v,v+1} & \cdots & t_{v,2v-1} & Y_{v,2v} \\ t_v^{(2)} & t_{v-1}^{(2)} & \cdots & t_1^{(2)} & Y_2 & 0 & \cdots & 0 \\ 0 & t_v^{(2)} & t_{v-1}^{(2)} & \cdots & t_1^{(2)} & Y_2 & 0 & \cdots \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & \cdots & 0 & t_v^{(2)} & t_{v-1}^{(2)} & \cdots & t_1^{(2)} & Y_2 \end{pmatrix},$$

where

$$Y_{i,v+i} = Y_{1,1} + \beta_{i,i},\ i = 1,\dots,v,\ Y_{i,v+j} = \alpha_{i,j} Y_2 + \beta_{i,j}, i = 1,\dots,v, j > i$$

and $\alpha_{i,j}, \beta_{i,j}, t_{i,j} \in \mathbb{K}$. The determinant of this matrix is

$$t_v^{(2)v} \left(\prod_{i=1}^{v} (Y_{1,1} + \beta_{i,i}) + F_1(Y_1, Y_2) \right) = t_v^{(2)v} \left(Y_{1,1}^v + F_2(Y_1, Y_2) \right),$$

with $F_1, F_2 \in \mathbb{K}[Y_1, Y_2]$ and such that the total degree of its terms are less than v. As $t_v^{(2)} \neq 0$ our resultant is zero if and only if

$$Y_{1,1}^v + F_2(Y_1, Y_2) = 0.$$

Using the definition of Y_1, Y_2 we have

$$Y_{1,1} = -\alpha^{(1)}(\gamma^{(1)h})^u + t_0^{(1)} - \beta^{(1)} - t_v^{(1)} \left(-\alpha^{(2)}(\gamma^{(2)h})^u + t_0^{(2)} - \beta^{(2)} \right) / t_v^{(2)}.$$

This expression simplifies to

$$Y_{1,1} = \alpha_1(\gamma^{(1)h})^u + \alpha_2(\gamma^{(2)h})^u + \beta$$

by setting $\alpha_1 = -\alpha^{(1)}, \alpha_2 = \alpha^{(2)} t_v^{(1)}/t_v^{(2)}$ and $\beta = t_0^{(1)} - \beta^{(1)} - t_v^{(1)} \left(t_0^{(2)} - \beta^{(2)} \right) / t_v^{(2)}$. Notice that $\alpha_1, \alpha_2 \neq 0$, and $\beta \in \mathbb{K}$.

Substituting the expressions for Y_1, Y_2 in F_2 our equation becomes

$$\left(\alpha_1(\gamma^{(1)h})^u + \alpha_2(\gamma^{(2)h})^u \right)^v + F_3\left((\gamma^{(1)h})^u, (\gamma^{(2)h})^u \right) = 0, \tag{3.2}$$

where $F_3(X,Y)$ denotes a polynomial with coefficients from $\mathbb{K}$ and such that the total degree of its monomials is at most $v-1$. Thus, if $|\gamma^{(1)}| \geq |\gamma^{(2)}|$ then

$$\left|F_3\left((\gamma^{(1)h})^u,(\gamma^{(2)h})^u\right)\right| \leq c_1|\gamma^{(1)}|^{hu(v-1)} \tag{3.3}$$

with an effective constant depending only on $k,v,h,$ the digits of w and on the coefficients of t and the defining polynomial of γ.

Up to now $\gamma^{(1)}$ and $\gamma^{(2)}$ denoted two different conjugates of γ. In the sequel we distinguish two cases.

Case I. $|\gamma^{(1)}| = |\gamma^{(2)}|$, *but* $\gamma^{(1)}/\gamma^{(2)}$ *is not a root of unity.*

As $\gamma^{(1)}/\gamma^{(2)}$ is not a root of unity there exist by Corollary 3.7. of Shorey and Tijdeman [**18**] effectively computable constants c_2,c_3,c_4 such that

$$\left|\alpha_1(\gamma^{(1)h})^u + \alpha_2(\gamma^{(2)h})^u\right| \geq c_2|\gamma^{(1)}|^{hu}\exp(-c_3\log u),$$

whenever $|u| \geq c_4$. Hence

$$\left|\alpha_1(\gamma^{(1)h})^u + \alpha_2(\gamma^{(2)h})^u\right|^v \geq c_2^v|\gamma^{(1)}|^{huv}\exp(-c_3 v\log u).$$

This lower bound together with the upper bound given in (3.3) implies that (3.2) has only finitely many effectively computable solutions.

Case II. $|\gamma^{(1)}| > |\gamma^{(2)}|$.

This case is much simpler as the first one. Indeed $|\gamma^{(1)}| > |\gamma^{(2)}|$ implies

$$\left|\alpha_1(\gamma^{(1)h})^u + \alpha_2(\gamma^{(2)h})^u\right|^v \geq c_5|\gamma^{(1)}|^{huv},$$

immediately, whenever $|u| \geq c_6$. The rest is the same as in the first case.

□

4. Rational integers with fixed representation word

In the last section we studied how many rational integers have periodic representation in a number system of a given field. In this section we changes the roles of the actors. We fix a finite word of integers w and search for number systems $(\gamma,\mathcal{D})$ and rational integers n such that $(n)_{(\gamma,\mathcal{D})} = w$. The underlying idea is simple. If $w = w_1\dots w_\ell$ and $(\alpha)_\gamma = w$ then

$$\alpha = w_1 + w_2\gamma + \cdots + w_\ell\gamma^{\ell-1}.$$

Denote k the degree of γ. If $k \geq \ell-1$ then $1,\gamma,\dots,\gamma^{\ell-1}$ are $\mathbb{Q}$-linearly independent numbers, thus $\alpha \in \mathbb{Z}$ is only possible if $w_2,\dots,w_\ell = 0$ and $\alpha = w_1$. The problem is more interesting if $k < \ell-1$. Then $\gamma^j = \sum_{i=0}^{k-1} g_{ij}\gamma^i$ holds for all $j \geq 0$ with suitable integers g_{ji}. Thus

$$\begin{aligned}\alpha &= \sum_{j=0}^{\ell-1} w_{j+1}\gamma^j\\ &= \sum_{j=0}^{\ell-1} w_{j+1}\sum_{i=0}^{k-1} g_{ij}\gamma^i\\ &= \sum_{i=0}^{k-1}\sum_{j=0}^{\ell-1} w_{j+1}g_{ij}\gamma^i.\end{aligned}$$

Now as $1, \gamma, \ldots, \gamma^{k-1}$ are $\mathbb{Q}$-linearly independent numbers $\alpha \in \mathbb{Z}$ holds if and only if $\sum_{j=0}^{\ell-1} w_{j+1} g_{ij} = 0$ for $i = 1, \ldots, k-1$.

We show that these condition can be interpreted as diophantine equations in the coefficients of the minimal polynomial of γ. It is well known that the sequences $(g_{ij})_{i \geq 0}$ are linearly recursive. More precisely we have

Lemma 4.1. *Let $X^k + g_{k-1}X^{k-1} + \ldots + g_0 \in \mathbb{Z}[X]$ be the minimal polynomial of γ. The sequences $(g_{ij})_{j \geq 0}$ have the initial values $g_{ij} = \delta_{ij}, 0 \leq j, i \leq k-1$ and satisfy the recursion*

$$g_{ij} = -g_{k-1} g_{i,j-1} - \cdots - g_0 g_{i,j-k} \tag{4.1}$$

for $j \geq k$. As usual δ_{ij} denotes Kronecker's δ, which is 1 for $j = i$ and zero otherwise.

For convenience of the reader we present here the easy proof.

Proof. The statement about the initial values is obviously true. Further, as $\gamma^k = \sum_{i=0}^{k-1} -g_i \gamma^i$, the recursion holds for $j = k$. Assume that $\gamma^j = \sum_{i=0}^{k-1} g_{ij}\gamma^i$ holds for all $0 \leq j \leq h$ for some $h \geq k$. Then

$$\begin{aligned}
\gamma^{h+1} &= \gamma\gamma^h = \gamma \sum_{i=0}^{k-1} g_{ih}\gamma^i \\
&= \sum_{i=0}^{k-2} g_{ih}\gamma^{i+1} + g_{k-1,h}\gamma^k \\
&= -g_0 g_{k-1,h} + \sum_{i=0}^{k-2} (g_{ih} - g_{i+1} g_{k-1,h})\gamma^{i+1},
\end{aligned}$$

where we used the expression for γ^k. As $1, \gamma, \ldots, \gamma^{k-1}$ are $\mathbb{Q}$-linearly independent, and setting $g_{-1,h} = 0$ we obtain

$$g_{i,h+1} = g_{i-1,h} - g_i g_{k-1,h}, \; i = 0, \ldots, k-1. \tag{4.2}$$

Summing these equalities for the pairs $(i, h) = (k-1, h+1), (k-2, h), \ldots, (0, h-k+2)$ we obtain the stated relation for $i = k-1$. Next we consider $i = 0$, whence we have $g_{0,h+1} = -g_0 g_{k-1,h}$, i.e., $(g_{0j})_{j \geq 1} = -g_0 (g_{k-1,j-1})_{j \geq 0}$, which proves the statement in this case.

Assume finally that (4.1) holds for some $0 \leq i < k-2$. The relation (4.2) with $i+1$ on the place of i means that the sequence $(g_{i+1,h})_{h \geq 0}$ is the sum of the sequences $(g_{i,h})_{h \geq 0}$ and $(g_{k-1,h})_{h \geq 0}$, which both satisfy the recursion (4.1), thus it must do the same. □

Lemma 4.1 means that the coefficient of γ^i, $0 \leq i \leq k-1$ in γ^h is a polynomial with integral coefficients in $g_0, \ldots, g_{k-1}$, whose degree increase with h. For example for $k = 2$ we have

h	0	1	2	3	4	5
g_{0h}	1	0	$-g_0$	g_0g_1	$-g_0g_1^2 + g_0^2$	$g_0g_1^3 - 2g_0^2g_1$
g_{1h}	0	1	$-g_1$	$g_1^2 - g_0$	$-g_1^3 + 2g_0g_1$	$g_1^4 - 3g_0g_1^2 + g_0^2$

The same data for $k = 3$.

h	0	1	2	3	4	5	6
g_{0h}	1	0	0	$-g_0$	g_0g_2	$-g_0g_2^2 + g_0g_1$	$g_0g_2^3 - g_0g_1^2 - g_0g_1g_2 + g_0^2$
g_{1h}	0	1	0	$-g_1$	$g_1g_2 - g_0$	$-g_1g_2^2 + g_0g_2 + g_1^2$	$g_1g_2^3 - g_0g_2^2 - 2g_1^2g_2 + 2g_0g_1$
g_{2h}	0	0	1	$-g_2$	$g_2^2 - g_1$	$-g_2^3 + 2g_1g_2 - g_0$	$g_2^4 - 3g_1g_2^2 + 2g_0g_2 + g_1^2$

Let $w = w_1 \dots w_\ell \in \mathbb{Z}^*$, i.e., w be a finite word, whose letters are integers. We shall consider w the word of digits of the representation of an element in a number system[1]. Extending w with a string of zeroes the represented element does not change, thus it is natural to assume that either $w = 0$ or $w_\ell \neq 0$.

Denote by $\mathcal{D}_w$ the set of letters of w. Choosing $g \in \mathbb{Z}$ larger than the size of $\mathcal{D}_w$ and such that $d_1 \not\equiv d_2 \pmod g$ for all $d_1, d_2 \in \mathcal{D}_w, d_1 \neq d_2$ one can extend $\mathcal{D}_w$ on infinitely many ways to a complete residue system modulo g. Now setting $n = \sum_{i=1}^{\ell} w_i g^{i-1}$ we see that $(n)_{(g,\mathcal{D})} = w$ for all $\mathcal{D}_w \subseteq \mathcal{D} \subset \mathbb{Z}$ such that $\mathcal{D}$ is a complete residue system modulo g. Thus in $\mathbb{Z}$ any finite word of integers appears as the word of digits of some integer in an appropriate number system. The situation is completely different if we consider the representations of rational integers in number systems in algebraic number fields. This is what we analyse in the sequel.

Our argument above shows that if for a given w there exist $g, \mathcal{D} \supset \mathcal{D}_w$ and $n \in \mathbb{Z}$ such that $(n)_{(g,\mathcal{D})} = w$ then replacing $z \in \mathcal{D} \setminus \mathcal{D}_w$ by any z', with $z' \equiv z \pmod g$ we obtain a different number system $(g, \mathcal{D}')$ in which the representation of n does not change. Thus such number systems are equivalent from the actual point of view. More generally the number systems $(\gamma, \mathcal{D}_1), (\gamma, \mathcal{D}_2)$ are called *w-equivalent* if there exists $n \in \mathbb{Z}$ such that $(n)_{(\gamma,\mathcal{D}_1)} = (n)_{(\gamma,\mathcal{D}_2)} = w$.

After these preparations we can present a method, which establish for a given $w \in \mathbb{Z}^*$ all algebraic integers γ for which there exist $\mathcal{D} \supset \mathcal{D}_w$ and $n \in \mathbb{Z}$ such that $(n)_{(\gamma,\mathcal{D})} = w$. Although we are not able to prove, but the construction indicates that there exist for any $w \in \mathbb{Z}^*$ only finitely many w-equivalent number systems $(\gamma, \mathcal{D})$, provided the degree of γ is less than $\ell - 1$.

Algorithm

Input: $w = w_1 \dots w_\ell \in \mathbb{Z}^*$ such that $\ell \geq 2$ and $w_\ell \neq 0$.

Output: The set S of triplets $(\gamma, \mathcal{D}, n)$ such that $[\mathbb{Q}(\gamma) : \mathbb{Q}] = k \geq 2$, $n \in \mathbb{Z}$ and $(n)_{(\gamma,\mathcal{D})} = w$.

```
1. $S \leftarrow \emptyset$;
2. for $k \leftarrow 2$ to $\ell$ do {
3.     for $i \leftarrow 1$ to $k-1$ do $L_i \leftarrow \sum_{j=0}^{\ell-1} w_{j+1} g_{ij}$;
           (* The $L_i$ are polynomials in $g_0, \dots, g_{k-1}$.*)
5.     $S_1 \leftarrow$ set of solutions of the system of equations $L_i = 0, i = 1, \dots, k-1$ in
           $(g_0, \dots, g_{k-1}) \in \mathbb{Z}^k$;
6.     for g $= (g_0, \dots, g_{k-1}) \in S_1$ do {
7.       $S_1 \leftarrow S_1 \setminus \{$g$\}$;
8.       if $0 \in \mathcal{D}_w$ and $g_0 \nmid v_i - v_h, 1 \leq i < h \leq |\mathcal{D}_w|, v_i, v_h \in \mathcal{D}_w$ and
           $P(X) = X^k + g_{k-1}X^{k-1} + \dots + g_0$ is irreducible in $\mathbb{Q}[X]$ then
9.       $S \leftarrow \{(\gamma, \mathcal{D}, n)\}$, where $\gamma$ is a zero of $P(X)$, $\mathcal{D} \supseteq \mathcal{D}_w$ is a complete residue
```

[1] In the everyday life the string of digits identifies the number whose decimal representation is the given string. For example 2020 means the number $2 \cdot 10^3 + 2 \cdot 10^0$.

```
    system modulo $g_0$ and $n = \sum_{j=0}^{\ell-1} w_{j+1}g_{0j}$ }
} (* end of the $k$ cycle*)
```

Remark 4.2. *We assume $\ell \geq 2$ because otherwise $w = w_1$ is the representation of the rational integer w_1 in any number systems $(\gamma, \mathcal{D})$, provided $0, w_1 \in \mathcal{D}$.*

Algorithm is not an algorithm in strict sense, because in Step 5 the system of equations

$$L_i(g_0, \dots, g_{k-1}) = \sum_{j=0}^{\ell-1} w_{j+1}g_{ij} = 0,\ i = 1, \dots, k-1 \tag{4.3}$$

may have for some k infinitely many solutions. This is not an option, but for $k = \ell - 1, \ell - 2$ typical. The reason is that the unknown $g_{k-2}, \dots, g_0$ appear in a linear term in $L_{k-1}, \dots, L_1$ respectively thus it is possible to express $g_{k-2}, \dots, g_0$ as polynomials in g_{k-1}, see the details in the proof of Proposition 4.4.

If, however, $k < \ell - 2$ then there is no linear terms in L_i, thus the system of equations (4.3) *can be solved by computing the Gröbner basis of the polynomial ideal generated by $L_1, \dots, L_{k-1}$ or by successive elimination of the unknowns $g_{k-2}, \dots, g_0$ by computing the resultant of $L_{k-2}, \dots, L_1$ with the previously computed resultant (see Pethő* [**14**]*, especially Sections 6.11 and 8.4.3). On this way we get a polynomial equation in two unknowns, which solutions parameterize the solutions of the original problem. By our experience these curves have high genus, thus only finitely many integer points may lie on them. This justifies our expectation that S_1 is finite for $k < \ell - 2$, i.e., for $k < \ell - 2$ there is no infinite loops in the Algorithm.*

Theorem 4.3. *The Algorithm is correct. If $w = w_1 \dots w_\ell \in \mathbb{Z}^*$ with $\ell \geq 2, w_\ell \neq 0$ then the set S includes all γ, n and a $\mathcal{D}_w \subseteq \mathcal{D} \subset \mathbb{Z}$ such that $[\mathbb{Q}(\gamma) : \mathbb{Q}] = k \geq 2$, $n \in \mathbb{Z}$ and $(n)_{(\gamma,\mathcal{D})} = w$.*

Proof. Let $w = w_1 \dots w_\ell \in \mathbb{Z}^*$ with $w_\ell \neq 0$. Assume that there exists an algebraic integer γ with minimal polynomial $P(X) = X^k + g_{k-1}X^{k-1} + \dots + g_0 \in \mathbb{Z}[X]$ such that $|g_0| \geq |\mathcal{D}_w|$. Assume further that there is a rational integer n such that

$$n = \sum_{j=0}^{\ell-1} w_{j+1}\gamma^j.$$

At this stage $g_0, \dots, g_{k-1}$ are unknown integers.

Using the notations of Lemma 4.1 we obtain

$$n = \sum_{i=0}^{k-1} \left(\sum_{j=0}^{\ell-1} w_{j+1}g_{ij} \right) \gamma^i.$$

By our assumption γ is of degree $k \geq 2$, thus $1, \gamma, \dots, \gamma^{k-1}$ are $\mathbb{Q}$-linear independent, hence the last equation holds if and only if the coefficients of γ^i, $i = 1, \dots, k-1$ are zero, which is the system of equations (4.3). This justifies Steps 4. and 5. Moreover, if $\ell \leq k-1$ then $L_i = w_{i+1}$ for $i = 1, \dots, \ell$, i.e., $w_i = 0$ for $i = 2, \dots, \ell$, hence $w = w_1 0^{\ell-1}$, which is not an allowed input. Thus non-trivial solutions can appear only if $\ell > k-1$, i.e., $k \leq \ell$ which justifies the choice of the upper limit of the loop in Step 2.

Note that from Step 6. $g_0, \dots, g_{k-1}$ denote concrete integers. In Step 8 we check the extendability of $\mathcal{D}_w$ to a complete residue system modulo g_0. This is possible only if the elements of $\mathcal{D}_w$ belong to different residue classes modulo g_0. (This excludes $|g_0| < |\mathcal{D}_w|$ too.) In the same step we test the irreducibility of $P(X)$, which is equivalent to that the degree of γ is k. After $P(X)$ and $\mathcal{D}_w$ pass all tests then the rational integer $n = \sum_{j=0}^{\ell-1} w_{j+1} g_{0j}$ satisfies $(n)_{(\gamma,\mathcal{D})} = w$. □

Now we investigate the cases $\ell = k+1$ and $k+2$.

Proposition 4.4. *Let $w_2 \dots w_\ell \in \mathbb{Z}^*$ with $\ell \geq 3, w_\ell \neq 0$. If $w_\ell | w_i,\ i = 2, \dots, \ell$ then for all $w_1 \in \mathbb{Z}$ and for $k = \ell, \ell - 1$ there exist $g_1, \dots, g_{k-1} \in \mathbb{Z}$, infinitely many $g_0 \in \mathbb{Z}$, and $\{w_1, \dots, w_\ell\} \subseteq \mathcal{D} \subset \mathbb{Z}$ such that if γ is a zero if the polynomial $P(X) = X^k + g_{k-1}X^{k-1} + \dots + g_0$ then $n = \sum_{i=0}^{\ell-1} w_{i+1}\gamma^i \in \mathbb{Z}$. In particular, if P is irreducible then $(n)_{(\gamma,\mathcal{D})} = w_1 \dots w_\ell$. Moreover*

- *if $\ell = k+2$ then not only w_1, but also $g_{k-1} \in \mathbb{Z}$ can be arbitrary,*
- *if $\ell = k+1$, and there is an $2 \leq i \leq \ell$ such that $w_\ell \nmid w_i$ then there is no $w_1 \in \mathbb{Z}$ with the above property.*

Proof. Let the defining polynomial of γ be $P(X)$. From the proof of Theorem 4.3 we know that γ satisfies the requirements of the proposition if and only if the coefficients of P solve the system of equations

$$L_i = \sum_{j=0}^{\ell-1} w_{j+1} g_{ij} = 0,\ i = 1, \dots, k-1.$$

In the sequel we treat the cases $\ell = k+1$ and $\ell = k+2$ separately.

Case $\ell = k+1$. By Lemma 4.1 we know that $g_{ij} = \delta_{ij},\ 0 \leq i,j \leq k-1$, further $g_{ik} = -g_i, i = 0, \dots, k-1$, hence

$$L_i = w_{i+1} - w_{k+1} g_i,\ i = 0, \dots, k-1.$$

We have $g_i \in \mathbb{Z}$ if and only if $w_{k+1} | w_{i+1}$ for all $i = 1, \dots, k-1$. If these relations hold then $g_i = \frac{w_{i+1}}{w_{k+1}},\ i = 1, \dots, k-1$. Now let $w_1 \in \mathbb{Z}$ be arbitrary, and $0, w_1 \neq g_0 \in \mathbb{Z}$ such that $w_i \not\equiv w_j \pmod{g_0}, 1 \leq i < j \leq k+1$, and, finally, $\mathcal{D} \subset \mathbb{Z}$ a complete residue system modulo g_0 including $\mathcal{D}_w$ then taking $n = w_1 - w_{k+1} g_0 \in \mathbb{Z}$ we have $(n)_{(\gamma,\mathcal{D})} = w$. The choice $g_0 = w_1$ is excluded because then $n = 0$.

Case $\ell = k+2$. We have by Lemma 4.1

$$g_{i,k+1} = -g_{k-1} g_{ik} - g_{i-1} = g_{k-1} g_i - g_{i-1},\ i = 1, \dots, k-1$$

and $g_{0,k+1} = -g_{k-1} g_{0k} = g_{k-1} g_0$. Hence

$$L_i = \begin{cases} w_{i+1} - w_{k+1} g_i + w_{k+2}(g_{k-1} g_i - g_{i-1}), & \text{if} \quad i = 1, \dots, k-1 \\ w_1 - w_{k+1} g_0 + w_{k+2} g_{k-1} g_0, & \text{if} \quad i = 0. \end{cases}$$

As $g_{k-2}, \dots, g_0$ are integers, the equations $L_i = 0,\ i = k-1, \dots, 1$ give conditions for g_{k-1}. For example $L_{k-1} = 0$ implies

$$g_{k-2} = \frac{w_k - w_{k+1} g_{k-1}}{w_{k+2}} + g_{k-1}^2,$$

hence $g_{k-2} \in \mathbb{Z}$ if and only if $w_k - w_{k+1} g_{k-1} \equiv 0 \pmod{w_{k+1}}$. With increasing k the conditions become more and more ugly, therefor we do not search for the general condition.

If $w_{k+2}|w_i, i=1,\dots,k+1$, then the situation is simpler, because $g_i = G_i(g_{k-1}), i = 1,\dots,k+2$, with a polynomial $G_i \in \mathbb{Z}[X]$ of degree $k+3-i$. With the choice $G_{k+2} = X$ the claim is true for $i = k+2$. Assume that $2 \leq i_0 \leq k+2$ is such that the claim is true for i_0. The condition $L_{i_0} = 0$ and the induction hypothesis implies

$$\begin{aligned} g_{i_0-1} &= g_{k-1}g_{i_0} - \frac{w_{k+1}}{w_{k+2}}g_{i_0} + \frac{w_{i_0+1}}{w_{k+2}} \\ &= g_{k-1}G_{i_0}(g_{k-1}) - \frac{w_{k+1}}{w_{k+2}}G_{i_0}(g_{k-1}) + \frac{w_{i_0+1}}{w_{k+2}}. \end{aligned}$$

Setting $G_{i_0-1}(X) = XG_{i_0}(X) - \frac{w_{k+1}}{w_{k+2}}G_{i_0}(X) + \frac{w_{i_0+1}}{w_{k+2}}$ we see that it has rational integer coefficients, its degree is $k+3-i_0+1 = k+3-(i_0-1)$ and $g_{i_0-1} = G_{i_0-1}(g_{k-1})$ thus our claim is proved. This means that $g_i = G_i(g_{k-1}), i = 1,\dots,k+2$ are integers for any $g_{k-1} \in \mathbb{Z}$. Choosing $w_1 \in \mathbb{Z}$ arbitrary and finally g_0 and $\mathcal{D}$ as in the case $\ell = k+1$ finishes the proof of this proposition. □

5. Repunits in number systems

Integers with simple decimal expansion fascinate people. Question concerning such numbers lead to interesting and hard diophantine problems. There are numbers whose decimal expansion contains only one repeating digit, in the simplest case this digit is the 1. A rational integer n is called *repunit* if $(n)_g = 1^\ell$ holds with some integers $g \geq 2, \ell \geq 1$. There are for any fixed g obviously infinitely many repunits. The challenging, and still open, problem is to find all rational integers, which are repunits in two different bases. You can find on this subject recent results and a good overview in the paper of Bugeaud and Shorey [**1**].

Repunit is a meaningful concept for number systems in algebraic number fields too, provided 1 belongs to the digit set. To be precise; let $\mathbb{K}$ be a number field and $(\gamma, \mathcal{D})$ be a number system in $\mathbb{Z}_\mathbb{K}$. The element $\alpha \in \mathbb{Z}_\mathbb{K}$ is called *repunit in* $(\gamma, \mathcal{D})$ if $(\alpha)_\gamma = 1^\ell$ for some $\ell \geq 0$. All repunits in $(\gamma, \mathcal{D})$ belong to $\mathbb{Z}_\mathbb{K}$, i.e. infinitely many elements of $\mathbb{Z}_\mathbb{K}$ are repunits in $(\gamma, \mathcal{D})$.

If $(\gamma, \mathcal{D})$ is fixed then under mild and natural conditions there exit by Theorem 3.1 only finitely many rational integers, which are repunits in $(\gamma, \mathcal{D})$. Similarly, by Proposition 4.4, if ℓ is fixed then the Algorithm finds up to equivalence all number systems for which there exists a rational integer, which is a repunit of length ℓ. We present here that rational integer repunits allow more precise description. To state our first result of this section we have to introduce a polynomial. For $i \geq 0$ let

$$G_i(X) = \sum_{h=0}^{i}(X-1)^h = \frac{(X-1)^{i+1}-1}{X-2}.$$

Corollary 5.1. *Let $k \geq 2$ and $\mathbb{K}$ be a number field of degree k. The only rational integer, which is a repunit of length $\ell \leq k$ in a number system in $\mathbb{Z}_\mathbb{K}$ is* 1.

- *If γ is a zero of $Q_m(X) = \sum_{i=1}^k X^i + m$, $0, \pm 1 \neq m \in \mathbb{Z}$ then $n = 1-m$ is a repunit in $(\gamma, \mathcal{D})$ of length $k+1$ provided $\mathcal{D}$ is a complete residue system modulo m including* 0, 1.
- *For $0, 1 \neq m \in \mathbb{Z}$ let $P_m(X) = \sum_{i=0}^k G_i(m)X^{k-i}$, γ be a zero of $P_m(X)$ and $\mathcal{D}$ be a complete residue system modulo $G_k(m)$ including* 0, 1. *Then $G_{k+1}(m)$ is a repunit in $(\gamma, \mathcal{D})$ of length $k+2$.*

Proof. The first assertion is true by the proof of Theorem 4.3.

Specifying the notations of Proposition 4.4 we have $w_i = 1,\ i = 1, \dots, k+1$. This, together with $L_i = 1 - g_i = 0$ implies $g_i = 1,\ i = 1, \dots, k$. Finally choosing $g_0 = m$, and taking into consideration $|g_0| \geq 2$ we obtain the second assertion.

To prove the third assertion we could proceed similarly, but we have chosen a different approach. The polynomials $G_i(X)$ satisfy the recursion $G_{i+1}(X) = (X-1)G_i(X) + 1,\ i \geq 0$. Using this we get

$$\begin{aligned}(m-1)P_m(X) &= \sum_{i=0}^{k}(m-1)G_i(m)X^{k-i}\\ &= \sum_{i=0}^{k}(G_{i+1}(m)-1)X^{k-i}\\ &= G_{k+1}(m) + XP_m(X) - \sum_{i=0}^{k+1} X^i,\end{aligned}$$

hence

$$G_{k+1}(m) \equiv \sum_{i=0}^{k+1} X^i \pmod{P_m(X)},$$

which means

$$G_{k+1}(m) = \sum_{i=0}^{k+1} \gamma^i.$$

The cases $m = 0, 1$ are excluded because $G_k(1) = 1$ for $k \geq 0$, and $G_k(0) = 0$ if k is odd, and $G_k(0) = 1$ if k is even, thus the roots of $P_0(X)$ and $P_1(X)$ cannot be bases of number systems. □

Remark 5.2. *By using the Algorithm, an elementary computation shows that there is no rational integer, which is a repunit of length five in a quadratic number field. As this approach became more and more complicated we returned to the approach of the proof of Theorem 3.1.*

For $k = 2$ we have $Q_m(X) = X^2 + X + m$ and $P_m(X) = X^2 + mX + m^2 - m + 1$. Then $1 - m$ as well as $m^3 - 2m^2 + 2m$ is a repunit of length 3 and 4 respectively in some number system generated by the roots of $P_m(X), Q_m(X)$. Their discriminants are $1 - 4m$ and $-3m^2 + 4m - 4$ respectively. Notice that the first is positive for all $m < 0$, but the second never. Our next result show that the number systems generated by $Q_m(X), m < 0$ are exceptional.

Theorem 5.3. *Let $\mathbb{K}$ be a number field. If $\ell > 0$ is odd and $\mathbb{K}$ has at least two, or $\ell > 0$ is even and $\mathbb{K}$ has at least three real conjugates, then there is no rational integer which is a repunit with respect to any number system in $\mathbb{K}$.*

Proof. Plainly 1 is a repunit of length one in any number systems, whose digit set includes 1. Let γ be an algebraic integer and assume that $1 \neq n \in \mathbb{Z}$ be a repunit in a number system $(\gamma, \mathcal{D})$. Then there is an $2 \leq \ell \in \mathbb{Z}$ such that

$$n = \sum_{i=0}^{\ell-1} \gamma^i = \frac{\gamma^\ell - 1}{\gamma - 1}.$$

Let γ' be a conjugate of γ. As the rational numbers are inert with respect to algebraic conjugation we get

$$\frac{\gamma^\ell - 1}{\gamma - 1} = \frac{\gamma'^\ell - 1}{\gamma' - 1}.$$

If ℓ is odd then the function $f(x) = \frac{x^\ell - 1}{x-1}$ is strictly monotonically increasing for $x < -1$ and $x > 1$. We have $|\gamma|, |\gamma'| > 1$, hence the last equality is impossible.

If ℓ is even, precisely $\ell = 2$, then the zeroes of $Q_m(X) = X^2 + X + m$ satisfy $f(\gamma) = f)\gamma')$. Now $f(x)$ is strictly decreasing over $(-\infty, -1)$ and strictly increasing over $(1, \infty)$, hence for fixed $y \in \mathbb{R}$ the equation $f(x) = y, |x| > 1$ may have at most two real solutions. □

Imre Kátai and Júlia Szabó [**8**] characterized the CNS in the imaginary, and Kátai and Kovács [**7**] in the real quadratic number fields. Summarizing their results is

THEOREM 5.4. *Let γ be a zero of the irreducible polynomial $X^2+aX+b \in \mathbb{Z}[X]$, and set $\mathbb{K} = \mathbb{Q}(\gamma)$. Then $(\gamma, \{0,1,\dots,|b|-1\})$ is a CNS in $\mathbb{Z}_{\mathbb{K}}$ if and only if $1 \le a \le b$, and $b \ge 2$.*

The roots of the polynomials $Q_m(X) = X^2 + X + m$ and $P_m(X) = X^2 + mX + m^2 - m + 1$ generate CNS in which $1-m$ as well as $m^3 - 2m^2 + 2m$ are repunits of length 3 and 4 respectively. We found these examples with the help of our Algorithm.

If $1 \le a \le b, b \ge 2$ be fixed then, by Theorem 3.1, there are only finitely many rational integer repunits in the CNS $\left(\frac{-a+\sqrt{a^2-4b}}{2}, \{0,1,\dots,b-1\}\right)$. We did not found any other CNS, in which some rational integer is a repunit. Therefore I propose the following conjectures.

CONJECTURE 5.5. *The only rational integer repunits in $\left(\frac{-1+\sqrt{1-4m}}{2}, \{0,1,\dots,m-1\}\right)$ and $\left(\frac{-m+\sqrt{-3m^2+4m-4}}{2}, \{0,1,\dots,m^2-m\}\right)$ are $1-m$ and m^3-2m^2+2m respectively.*

Probably the following much stronger conjecture is still true.

CONJECTURE 5.6. *Apart from the examples of Conjecture 5.5 there are no CNS in quadratic number fields in which there are rational integer repunits.*

References

[1] Y. Bugeaud and T. N. Shorey, *On the Diophantine equation $\frac{x^m-1}{x-1} = \frac{y^n-1}{y-1}$*, Pacific Journal of Mathematics, 207 (2002), pp. 61–75.

[2] J. M. Dumont, P. J. Grabner, and A. Thomas, *Distribution of the digits in the expansions of rational integers in algebraic bases*, Acta Sci. Math. (Szeged), 65 (1999), pp. 469–492.

[3] J.-H. Evertse, *On sums of S-units and linear recurrences*, Compositio Math, 53 (1984), pp. 225–244.

[4] J.-H. Evertse, K. Győry, A. Pethő, and J. M. Thuswaldner, *Number systems over general orders*, Acta Math. Hungar., 159 (2019), pp. 187–205.

[5] J.-H. Evertse and K. Győry, *Discriminant equations in Diophantine number theory*, vol. 32 of New Mathematical Monographs, Cambridge University Press, Cambridge, 2017.

[6] V. Grünwald, *Intorno all'aritmetica dei sistemi numerici a base negativa con particolare riguardo al sis- tema numerico a base negativo-decimale per lo studio delle sue analogie coll'aritmetica ordinaria (decimale)*, Giornale di matematiche di Battaglini, 23 (1885), pp. 203–221, 367.

[7] I. Kátai and B. Kovács, *Kanonische Zahlsysteme in der Theorie der quadratischen Zahlen*, Acta Sci. Math., 42 (1980), pp. 99–107.

[8] I. Kátai and J. Szabó, *Canonical number-systems for complex integer*, Acta Sci. Math., 37 (1975), pp. 255–260.

[9] P. Kirschenhofer and J. M. Thuswaldner, *Shift radix systems – a survey*, Numeration and substitution 2012, RIMS Kôkyûroku Bessatsu, B46, Res. Inst. Math. Sci. (RIMS), Kyoto, 2014.

[10] D. E. Knuth, *An imaginary number system*, Comm. ACM, 3 (1960), pp. 245–247.

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

[12] W. Penney, *A "binary" system for complex numbers*, J. ACM, 12 (1965), pp. 247–248.

[13] A. Pethő, *On a polynomial transformation and its application to the construction of a public key cryptosystem*, Computational Number Theory, Proc., Eds.: A. Pethő, M. Pohst, H. G. Zimmer and H. C. Williams, Walter de Gruyter Publ. Comp., 1991.

[14] ———, *Algebraische Algorithmen*, Braunschweig; Wiesbaden, Vieweg, 1999.

[15] A. Pethő, *Variations on a theme of K. Mahler, I*, Ann. Univ. Sci. Budapest. Sect. Comput, 48 (2018), pp. 137–149.

[16] A. Pethő and J. M. Thuswaldner, *Number systems over orders*, Monatsh. Math., 187 (2018), pp. 681–704.

[17] R. Robinson, *Conjugate algebraic integers on a circle*, Math. Z., 110 (1969), pp. 41–51.

[18] T. Shorey and R. Tijdeman, *Exponential Diophantine Equations*, vol. 87 of Cambridge Tracts in Mathematics, Cambridge University Press, 1986.

[19] A. J. van der Poorten and H. P. Schlickewei, *The growth condition for recurrence sequences*, Macquarie University Math. Rep., 82-0041 (1982).

[20] A. Vince, *Replicating tessellations*, SIAM J. Discrete Math., 6 (1993), pp. 501–521.

Department of Computer Science, University of Debrecen, H-4002 Debrecen, P.O. Box 400, HUNGARY

E-mail address: Petho.Attila@inf.unideb.hu