Annales Univ. Sci. Budapest., Sect. Comp. 48 (2018) 137–149

VARIATIONS ON A THEME OF K. MAHLER, I.

Attila Pethő (Debrecen, Hungary)

Communicated by Imre Kátai

(Received February 22, 2018; accepted April 30, 2018)

Abstract. For an integer n denote $(n)_g$ the sequence of digits of the g-ary representation of n. Mahler [17] proved that the number $0.(1)_{10}(g)_{10}(g^2)_{10}\dots$ is irrational for any $g \geq 2$. It has many generalizations and refinements. Here we prove further generalizations. In the first direction we replace the sequence of powers by weighted sums of elements of a finitely generated multiplicative semigroup of a number field. In the second direction, the base g is replaced by an algebraic integer. As a byproduct, we prove a Mahler-type result replacing the sequence of powers by a fixed coordinate of solutions of a norm form equation.

1. Introduction

Let $\mathbb{K}$ be an algebraic number field and denote $\mathbb{Z}_{\mathbb{K}}$ its ring of integers. Let R be a subring of $\mathbb{Z}_{\mathbb{K}}, p \in R[X]$ monic and $\mathcal{D} \subset R$ be finite, which includes a complete residue system modulo $p(0)$. The pair $(p, \mathcal{D})$ is called a number system with finiteness property, with shorthand GNS, in $R[X]$, if for any $0 \neq a \in R[X]$ there exist an integer $\ell \geq 0$ and $a_0, \dots, a_\ell \in \mathcal{D}, a_\ell \neq 0$ such that

$$a \equiv a_0 + a_1 X + \cdots + a_\ell X^\ell \pmod{p}. \tag{1.1}$$

With other words any element of $R/(p)$ has a representative polynomial with coefficients belonging to $\mathcal{D}$. In the sequel ℓ will be called the length of the

Key words and phrases: Number system, Mahler number, periodic words, unit equations.
2010 Mathematics Subject Classification: 11A63, 11D57, 11J72.
Research is supported in part by the OTKA grant NK115479.

$(p, \mathcal{D})$-representation of a. It will be denoted by $l(a)$. Further, we denote the sequence of the digits $a_0, a_1, \ldots, a_\ell$ by $(a)_p$.

This concept generalizes the radix as well as the negative-base representations of the integers and the canonical number systems in algebraic number fields. Indeed if p is irreducible in $R[X]$ and γ is a complex zero of p then $\mathbb{L} = \mathbb{K}(\gamma)$ is a finite extension of $\mathbb{K}$, i.e., itself an algebraic number field. Moreover $R[\gamma]$ is a subring of $\mathbb{Z}_\mathbb{L}$, which is isomorphic to $R/(p)$. Thus, inserting γ on the place of X in (1.1) we get

$$\beta = a(\gamma) = a_0 + a_1\gamma + \cdots + a_\ell\gamma^\ell. \tag{1.2}$$

The elements β run through $R[\gamma]$. In this case we call the pair $(\gamma, \mathcal{D})$ a GNS in $R[\gamma]$ and denote the sequence or word of digits $a_0a_1 \ldots a_\ell$ of β by $(\beta)_\gamma$.

In the case of $\mathbb{K} = \mathbb{Q}$, hence $\mathbb{Z}_\mathbb{K} = \mathbb{Z}$, $p = X - 10$ and $\mathcal{D} = \{0, 1, \ldots, 9\}$, which means $\gamma = 10$, our equation (1.2) gives the decimal representation of the positive integer β. The negative integers can not have similar representation because the sum of the right hand side is always non-negative. However, choosing $p = X + 10$ and the same $\mathcal{D}$ as before, it is easy to see that $(p, \mathcal{D})$ is a GNS in $\mathbb{Z}[x]$, thus, any integer β has a representation (1.2) with $\gamma = -10$.

The positive-based, especially decimal, representation is used since the ancient time while the negative-based representation was introduced by Grünwald [10]. Knuth [15] and Penney [19] studied radix representations in some quadratic number fields. A GNS with the special digit set $\mathcal{D} = \{0, 1, \ldots, |p(0)| - 1\}$ was called canonical number system, CNS, by Kátai and Szabó [14]. They, Gilbert [9] as well as Kátai and Kovács [13] characterized completely the bases of CNS in quadratic number fields. GNS over $\mathbb{Z}$ was defined by Pethő [20], and over orders of algebraic number fields by Pethő and Thuswaldner [21]. Indlekofer, Kátai and Racskó [12] studied connections between number systems and fractal geometry.

For an integer n denote $(n)_g$ the sequence of digits of the g-ary representation of n, where $g \geq 2$. Plainly, $(n)_g$, and $(a)_p$ above, are finite words over the actual digit set, as alphabet. For finite words concatenation is the operation of joining them end-to end. If w_1, w_2 are finite words over the alphabet A then their concatenation will be denoted by w_1w_2. Plainly, w_1w_2 is a finite word over A as well.

Mahler [17] proved that the number $0.(1)_{10}(g)_{10}(g^2)_{10}\ldots$ is irrational for any $g \geq 2$. Bundschuh [6], Niederreiter [18], Shan [23] generalized and/or gave new proofs of the result of Mahler. The most general statement of this art is due to Shan and Wang [24]: Let $g, h \geq 2$ be two integers, $(n_i)_{i=1}^\infty$ be a strictly increasing sequence of integers. Then the positive real number $0.(g^{n_1})_h(g^{n_2})_h\ldots$ is irrational. Notice that their proof works for unbounded sequences of integers $(n_i)_{i=1}^\infty$ too. Mahler's result was generalized for numeration systems based on

linear recursive sequences of integers by Barat, Frougny and Pethő [1] and by Becker [3]. Refinements and applications were given by Becker and Sander [4] as well as by Barat, Tichy and Tijdeman [2].

The g-ary representation of a real number is periodic exactly for the rational numbers. Thus, the result of Mahler and his successors means that the infinite word $(g^{n_1})_h(g^{n_2})_h \dots$ is not periodic. This version of Mahler's statement allows far reaching generalizations. Equipped with the GNS concept it is straightforward to ask under which condition is the infinite word $(\alpha^{n_1})_\gamma(\alpha^{n_2})_\gamma \dots$ not periodic. Here the algebraic integer γ is chosen such that $(\gamma, \mathcal{D})$ is a GNS in $R[\gamma]$ and $\alpha \in R[\gamma]$. Fortunately, we can go further by replacing the powers of α by linear combinations of elements of a finitely generated multiplicative group of $R[\gamma]$.

2. Main results

In this section we collect the main results of these notes. Let $\mathbb{K}$ be an algebraic number field and $S \subset \mathbb{Z}_\mathbb{K}$ be finite. With $\Gamma(S)$ and $\Gamma^*(S)$ we will denote the multiplicative semigroup and multiplicative group generated by S in $\mathbb{K}$, respectively.

Our first result deals with $(p, \mathcal{D})$-representations of weighted sums of elements of a multiplicative semigroup of polynomials.

Theorem 2.1. *Let $\mathbb{K}$ be a number field, R be a subring of $\mathbb{Z}_\mathbb{K}$ and $(p, \mathcal{D})$ be a GNS over R. Let $0 \notin \mathcal{A}, \mathcal{B} \subset R[X]$ be finite, Γ' be the multiplicative semigroup generated by $\mathcal{B}$ and $s \geq 1$. Let (c_n) be a sequence of elements of form $c_n = a_{n1}u_{n1} + \dots + a_{ns}u_{ns}$ with $u_{ni} \in \Gamma', a_{ni} \in \mathcal{A}, 1 \leq i \leq s, n \geq 1$. If there exists a zero γ of p such that $(c_n(\gamma))$ has infinitely many different members, $a(\gamma), b(\gamma) \neq 0$ for all $a \in \mathcal{A}, b \in \mathcal{B}$ and $\gamma \notin \Gamma^*(\{b(\gamma) : b \in \mathcal{B}\})$, then the infinite word $W = (c_1)_p(c_2)_p \dots$ is not periodic.*

The next theorem follows from the first one, but is interesting on its own right. The principal difference is that here we are dealing with radix representations in algebraic number fields.

Theorem 2.2. *Let $\mathbb{L} = \mathbb{K}(\gamma)$ be a finite extension of the number field $\mathbb{K}$, where γ is an algebraic integer. Let $G = \mathbb{Z}_\mathbb{K}[\gamma]$ and $\mathcal{D}$ be a complete residue system modulo γ in $\mathbb{Z}_\mathbb{K}$. Let $0 \notin \mathcal{A}_G, \mathcal{B}_G \subset G$ be finite, and $\Gamma_G = \langle \beta : \beta \in \mathcal{B}_G \rangle$. Let (c'_n) be a sequence whose terms have the form $c'_n = \alpha_{n1}\mu_{n1} + \dots + \alpha_{ns}\mu_{ns}$ with $\alpha_{nj} \in \mathcal{A}_G, \mu_{nj} \in \Gamma_G, 1 \leq j \leq s, n \geq 1$. If $(\gamma, \mathcal{D})$ is a GNS in G, $\gamma \notin \Gamma_G^*$ and (c'_n) has infinitely many distinct terms then the infinite word $(c'_1)_\gamma(c'_2)_\gamma \dots$ is not periodic.*

Specialising the last theorem to the simplest case, when $\mathbb{K}$ is the rational number field and considering the ordinary g-ary representation we get immediately the following far reaching generalization of Mahler's result.

Corollary 2.3. *Let $\mathcal{A}, \mathcal{B}$ be finite sets of positive integers and $g \geq 2$ be a positive integer. Let $\Gamma = \Gamma(\mathcal{B})$ and $c_n = a_{n1}u_{n1} + \cdots + a_{ns}u_{ns}$ with $u_{ni} \in \Gamma$, $a_{ni} \in \mathcal{A}, 1 \leq i \leq s, n \geq 1$. If $g \notin \Gamma$ then the number $0.(c_1)_g(c_2)_g\ldots$ is irrational.*

To illustrate the power of Theorem 2.2 we formulate a further corollary which is dealing with $(\gamma, \mathcal{D})$-representations of sequences of algebraic integers with given norm.

Corollary 2.4. *Let γ be an algebraic integer, which is neither rational nor imaginary quadratic. Let $\mathbb{K} = \mathbb{Q}(\gamma)$, $\mathcal{D}$ be a complete residue system modulo γ in $\mathbb{Z}_\mathbb{K}$ and $(p, \mathcal{D})$ be a GNS in $\mathbb{Z}[\gamma]$. If (c_n) is a sequence of elements of $\mathbb{Z}[\gamma]$ of given norm, which includes infinitely many pairwise different terms, then the word $(c_1)_\gamma(c_2)_\gamma\ldots$ is not periodic.*

Notice that in the rational and in the imaginary quadratic fields there are only finitely many units, and, more generally, finitely many elements with given norm, hence there are cases, when $(c_1)_\gamma(c_2)_\gamma\ldots$ is, and other cases, when it is not periodic.

Our final result deals with the coordinates of solutions of norm form equations. Let $\mathbb{K}$ be an algebraic number field of degree k. It has k isomorphic images, $\mathbb{K}^{(1)} = \mathbb{K}, \ldots, \mathbb{K}^{(k)}$ in $\mathbb{C}$. Let $\alpha_1 = 1, \alpha_2, \ldots, \alpha_s \in \mathbb{Z}_\mathbb{K}$ be $\mathbb{Q}$-linear independent elements and $L(\mathbf{X}) = \alpha_1 X_1 + \cdots + \alpha_s X_s$. Plainly $s \leq k$. Consider the norm form equation

$$N_{\mathbb{K}/\mathbb{Q}}(L(\mathbf{X})) = \prod_{j=1}^{k}(\alpha_1^{(j)}X_1 + \cdots + \alpha_s^{(j)}X_s) = t, \tag{2.1}$$

where $0 \neq t \in \mathbb{Z}$, which solutions are searched in $\mathbb{Z}$. Notice that the polynomial $N_{\mathbb{K}/\mathbb{Q}}(L(\mathbf{X}))$ is invariant against conjugation, thus, it has rational integer coefficients. For the theory of norm form equations we refer to the books of Borevich and Safarevich [5] and of Schmidt [22]. Now we are in the position to state our Mahler-type result on the solutions of (2.1).

Theorem 2.5. *Let $(\mathbf{x}_n) = ((x_{n1}, \ldots, x_{ns}))$ be a sequence of solutions of (2.1), including infinitely many different ones. Let $1 \leq j \leq s$ be fixed and $g \geq 2$. If (x_{nj}) is not ultimately zero then the infinite word $(|x_{1j}|)_g(|x_{2j}|)_g\ldots$ is not periodic.*

3. Proof of Theorems 2.1, 2.2 and of Corollary 2.4

The basic tool of our proofs is the theory of S-unit equations. We define them here and cite the fundamental theorem on such equations. 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, let $\mathcal{O}_S$ denote 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 $v \in M_{\mathbb{K}} \setminus S$.

Consider the *weighted S-unit equation*

$$\alpha_1 X_1 + \cdots + \alpha_s X_s = 1, \tag{3.1}$$

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 $\mathcal{O}_S$. A solution $x_1, \ldots, x_s$ of (3.1) 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 [7] and independently by van der Poorten and Schlickewei [25], see also [8].

Theorem 3.1. *Equation* (3.1) *has only finitely many non-degenerate solutions in $x_1, \ldots, x_s \in \mathcal{O}_S$.*

In the sequel $q \bmod p$ denotes the reminder of q by applying on it the Euclidean division by p. The function $q \bmod p$ is defined for all elements of $\mathbb{Z}_{\mathbb{K}}[X]$ because p is monic. Notice that the degree of $q \bmod p$ is less than m.

Proof of Theorem 2.1. The spirit of the proof goes back to Shan and Wang [24]. Assume in the contrary that W is eventually periodic. We deduce a weighted S-unit equation with infinitely many solutions, which lead to a contradiction.

Step 1. *Preparation for the deduction of the S-unit equation.* Assume that a period of W is H of period length h, i.e., $W = W_0 H^\infty$, where W_0 is a finite word over $\mathcal{D}$. Omitting, if necessary, some starting members of (c_n) we may assume without loss of generality that $W_0 = \lambda$[1], i.e., W is purely periodic. Thus, there exist for all $n \geq 1$ $c_{n0}, c_{n1} \in \mathcal{D}^*$ of length less than h and non-negative integers e_n such that $(c_n)_p = c_{n0} H^{e_n} c_{n1}$. More precisely, c_{n0} is a suffix and c_{n1} is a prefix of H.

There exist only finitely many, modulo p, pairwise incongruent polynomials with a $(p, \mathcal{D})$-representation of bounded length. Thus, the length of the words $(c_n)_p, n = 1, 2, \ldots$ is not bounded. Further, there are only $|\mathcal{A}|^s$ possible choices for the s-tuple $(a_{n1}, \ldots, a_{ns})$. Thus, there exists an infinite sequence $k_1 < k_2 < \ldots$ of integers such that $l((c_{k_n})_p) \geq h$ and $l((c_{k_{n+1}})_p) > l((c_{k_n})_p)$ and the s-tuples $(a_{k_n 1}, \ldots, a_{k_n s})$ are the same for all $n \geq 1$.

[1] λ denotes the empty word

Write $(c_{k_n})_p = c_{k_n 0} H^{e_{k_n}} c_{k_n 1}$, where $c_{k_n 0}$ is a suffix and $c_{k_n 1}$ is a prefix of H both of length at most $h-1$ for all $n \geq 1$. As H has at most $h-1$ proper prefixes and $h-1$ proper suffixes there exists an infinite subsequence of $k_n, n \geq 1$ such that the corresponding words satisfy $c_{k_n 0} = C_0$ and $c_{k_n 1} = C_1$. In the sequel we work only with this subsequence, therefore, to simplify the notation, we omit the subindexes. With this simplified notation we have $(c_n)_p = C_0 H^{e_n} C_1$, where C_0 denotes a proper suffix, and C_1 a proper prefix of H and (e_n) tends to infinity. Finally, replacing H by the suffix of length h of HC_1, and denoting it again by H we have $(c_n)_p = C_0 H^{e_n}$. If $C_0 \neq \lambda$ then set $C_0 = d_t d_{t+1} \dots d_{h-1}$ and $H = d_0 d_1 \dots d_{h-1}$ with $t > 0$ and $d_j \in \mathcal{D}$.

Now we are in the position to turn the last equation into a weighted S-unit equation. Indeed, put $q_0 = 0$, if $C_0 = \lambda$ and $q_0 = d_t + d_{t+1}X + \ldots + d_{h-1}X^{h-t-1}$ otherwise, and $q = d_0 + d_1 X + \ldots + d_{h-1}X^{h-1}$ the polynomials corresponding to C_0 and H, respectively. Then

$$\begin{aligned} c_n &\equiv q_0 + X^{h-t} \sum_{i=0}^{e_n-1} X^{ih} q \equiv \\ &\equiv q_0 + qX^{h-t} \sum_{i=0}^{e_n-1} X^{ih} \equiv \\ &\equiv q_0 + qX^{h-t} \frac{X^{he_n}-1}{X^h-1} \equiv \\ &\equiv \frac{q}{X^h-1} X^{he_n+h-t} + q_0 - \frac{qX^{h-t}}{X^h-1} \pmod{p}. \end{aligned}$$

Step 2 *Application of the theory of S-unit equations.* The last congruence lead to a weighted S-unit equation. Indeed, by the assumption, there exists a zero γ of p such that $a(\gamma), b(\gamma) \neq 0$ for all $a \in \mathcal{A}, b \in \mathcal{B}$. Substituting γ for X, the last congruence implies

$$c_n(\gamma) = a_1(\gamma)u_{n1}(\gamma) + \ldots + a_s(\gamma)u_{ns}(\gamma) = a_{s+1}(\gamma)\gamma^{he_n+h-t} + a_{s+2}(\gamma), \tag{3.2}$$

where we set

$$\begin{aligned} a_{s+1}(\gamma) &= \frac{q(\gamma)}{\gamma^h - 1}, \\ a_{s+2}(\gamma) &= q_0(\gamma) - \frac{q(\gamma)\gamma^{h-t}}{\gamma^h - 1}. \end{aligned}$$

By Proposition 2.3. of [21] $|\gamma| > 1$, hence $\gamma^h \neq 1$ and the right hand side of (3.2) is well defined. Plainly $a_k(\gamma) \in \mathbb{K}(\gamma), k = 1, \ldots, s+2$ and $a_k(\gamma) \neq 0$, $k = 1, \ldots, s$ by assumption. If $a_{s+1}(\gamma) = 0$ then $(c_n(\gamma))$ is a constant sequence, which again contradicts the assumptions. Thus, $a_{s+1}(\gamma) \neq 0$ either. Taking

Γ_1 the multiplicative semigroup generated by γ and $b(\gamma), b \in \mathcal{B}$ we see that the equation (3.2) has infinitely many solutions in $(u_1, \dots, u_s, u_{s+1}) \in \Gamma_1^{s+1}$. Moreover, we show that it is an S-unit equation in s or $s+1$ unknowns according as $a_{s+2} = 0$ or not.

Assume first $a_{s+2}(\gamma) = 0$. After division by $a_1(\gamma)u_{n1} \neq 0$ and rearranging the terms we get from (3.2) the equation

$$\alpha_1 x_1 + \cdots + \alpha_s x_s = 1, \tag{3.3}$$

with

$$\begin{aligned} \alpha_i &= -\frac{a_{i+1}(\gamma)}{a_1(\gamma)}, \text{ if } 1 \leq i < s, \\ \alpha_s &= \frac{a_{s+1}(\gamma)}{a_1(\gamma)}, \end{aligned}$$

which has infinitely many solutions in $x_1, \dots, x_s \in \Gamma_1^*$, namely

$$\begin{aligned} x_i &= \frac{u_{n,i+1}(\gamma)}{u_{n1}(\gamma)}, \text{ if } 1 \leq i < s, \\ x_s &= \frac{\gamma^{he_n+h-t}}{u_{n1}(\gamma)}, \ n = 1, 2, \dots. \end{aligned}$$

Notice that $x_1, \dots, x_{s-1}$ belong to the multiplicative group Γ^*, which is a proper subgroup of Γ_1^* by the assumption $\gamma \notin \Gamma^*$. Equation (3.3) has infinitely many solutions $(x_1, \dots, x_s) \in \Gamma_1^*$, hence, by Theorem 3.1, there is a proper subset I of $\{1, \dots, s\}$ such that $\sum_{i \in I} \alpha_i x_i = 0$ hold for infinitely many solutions. Now we distinguish two cases

Case 1. $s \in I$**.** Plainly I has at least two elements. Let $k \in I \setminus \{s\}$. Dividing the equation $\sum_{i \in I} \alpha_i x_i = 0$ by $\alpha_k x_k \neq 0$ and rearranging we get an equation with infinitely many solutions in Γ_1^* of the same shape as (3.3), but in less unknowns. Notice that all but exactly one coordinates of the solution vector belong to Γ^*. After some steps we get an equation of form $\alpha x = 1$ with $0 \neq \alpha \in \mathbb{K}(\gamma)$, which has infinitely many solutions in $x \in \Gamma_1^*$ and such that the set of exponents of γ in the solutions is unbounded.

Let $u_1, u_2 \in \Gamma$ be two solutions of $\alpha x = 1$ such that the exponents of γ in u_1 and u_2 are different. Then $\alpha u_1 = \alpha u_2 = 1$, which implies $u_1/u_2 = 1$. As the exponents of γ in u_1/u_2 is not zero and $\gamma \notin \Gamma$ this is a contradiction.

Case 2. $s \notin I$**.** Then $J = \{1, \dots, s\} \setminus I$ is such a proper subset of $\{1, \dots, s\}$ for which $\sum_{i \in J} \alpha_i x_i = 1$ holds for infinitely many $x_i \in \Gamma^*, i \in J \setminus \{s\}$, and $x_s \in \Gamma_1^*$. Hence, we arrived again the equation (3.3) in less unknowns. The argument of Case 1 applies again.

In the case $a_{s+2}(\gamma) \neq 0$ we can use the same argument as in the case of $a_{s+2}(\gamma) = 0$ with the only difference that the number of unknowns is one more. ■

Proof of Theorem 2.2. The minimal polynomial p of γ over $\mathbb{K}$ is monic and its coefficients are integers in $\mathbb{K}$. As $G = \mathbb{Z}_{\mathbb{K}}[\gamma]$ the mapping $\pi : \mathbb{Z}_{\mathbb{K}}[X]/p\mathbb{Z}_{\mathbb{K}}[X] \mapsto G$, $\pi(q) = (q \bmod p)(\gamma)$ for $q \in \mathbb{Z}_{\mathbb{K}}[X]$, is an isomorphism.

Thus, for all $\beta \in \mathcal{B}_G$ and $\alpha \in \mathcal{A}_G$ there exist $b \in \mathbb{Z}_{\mathbb{K}}[X]$ with $\beta = \pi(b) = b(\gamma)$ and $a \in \mathbb{Z}_{\mathbb{K}}[X]$ with $\alpha = \pi(a) = a(\gamma)$, respectively. Plainly $a, b \neq 0$ for all $a \in \mathcal{A}_G$ and $b \in \mathcal{B}_G$. In the rest of this proof we fix these polynomials and set $\mathcal{A} = \{a : \pi(a) = \alpha, \alpha \in \mathcal{A}_G\}$, $\mathcal{B} = \{b : \pi(b) = \beta, \beta \in \mathcal{B}_G\}$ and set $\Gamma = \langle b : b \in \mathcal{B}\rangle$. We have $\mu \in \Gamma_G$ if and only if $\mu = \beta_1^{n_1} \cdots \beta_r^{n_r}$ with $n_1, \ldots, n_r \in \mathbb{Z}_{\geq 0}$. The mapping π is obviously an isomorphism between Γ and Γ_G. We supposed $\gamma \notin \Gamma_G^*$, hence all assumptions on $\mathcal{A}, \mathcal{B}$ and Γ of Theorem 2.1 satisfy.

It remains to prove that the sequence $(c_n(\gamma))$ has infinitely many distinct terms for a suitably chosen sequence (c_n) with $c_n \in \mathbb{Z}_{\mathbb{K}}[X]$. To prove this set (c_n) the sequence with $c_n = a_{n1}\mu_{n1} + \cdots + a_{ns}\mu_{ns}$ with $\pi(a_{nj}) = \alpha_{nj}$, $\pi(u_{nj}) = \mu_{nj}$ for all $j = 1, \ldots, s, n \geq 1$. Then $\pi(c_n) = c'_n$, i.e, $(c_n \bmod p)(\gamma) = c'_n \in G$ for all $n \geq 1$.

If $\delta \in G$ then there exists on one hand a polynomial $d \in \mathbb{Z}_{\mathbb{K}}[X]$ of degree less then $\deg p$ such that $\delta = d(\gamma)$. On the other hand there exist $d_j \in \mathcal{D}$, $j = 0, \ldots, l$ such that

$$\delta = d(\gamma) = \sum_{j=0}^{l} d_j \gamma^j$$

because $(\gamma, \mathcal{D})$ is a GNS in G. Let σ be a relative conjugation of the field extension $\mathbb{L}/\mathbb{K}$. Then

$$\sigma(\delta) = d(\sigma(\gamma)) = \sum_{j=0}^{l} d_j \sigma(\gamma)^j,$$

which means

$$d(X) \equiv \sum_{j=0}^{l} d_j X^j \bmod (X - \sigma(\gamma))$$

for all σ. The relative conjugates of γ runs through the roots of p, which are pairwise different. Hence

$$d \equiv \sum_{j=0}^{l} d_j X^j \pmod{p}.$$

This is the $(p, \mathcal{D})$-representation of d, moreover $\pi(d) = \gamma$. As π is an isomorphism, $(p, \mathcal{D})$ is a GNS in $\mathbb{Z}_{\mathbb{K}}[X]$. Hence, by Theorem 2.1, $(c_1)_p(c_2)_p \dots$ is not periodic. Because of $(c_n)_p = (c'_n)_\gamma$ for all $n \geq 1$ the sequence $(c'_1)_\gamma(c'_2)_\gamma \dots$ is not periodic either, as stated. ∎

Remark 3.2. Becker proved in [3], see Corollary, a Mahler type result for sequences (f_k) where $f_k = \sum_{i=1}^{n} a_i u_i^{n_k}$ and (n_k) is a strictly increasing sequence of natural numbers. He assumed $a_1, \dots, a_n, u_1, \dots, u_n$ nonzero algebraic numbers such that neither u_i nor $u_i u_j^{-1}$ are roots of unity and (f_k) to be natural numbers for all k. He actually proved that $(f_1)_h(f_2)_h \dots$ is not periodic for each $h \geq 2$. If $h \notin \langle u_1, \dots, u_n \rangle$ then Becker's result is a special case of Corollary 2.2. Analyzing more carefully Step 2 of the proof of Theorem 2.1 in the special case treated by Becker our method is capable to handle the remaining cases.

Proof of Corollary 2.4. Assume that $N_{\mathbb{K}/\mathbb{Q}}(c_n) = N$ for all $n \geq 1$, where $N_{\mathbb{K}/\mathbb{Q}}$ denotes the norm function from $\mathbb{K}$ to $\mathbb{Q}$. It is well known, see e.g. [5], that there exists a finite set $\mathcal{A}$ such that any element of $\mathbb{Z}_{\mathbb{K}}$ of norm N can be written as αu, with $\alpha \in \mathcal{A}$ and u a unit of $\mathbb{Z}_{\mathbb{K}}$. As $\mathbb{K}$ is neither the field of rational numbers nor an imaginary quadratic number field, it has infinitely many units, and, by Dirichlet's unit theorem there are units $\varepsilon_1, \dots, \varepsilon_r$ of infinite order and non-negative integers $n_1, \dots, n_r$ such that $u = \varepsilon_1^{n_1} \dots \varepsilon_r^{n_r}$.

The number γ is a base of a radix system in $\mathbb{Z}[\gamma]$, thus, its norm is at least two in modulus, see [16], hence it is not a unit, i.e. $\gamma \notin \langle \varepsilon_1, \dots, \varepsilon_r \rangle$. Taking $s = 1$ all assumptions of Corollary 2.2 satisfy, hence $(c_1)_\gamma(c_2)_\gamma \dots$ is not periodic. ∎

4. Proof of Theorem 2.5

For the convenience of the reader we repeat the definition of the norm form equation. Let $\mathbb{K}$ be an algebraic number field of degree k. It has k isomorphic images, $\mathbb{K}^{(1)} = \mathbb{K}, \dots, \mathbb{K}^{(k)}$ in $\mathbb{C}$. Let $\alpha_1 = 1, \alpha_2, \dots, \alpha_s \in \mathbb{Z}_{\mathbb{K}}$ be $\mathbb{Q}$-linear independent elements and $L(\mathbf{X}) = \alpha_1 X_1 + \dots + \alpha_s X_s$. Plainly $s \leq k$. Consider the norm form equation

$$N_{\mathbb{K}/\mathbb{Q}}(L(\mathbf{X})) = \prod_{j=1}^{k} (\alpha_1^{(j)} X_1 + \dots + \alpha_s^{(j)} X_s) = t, \tag{4.1}$$

where $t \in \mathbb{Z}$, which solutions are searched in $\mathbb{Z}$. For the theory of norm form equations we refer to the books of Borevich and Safarevich [5] and of Schmidt [22].

Proof of Theorem 2.5. Let M denote the $\mathbb{Z}$-module generated by $\alpha_1, \dots, \alpha_s$. Plainly $M \subseteq \mathbb{Z}_{\mathbb{K}}$ and it coincides with the values of $L(\mathbf{x})$, when $\mathbf{x}$ runs through $\mathbb{Z}^s$. The module M is called *full* if $s = k$. Further M is called *degenerate* if it contains a submodule M_0, which is proportional to a full module in some subfield $\mathbb{L}$ of $\mathbb{K}$, where $\mathbb{L}$ is neither rational nor imaginary quadratic. It was proved by Schmidt, [22] (Theorem 1D, p. 212), that there exists a t such that (4.1) has infinitely many solutions $\mathbf{x} \in \mathbb{Z}^s$ if and only if M is degenerate.

If M is a degenerate module, $0 \neq \mu \in M$ such that $N_{\mathbb{K}/\mathbb{Q}}(\mu) = t$ and $M_0 = \mu M^{\mathbb{L}}$, where $M^{\mathbb{L}}$ is a full module in $\mathbb{L}$ then the group of units U_{M_0} of the multiplication ring of $M^{\mathbb{L}}$ is infinite. The set μU_{M_0} is called a *family* of solutions. Schmidt proved, [22] (Theorem 4B, p. 217), that the solutions of (4.1) are contained in finitely many families of solutions.

There exists a family and an infinite subsequence of $(\mathbf{x}_n)$ such that the sequence of the j-th coordinate of its members is not ultimately zero. It will be clear that we may assume without loss of generality that already $(\mathbf{x}_n)$ satisfies this property. Thus, there exists $\mu \in M$ and an infinite subgroup U of the group of units of $\mathbb{Z}_{\mathbb{K}}$ such that for each $n \geq 1$ there exists $u_n \in U$ such that

$$\alpha_1 x_{n1} + \cdots + \alpha_s x_{ns} = \mu u_n.$$

Taking conjugates we obtain the system of linear equations

$$\alpha_1^{(i)} x_{n1} + \cdots + \alpha_s^{(i)} x_{ns} = \mu^{(i)} u_n^{(i)}, i = 1, \dots, k,$$

which implies

$$x_{nj} = \nu_1 u_n^{(1)} + \cdots + \nu_k u_n^{(k)}$$

with some constants ν_i belonging to the normal closure of $\mathbb{K}$. As (x_{nj}) is not ultimately zero, not all of the $\nu_i, 1 \leq i \leq k$ can be zero. On the other hand it can happen, that some of them is zero. Omitting such virtual terms only the length, but not the essence of the expression on the right hand side changes. We may assume again without loss of generality that $\nu_1, \dots, \nu_k \neq 0$.

We claim that (x_{nj}) is not bounded. Indeed, assume that this is false, i.e., (x_{nj}) is bounded. Then it has an infinite constant subsequence $(x_{n_i j})$ such that $x_{n_i j} = z \neq 0$ for all $i \geq 1$, but $(\mathbf{x}_{n_i j})$ are pairwise different. To simplify the notation we assume that already $(\mathbf{x}_n)$ satisfies this property. Thus, the unit equation

$$\nu_1' u_n^{(1)} + \cdots + \nu_k' u_n^{(k)} = 1 \tag{4.2}$$

admits infinitely many solutions $u_n^{(1)}, \dots, u_n^{(k)}$, where $\nu_i' = \nu_i / z, i = 1, \dots, k$. (4.2) is indeed a unit equation because U, as a subgroup of the group of units of $\mathbb{Z}_{\mathbb{K}}$, is finitely generated. Denote $\eta_1, \dots, \eta_r$ the basis of its free part. Now let

$\Gamma = \langle \eta_i^{(h)}, 1 \le i \le r, 1 \le h \le k \rangle$, which is defined in the normal closure of $\mathbb{K}$. Plainly $u_n^{(1)}, \dots, u_n^{(k)} \in \Gamma$, i.e., (4.2) is a unit equation. By Theorem 3.1 the set $\{1, \dots, k\}$ has a proper subset I such that $\sum_{i \in I} \nu_i' u_n^{(i)} = 0$ has infinitely many solutions $u_n \in \Gamma$. Hence $\sum_{i \in \{1,\dots,k\} \setminus I} \nu_i' u_n^{(i)} = 1$ has infinitely many solutions $u_n \in \Gamma$ either. The shape of the last equation is the same as of (4.2), but it has less summands. Thus, after some step we arrive the equation $\nu_h' u^{(h)} = 1$ for some $1 \le h \le k$, which has infinitely many solutions $u \in \Gamma$, more precisely $u \in \langle \eta_1, \dots, \eta_r \rangle$, which is absurd because $\eta_1, \dots, \eta_r$ have infinite order. Thus, the claim is proved.

As (x_{nj}) is not bounded $(|x_{nj}|)$ has a strictly monotone increasing infinite subsequence. From here on we can repeat the proof of Theorem 2.1. ■

Remark 4.1. If $\mathbb{K}$ is a real quadratic number field (4.1) is called Pell equation, which solutions can be expressed by the union of finitely many linear recursive sequences. In this case Theorem 2.5 is included implicitly in Theorem 1 of [1].

Győry, Mignotte and Shorey [11] proved with the notation of Theorem 2.5 that if the set of the j-th coordinate of the solutions of (4.1) is not bounded then the greatest prime factor of them tends to infinity. Our Theorem 2.5 shows that the assumption of Győry, Mignotte and Shorey always holds if (4.1) has infinitely many solutions, which j-th coordinates is non-zero.

Acknowledgement. The author thanks the anonymous referee for his/here comments.

References

[1] **Barat, G., C. Frougny and A. Pethő,** On linear recurrent Mahler numbers, *Integers*, **5** (2005), A1 17 pages.

[2] **Barat, G., R. Tichy and R. Tijdeman,** Digital blocks in linear numeration systems, In: *Number Theory in Progress Zakopane-Koscielisko, 1997*, **2**, Walter de Gruyter, Berlin, 1999, 607–631.

[3] **Becker, P.-G.,** Exponential Diophantine equations and the irrationality of certain real numbers, *J. Number Theory*, **39** (1991), 108–116.

[4] **Becker, P.-G. and J.W. Sander,** Irrationality and codes, *Semigroup Forum*, **51** (1995), 117–124.

[5] **Borevich, Z.I. and I.R. Safarevich,** *Number Theory*, 2nd edition, Academic Press, 1967.

[6] **Bundschuh, P.,** Generalization of a recent irrationality result of Mahler, *J. Number Theory*, **19** (1984), 248–253.

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

[8] **Evertse, J.-H. and K. Győry,** *Discriminant Equations in Diophantine Number Theory*, New Mathematical Monographs, **32**, Cambridge University Press, Cambridge, 2017, pp. xviii+457.

[9] **Gilbert, W.J.,** Radix representations of quadratic fields, *J. Math. Anal. Appl.*, **83(1)** (1981), 264–274.

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

[11] **Győry, K., and M. Mignotte and T.N. Shorey,** On some arithmetical properties of weighted sums of S-units, *Math. Pannon.*, **1** (1990), 25–43.

[12] **Indlekofer, K.-H., and I. Kátai and P. Racskó,** Number systems and fractal geometry, Probability theory and applications, Essays to the Mem. of J. Mogyoródi, *Math. Appl.*, **80** (1992), 319–334.

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

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

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

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

[17] **Mahler, K.,** On some irrational decimal fractions, *J. Number Theory*, **13** (1981), 268–269.

[18] **Niederreiter, H.,** On an irrationality theorem of Mahler and Bundschuh, *J. Number Theory*, **24** (1986), 197–199.

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

[20] **Pethő, A.,** On a polynomial transformation and its application to the construction of a public key cryptosystem, in: *Computational Number Theory, Proc.*, Eds.: A. Pethő, M. Pohst, H. G. Zimmer and H. C. Williams, Walter de Gruyter Publ. Comp., 1991, 31–43.

[21] **Pethő, A. and J.M. Thuswaldner,** Number systems over orders, *Monatshefte Math.*, to appear.

[22] **Schmidt, W.M.,** *Diophantine Approximation*, Lecture Notes in Mathematics, **785**, Springer-Verlag, Berlin Heidelberg New York, 1980, pp. x+299.

[23] **Shan, Z.,** A note on irrationality of some numbers, *J. Number Theory*, **25** (1987), 211–212.

[24] **Shan, Z and E. Wang,** Generalization of a theorem of Mahler, *J. Number Theory*, **32** (1989), 111-113.

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

A. Pethő
Department of Computer Science
University of Debrecen
H-4002 Debrecen
P.O. Box 400
Hungary
and
University of Ostrava
Faculty of Science, Dvořákova 7
70103 Ostrava
Czech Republic
Petho.Attila@inf.unideb.hu