Results and problems on diophantine properties of radix representations

Attila Pethő

Department of Computer Science
University of Debrecen, Debrecen, Hungary

Representation Theory XVI, Number Theory Section
IUC, Dubrovnik, Croatia, June 26, 2019.

Talk is based partially on joint works with Jan-Hendrik Evertse, Kálmán Győry and Jörg Thuswaldner.

1. Radix representation in number fields

Let $g, h \geq 2$. Denote $(n)_g$ the sequence of digits of the g-ary representation of n, e.g. $(2018)_{10} = 2018, (2018)_5 = 31033$.
Let $\mathbb{K}$ an algebraic number field with ring of integers $\mathbb{Z}_{\mathbb{K}}$.
$\mathbb{L}$ a finite extension of $\mathbb{K}$ with ring of integers $\mathbb{Z}_{\mathbb{L}}$.
The pair $(\gamma, \mathcal{D})$, where $\gamma \in \mathbb{Z}_{\mathbb{L}}$ and $\mathcal{D}$ is a complete residue system modulo γ, in $\mathbb{Z}_{\mathbb{K}}$ is called a GNS in $\mathbb{Z}_{\mathbb{L}}$ if for any $0 \neq \beta \in \mathbb{Z}_{\mathbb{L}}$ there exist an integer $\ell \geq 0$ and $a_0, \ldots, a_\ell \in \mathcal{D}, a_\ell \neq 0$ such that

$$\beta = a_\ell \gamma^\ell + \cdots + a_1 \gamma + a_0. \tag{1}$$

Denote the sequence or word of the digits $a_\ell \ldots a_1 a_0$ by $(\beta)_\gamma$.

The GNS concept was initiated by D. Knuth, and developed further by Penney, I. Kátai, J. Szabó, B. Kovács, etc.

Not all $(\gamma, \mathcal{D})$ is a GNS! For example $\left(\frac{-1+\sqrt{-7}}{2}, \{0.1\}\right)$ is, but $\left(\frac{1+\sqrt{-7}}{2}, \{0.1\}\right)$ is not a GNS in $\mathbb{Z}[\sqrt{-7}]$.

This GNS is a special case of GNS in polynomial ring over an order, i.e., a commutative ring with unity, whose additive structure is a free $\mathbb{Z}$-module of finite rank. To avoid technical difficulties we restrict ourself to maximal orders of number fields. The GNS property is decidable in the general setting.

Problem 1. *Let $\mathcal{D} \subset \mathbb{Z}_{\mathbb{K}}$ be given. How many $\gamma \in \mathbb{Z}_{\mathbb{L}}$ exist such that $(\gamma, \mathcal{D})$ is a GNS in $\mathbb{Z}_{\mathbb{L}}$?*

For $\mathbb{K} = \mathbb{Q}$ the answer is: at most one! If $\mathcal{D} \subset \mathbb{Z} \subset \mathbb{Z}_{\mathbb{K}}$ then there are only finitely many, effectively computable. (Idea of the proof later.) In general the problem is open.

2. A theme of K. Mahler

K. Mahler, 1981, proved that the number $0.(1)_g(h)_g(h^2)_g\ldots$ is irrational, equivalently: the infinite word $(1)_g(h)_g(h^2)_g\ldots$ is not periodic. Refinements, generalizations and new methods by

- P. Bundschuh, 1984
- H. Niederreiter, 1986
- Z. Shan, 1987
- Z. Shan and E. Wang, 1989: Let $(n_i)_{i=1}^{\infty}$ be a strictly increasing sequence of integers. Then $0.(g^{n_1})_h(g^{n_2})_h\ldots$ is irrational. In the proof they used the theory of Thue equations.

Generalizations for numeration systems based on linear recursive sequences:

- P.G. Becker, 1991
- P.G. Becker and J. Sander 1995
- G. Barat, R. Tichy and R. Tijdeman, 1997
- G. Barat, C. Frougny and A. Pethő, 2005

3.1. Results on power sums

Let $0 \notin \mathcal{A}, \mathcal{B} \subset \mathbb{Z}_{\mathbb{L}}$ be finite, and Γ, Γ^{+} be the semigroup, group generated by $\mathcal{B}$. Put

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

Example: $\mathbb{L} = \mathbb{Q}, \mathcal{A} = \{1\}, \mathcal{B} = \{2, 3\}$ then

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

Theorem 1. *Let $s \geq 1$ and $\mathcal{A}, \mathcal{B}$ as above. Let (c_n) be such that $c_n \in S(\mathcal{A}, \mathcal{B}, s)$. If $(\gamma, \mathcal{D})$ is a GNS in $\mathbb{Z}_{\mathbb{L}}$, $\gamma \notin \Gamma^+$ and (c_n) has infinitely many distinct terms then the infinite word $(c_1)_\gamma (c_2)_\gamma \dots$ is not periodic.*

Let $(c_1)_\gamma (c_2)_\gamma \dots = f_0 f_1 \dots$. Then

$$g = \sum_{j=0}^{\infty} f_j \gamma^{-j}$$

is a well defined complex number. A result of B. Kovács and I. Környei, 1992 implies $g \notin \mathbb{Q}$. We expect at least $g \notin \mathbb{L}$, but we are unable to prove this.

The proof of Theorem 1 is based on the following

Lemma 1. *For any $w \in \mathcal{D}^*$ there are only finitely many $U \in S(\mathcal{A}, \mathcal{B}, s)$ such that $(U)_\gamma = w_1 w^k$, where w_1 is a suffix of w.*

Proof. Let $w = d_0 \ldots d_{h-1}$. If $(U)_\gamma = w_1 w^k$ then $w_1 = \lambda$ or $w_1 = d_t \ldots d_{h-1}$. Set $q_0 = 0$ if $w_1 = \lambda$, and $q_0 = d_t + d_{t+1}\gamma + \ldots + d_{h-1}\gamma^{h-t-1}$ otherwise. Further let $q = d_0 + d_1\gamma + \ldots + d_{h-1}\gamma^{h-1}$. We also have $U = \alpha_1\mu_1 + \cdots + \alpha_s\mu_s$. Then

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

Setting

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

we get the equation

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

As $(\gamma, \mathcal{D})$ is a GNS $|\gamma| > 1$, hence $\gamma^h \neq 1$ and $\alpha_{s+1}, \alpha_{s+2}$ are well defined. Plainly $\alpha_j \in \mathbb{L}, j = 1, \ldots, s+2$ and $\alpha_j \neq 0, k = 1, \ldots, s$ by assumption. It is easy to see that $\alpha_{s+1} \neq 0$ holds too.

Taking Γ_1 the multiplicative semigroup generated by γ and $b \in \mathcal{B}$ (2) is a Γ_1-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 can take arbitrary large values and (2) has infinitely many solutions in $(\mu_1, \ldots, \mu_s, \gamma^{hk}) \in \Gamma_1^{s+1}$. By the theory of weighted S-unit equations the assumption $\gamma \notin \Gamma^+$ excluded this. $\square$

Proof of Theorem 1. Let $W = (c_1)_\gamma(c_2)_\gamma \dots$ and assume that it is eventually periodic. Omitting, if necessary, some starting members of (c_n) we may assume that it is periodic, i.e. $W = H^\infty$ with $H \in \mathcal{D}^h$.

There exist for all $n \geq 1$ a suffix c_{n0} a prefix c_{n1} of H and an integer $e_n \geq 0$ such that $(c_n)_\gamma = c_{n0}H^{e_n}c_{n1}$.

There exist only finitely many, elements of $\mathbb{Z}_\mathbb{K}$ with a $(\gamma, \mathcal{D})$-representation of bounded length. Thus, the length of the words $(c_n)_\gamma, n = 1, 2, \dots$ is not bounded. Further, there are only $|\mathcal{A}|^s$ possible choices for the s-tuple $(a_{n1}, \dots, a_{ns})$. Thus, there exists an infinite sequence $k_1 < k_2 < \dots$ of integers such that $l((c_{k_n})_\gamma) \geq h$ and $l((c_{k_{n+1}})_\gamma) > l((c_{k_n})_\gamma)$ and the s-tuples $(a_{k_n1}, \dots, a_{k_ns})$ are the same for all $n \geq 1$.

Write $(c_{k_n})_\gamma = c_{k_n 0} H^{e_{k_n}} c_{k_n 1}$, where $c_{k_n 0}$ is a suffix and $c_{k_n 1}$ is a prefix of H 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 we omit the subindexes.

With this simplified notation we have $(c_n)_\gamma = C_0 H^{e_n} C_1$, 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 $(c_n)_\gamma = C_0 H^{e_n}$. This contradicts Lemma 1. $\square$

Considering for $\mathbb{K} = \mathbb{Q}$ the ordinary g-ary representation of integers we get immediately the following far reaching generalization of Mahler's result.

Corollary 1. *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* $g \notin \Gamma$ *and* (c_n) *is not bounded, then* $0.(c_1)_g(c_2)_g...$ *is irrational.*

To illustrate the power of Theorem 1 we formulate a further corollary.

Corollary 2. *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 $(\gamma, \mathcal{D})$ 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 $(c_1)_\gamma(c_2)_\gamma \dots$ is not periodic.*

Proof. There exists in $\mathbb{Z}_\mathbb{K}$ only finitely many pairwise not associated elements with given norm. Let $\mathcal{A}$ be such a set. There exist by Dirichlet's theorem $\varepsilon_1, \dots, \varepsilon_r$ such that every unit of infinite order of $\mathbb{Z}_\mathbb{K}$ can be written in the form $\varepsilon_1^{m_1} \cdots \varepsilon_r^{m_r}$. Setting $\mathcal{B} = \{\varepsilon_1, \dots, \varepsilon_r\}$ apply Theorem 1. $\square$

Notice that in the rational and in the imaginary quadratic fields there are only 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.

Problem 2. *Let $A > 0$ and $B \geq \max\{2, A\}$. Establish all repunits with respect to the GNS $\left(\frac{-A+\sqrt{A^2-4B}}{2}, \{0, 1, \ldots, B-1\}\right)$ for various values of A, B.*

3.2. Results on rational integers

We consider analogous questions on rational integers.

Theorem 2. *Let* $[\mathbb{L}:\mathbb{Q}]=\ell\geq 2$ *and* $\gamma\in\mathbb{Z}_{\mathbb{L}},\mathcal{D}\subset\mathbb{Z}$ *such that* $\gamma^{\ell}\notin\mathbb{Z}$ *and* $\mathcal{D}$ *is a complete residue system modulo* γ. *Assume that* $(\gamma,\mathcal{D})$ *is a GNS in* $\mathbb{Z}_{\mathbb{L}}$. *Let* $n_1,n_2,\ldots$ *be an unbounded sequence of rational integers. Then* $0.(n_1)_{\gamma}(n_2)_{\gamma}\ldots\notin\mathbb{Q}$.

Similarly to Theorem 1 the proof is rooted in

Lemma 2. *Let* $[\mathbb{L}:\mathbb{Q}]=\ell\geq 2$ *and* $\gamma\in\mathbb{Z}_{\mathbb{L}},\mathcal{D}\subset\mathbb{Z}$ *such that* $\gamma^{\ell}\notin\mathbb{Z}$ *and* $\mathcal{D}$ *is a complete residue system modulo* γ. *Assume that* $(\gamma,\mathcal{D})$ *is a GNS in* $\mathbb{Z}_{\mathbb{L}}$. *For any* $w\in\mathcal{D}^*$ *there are only finitely many* $n\in\mathbb{Z}$ *such that* $(n)_{\gamma}=w_1w^k$, *where* w_1 *is a suffix of* w.

A simple consequence of this lemma is

Corollary 3. *Let $\mathbb{L}, \gamma, \mathcal{D}$ be as in Lemma 2. There are only finitely many rational integers, which are repunits in the GNS $(\gamma, \mathcal{D})$, i.e., $(n)_\gamma = 1^k$.*

Scats of the proof of Corollary 3. We have $\mathbb{Q}(\gamma) = \mathbb{L}$, thus the degree of γ is ℓ. Denote $\gamma^{(j)}, j = 1, \ldots, \ell$ the conjugates of γ. We have:

- $|\gamma^{(j)}| > 1, j = 1, \ldots, \ell$ because $(\gamma, \mathcal{D})$ is a GNS.
- If $1 \le i < j \le \ell$ then $\gamma^{(i)}$ and $\gamma^{(j)}$ are multiplicatively independent by Dobrowolski, 1979.

If $n \in \mathbb{Z}$ such that $(n)_\gamma = 1^k$ with some k then $n = \sum_{j=0}^{k-1} \gamma^j = \frac{\gamma^k - 1}{\gamma - 1}$. Let $\gamma' \neq \gamma$ be a conjugate of γ. We may assume $1 < |\gamma'| \leq |\gamma|$, but γ'/γ is not a root of unity. Then $n = \sum_{j=0}^{k-1} \gamma'^j = \frac{\gamma'^k - 1}{\gamma' - 1}$ too. Thus

$$\frac{\gamma^k - 1}{\gamma - 1} = \frac{\gamma'^k - 1}{\gamma' - 1}$$

or, equivalently,

$$\left(\frac{\gamma}{\gamma'}\right)^k - 1 = \frac{\gamma' - \gamma}{\gamma - 1} \frac{1}{\gamma'^k}.$$

If $|\gamma'| < |\gamma|$ simply analysis, otherwise Bakery. $\square$

3.3. 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

$$N_{\mathbb{K}/\mathbb{Q}}(L(\mathbf{X})) = \prod_{j=1}^{k} (\alpha_1^{(j)} X_1 + \cdots + \alpha_s^{(j)} X_s) = t, \qquad (3)$$

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.

Now we are in the position to state our Mahler-type result on the solutions of (3).

Theorem 3. *Let* $(\mathbf{x}_n) = ((x_{n1}, \ldots, x_{ns}))$ *be a sequence of solutions of (3), 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.*

Outline of the proof By a deep theorem of W.M. Schmidt there exist a finite set $\mathcal{A} \subset \mathbb{Z}_{\mathbb{K}}$ such that

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

with $\mu \in \mathcal{A}$ and with a unit $u_n \in \mathbb{Z}_{\mathbb{K}}$. Taking conjugates we obtain the system of linear equations

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

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 $\mathbb{K}$. The assumption (x_{nj}) is not ultimately zero implies that (x_{nj}) is not bounded. Now we can apply Theorem 1.$\square$

Corollary 4. *Let $g \geq 2$ be an integer. There are only finitely many g-repunits among the solutions of* (3)*.*

Remark 1. *If $\mathbb{K}$ is a real quadratic number field* (3) *is called Pell equation, which solutions can be expressed by the union of finitely many linear recursive sequences. In this case Theorem 3 is included implicitly in Theorem 1 of Barat, Frougny and Pethő.*

Győry, Mignotte and Shorey, 1990 proved with the notation of Theorem 3 that if the set of the j-th coordinate of the solutions of (3) *is not bounded then the greatest prime factor of them tends to infinity. Our Theorem 3 shows that their assumption always holds if* (3) *has infinitely many solutions, which j-th coordinates is non-zero.*

4. Families of GNS

B. Kovács, 1981: If $\mathbb{K} = \mathbb{Q}$ then for any $\gamma \in \mathbb{Z}_{\mathbb{L}}$ there exists $N_1 = N_1(\gamma)$ such that $(\gamma - m, \{0, 1, \ldots, N_{\mathbb{L}/\mathbb{Q}}(\gamma - m)\})$ **is** a GNS in $\mathbb{Z}_{\mathbb{L}}$ for all $m \geq N_1$. Moreover there exists $N_2 = N_2(\gamma)$ such that $(\gamma + m, \{0, 1, \ldots, N_{\mathbb{L}/\mathbb{Q}}(\gamma + m)\})$ **is not** a GNS in $\mathbb{Z}_{\mathbb{L}}$ for all $m \geq N_2$.

Refinements by Akiyama and Rao, Scheicher and Thuswaldner. The proofs are based on the principle: Denote by $p(x)$ the minimal polynomial of γ. For $m \in \mathbb{N}$ we have $p(\mp m) = N_{\mathbb{L}/\mathbb{Q}}(\gamma \pm m)$. If m is large enough then $p(m)$ is dominating among the coefficients of $p(x+m)$ and $(\gamma - m, \{0, 1, \ldots, p(m) - 1\})$ is a GNS, while $|p(-m)| \in \{0, 1, \ldots, |p(-m-1)| - 1\}$, hence $(\gamma + m, \{0, 1, \ldots, |p(-m)| - 1\})$ is not a GNS.

In relative extensions we does not have natural ordering of the elements of the base field! A.P.and Thuswaldner, 2018 found a way to overcome this difficulty.

Let $\mathbb{K}$ be a number field of degree k. Let $\mathcal{F}$ be a bounded fundamental domain for the action of $\mathbb{Z}^k$ on $\mathbb{R}^k$, *i.e.*, a set that satisfies $\mathbb{R}^k = \mathcal{F} + \mathbb{Z}^k$ without overlaps. Let $\mathcal{O}$ be an order in $\mathbb{Z}_{\mathbb{K}}$, $\omega_1 = 1, \omega_2, \ldots, \omega_k$ be a $\mathbb{Z}$-basis of $\mathcal{O}$ and let $\alpha \in \mathcal{O}$ be given. Define

$$D_{\mathcal{F},\alpha} = \left\{ \tau \in \mathcal{O} \,:\, \frac{\tau}{\alpha} = \sum_{j=1}^{k} r_j \omega_j,\, (r_1, \ldots, r_k) \in \mathcal{F} \right\}. \tag{4}$$

Lemma 3. *$D_{\mathcal{F},\alpha}$ is a complete residue system modulo α.*

Set $\mathbf{e}_1 = (1, 0, \ldots, 0) \in \mathbb{R}^k$. int_+ is the interior taken w.r.t. the subspace topology on $\{(r_1, \ldots, r_k) \in \mathbb{R}^k \, : \, r_1 \geq 0\}$.

Theorem 4. *Let $\mathbb{K}$ be a number field of degree k and let $\mathcal{O}$ be an order in $\mathbb{K}$. Let a bounded fundamental domain $\mathcal{F}$ for the action of $\mathbb{Z}^k$ on $\mathbb{R}^k$ be given. Suppose that*

- $\mathbf{0} \in \mathrm{int}(\mathcal{F} \cup (\mathcal{F} - \mathbf{e}_1))$ *and*
- $\mathbf{0} \in \mathrm{int}_+(\mathcal{F})$.

Let $\mathbb{L}$ be a finite extension of $\mathbb{K}$ and $\gamma \in \mathbb{Z}_{\mathbb{L}}$. Then there is $\eta > 0$ such that $(\gamma + \alpha, D_{\mathcal{F}, N_{\mathbb{L}/\mathbb{Q}}(\gamma+\alpha)})$ is a GNS whenever $\alpha = m_1\omega_1 + \cdots + m_k\omega_k \in \mathcal{O}$ satisfies $\max\{1, |m_2|, \ldots, |m_k|\} < \eta m_1$.

Remark 2. *Note that this implies that for each bounded fundamental domain $\mathcal{F}$ satisfying*

- $\mathbf{0} \in \mathrm{int}(\mathcal{F} \cup (\mathcal{F} - \mathbf{e}_1))$ *and*
- $\mathbf{0} \in \mathrm{int}_+(\mathcal{F})$.

the family $\mathcal{G}_\mathcal{F}$ contains infinitely many GNS.

Corollary 5. *Let* $\mathbb{K}$ *be a number field of degree* k *and let* $\mathcal{O}$ *be an order in* $\mathbb{K}$. *Let a bounded fundamental domain* $\mathcal{F}$ *for the action of* $\mathbb{Z}^k$ *on* $\mathbb{R}^k$ *be given such that* $\mathbf{0} \in \mathrm{int}(\mathcal{F})$. *Let* $\mathbb{L}$ *be a finite extension of* $\mathbb{K}$ *and* $\gamma \in \mathbb{Z}_{\mathbb{L}}$. *Then there is* $\eta > 0$ *such that* $(\gamma + \alpha, D_{\mathcal{F}, N_{\mathbb{L}/\mathbb{Q}}(\gamma+\alpha)})$ *has the finiteness property whenever* $\alpha = m_1\omega_1 + \cdots + m_k\omega_k \in \mathcal{O}$ *satisfies* $\max\{1, |m_2|, \ldots, |m_k|\} < \eta|m_1|$.

4.2. Families on non-GNS

Theorem 5. *Let* $\mathbb{K}$ *be a number field and let* $\mathcal{O}$ *be an order in* $\mathbb{K}$*. Let a bounded fundamental domain* $\mathcal{F}$ *for the action of* $\mathbb{Z}^k$ *on* $\mathbb{R}^k$ *be given. Suppose that* $\mathbf{0} \in \mathrm{int}_{-}(\mathcal{F} - \mathbf{e}_1)$*. Let* $\mathbb{L}$ *be a finite extension of* $\mathbb{K}$ *and* $\gamma \in \mathbb{Z}_{\mathbb{L}}$*. There exists* $M \in \mathbb{N}$ *such that* $(\gamma + m, D_{\mathcal{F},N_{\mathbb{L}/\mathbb{Q}}(\gamma+m)})$ *is not a GNS for* $m \geq M$*.*

4.3. GNS in number fields

Proposition 1 (Kovács and Pethő, 1991). *Let $\mathcal{O}$ be an order in the algebraic number field $\mathbb{K}$. There exist $\alpha_1, \ldots, \alpha_t \in \mathcal{O}$, $n_1, \ldots, n_t \in \mathbb{Z}$, and $N_1, \ldots, N_t$ finite subsets of $\mathbb{Z}$, which are all effectively computable, such that $(\alpha, \{0, 1, \ldots, N_{\mathbb{K}/\mathbb{Q}}(\alpha)\})$ is a GNS in $\mathcal{O}$ if and only if $\alpha = \alpha_i - h$ for some integers i, h with $1 \leq i \leq t$ and either $h \geq n_i$ or $h \in N_i$.*

Pethő and Thuswaldner, 2018 proved that the relation between power integral bases and GNS is usually stronger, the theorem of Kovács and Pethő describes a kind of "boundary case" *viz.* a case where $0 \in \partial\mathcal{F}$.

Theorem 6. *Let $\mathcal{O}$ be an order in the algebraic number field $\mathbb{K}$. Let $\mathcal{F}$ be a bounded fundamental domain for the action of $\mathbb{Z}$ on $\mathbb{R}$. If $0 \in \mathrm{int}(\mathcal{F})$ then all but finitely many generators of power integral bases of $\mathcal{O}$ form a basis for a GNS. Moreover, the exceptions are effectively computable.*

Evertse, Győry, Pethő and Thuswaldner, 2019 generalized to étale orders.

Partial answer to Problem 1.

Theorem 7. *Let* $\mathcal{O}$ *be an effectively given étale order, and* $\mathcal{D}$ *a given finite subset of* $\mathbb{Z}$ *containing* 0*. Then there exist only finitely many, effectively computable* $\gamma \in \mathcal{O}$ *such that* $(\gamma, \mathcal{D})$ *ia a GNS.*

Proof. Let $\gamma \in \mathcal{O}$ and $\mathcal{D} \subset \mathbb{Z}$ be such that $(\gamma, \mathcal{D})$ is a GNS. The set $\mathcal{D}$ has to be a complete residue system of $\mathcal{O}$ modulo γ, which is only possible if $|N(\gamma)| = |\mathcal{D}|$. If there is no such γ then we are done. Otherwise, if $\mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Q} = \mathbb{K}_1 \times \ldots \times \mathbb{K}_\ell$ and $\mathbb{K}_h$ are either the rational or an imaginary quadratic number field for all $h = 1, \ldots, \ell$ then there are only finitely many α with $|N(\gamma)| = |\mathcal{D}|$ and our assertion holds again.

We now assume that there are infinitely many $\gamma \in \mathcal{O}$ such that $|N(\gamma)| = |\mathcal{D}|$. If $(\gamma, \mathcal{D})$ is a GNS then there exist for all $\alpha \in \mathcal{O}$ an integer L and $d_i \in \mathcal{D}, i = 0, \dots, L$ such that

$$\alpha = \sum_{i=0}^{L} d_i \gamma^i,$$

hence $\mathcal{O}$ is monogenic. By a deep theorem of Evertse and Győry there exist only finitely many $\mathbb{Z}$-equivalence classes of $\beta \in \mathcal{O}$ such that $\mathcal{O} = \mathbb{Z}[\beta]$. Hence there is such a β and $u \in \mathbb{Z}$ with $\alpha = \beta + u$. For fixed β there are only finitely many effectively computable $u \in \mathbb{Z}$ with $|N(\beta + u)| = |\mathcal{D}|$, thus the assertion is proved. $\square$

5. Integers with bounded number of non-zero digits

Let $g_1, g_2 \geq 2$ be integers.

• Senge and Straus, 1973: the number of integers, the sum of whose digits in each of the bases g_1 and g_2 lies below a fixed bound, is finite if and only if g_1 and g_2 are multiplicatively independent.

• Stewart, 1980: gave an effective version.

• Schlickewei, 1990: ineffective generalization to more than two bases.

• Pethő and Tichy, 1993: generalization to numeration systems based on linear recursive sequences and to GNS.

Theorem 8. *Let* $[\mathbb{L} : \mathbb{Q}] = \ell \geq 2$ *and* $\gamma \in \mathbb{Z}_{\mathbb{L}}, \mathcal{D} \subset \mathbb{Z}$ *such that* $\gamma^\ell \notin \mathbb{Z}$ *and* $\mathcal{D}$ *is a complete residue system modulo* γ. *Assume* *that* $(\gamma, \mathcal{D})$ *is a GNS in* $\mathbb{Z}_{\mathbb{L}}$. *Denote* $r_\gamma(\alpha)$ *the number of non-zero digits in the representation of* $\alpha \in \mathbb{Z}_{\mathbb{L}}$ *in* $(\gamma, \mathcal{D})$. *For any* $c > 0$ *there are only finitely many* $n \in \mathbb{Z}$ *such that* $r_\gamma(n) \leq c$.