On diophantine properties of generalized number systems - finite and periodic representations

Attila Pethő

Department of Computer Science
University of Debrecen, Debrecen, Hungary

One World Numeration Seminar
July 14, 2020.

.

1. Radix representation of rational integers

Distinction between (algebraic) **integer** and **rational integer**.

Let $g \geq 2$. If $n \in \mathbb{Z}, n > 0$ then there exist uniquely $l \geq 0, 0 \leq a_0, \ldots, a_l < g$ such that

$$n = n_l g^l + n_{l-1} g^{l-1} + \ldots + n_0.$$

Let $(n)_g = n_0 n_1 \ldots n_l$ the word (sequence) of digits of the g-ary representation of n, e.g. $2020 = 2 \cdot 10^3 + 0 \cdot 10^2 + 2 \cdot 10^1 + 0 \cdot 10^0 = 3 \cdot 5^4 + 1 \cdot 5^3 + 0 \cdot 5^2 + 4 \cdot 5^1 + 0 \cdot 5^0$, thus

$(2020)_{10} = 0202, (2020)_5 = 04013$. $(0)_g = 0$ for all $g \geq 2$.

Unfamiliar notation, but simplifies considerably the manipulation with the equations.

General question: Assume that $(n)_g$ admits some property. What can we prove about the set of such n. The property can be e.g. periodicity, subword of special shape, few non-zero digits, etc.

If $(n)_g = b^l$ then n is called a *base g repdigit*, if $b = 1$ then *repunit*. Plainly

$$(n)_g = b^l \text{ if and only if } n = b\frac{g^l - 1}{g - 1}.$$

Does there exist integers which are repunits in two different bases?

Yes: trivial examples $(1)_g = 1, (n)_g = 1^l, h = n - 1 \Rightarrow (n)_h = 1^2$.
Non trivial examples

$$\begin{aligned} (31)_5 &= 1^3 \text{ and } (31)_2 = 1^5, \\ (8191)_{90} &= 1^3 \text{ and } (8191)_2 = 1^{13}. \end{aligned}$$

Goormaghtigh conjecture: there are no more non-trivial examples.

Reformulation to the language of Diophantine equations: *If* $(x, y, n, m), x, y > 1, m, n > 2, x \neq y$ *is a solution of*

$$\frac{x^n - 1}{x - 1} = \frac{y^m - 1}{y - 1}$$

then $(x, y, n, m) = (5, 2, 3, 5)$ *and* $(90, 2, 3, 13)$.

When either the bases x and y, or the base x and the exponent n, or the exponents m and n are fixed, then our equation has finitely many solutions.

2. Radix representation in algebraic number fields

Let $\mathbb{K}$ an algebraic number field with ring of integers $\mathbb{Z}_{\mathbb{K}}$.
The pair $(\gamma, \mathcal{D})$, where $\gamma \in \mathbb{Z}_{\mathbb{K}}$ and $\mathcal{D} \subset \mathbb{Z}$ is a complete residue system modulo γ is called a *generalized number system with finiteness property*, GNS, in $\mathbb{Z}_{\mathbb{K}}$ 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 $a_0 a_1 \ldots a_\ell$ 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 $\mathbb{Z}[\sqrt{-7}]$. **Pelda!**

This GNS is a special case of GNS in a 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.

3. 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 $(h^{n_1})_g(h^{n_2})_g\ldots$ is not periodic. 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

Problem 1. *Is it true that if* $(n_i)_{i=1}^{\infty}$ *is a strictly increasing sequence of integers then* $(h^{n_1})_g(h^{n_2})_g \ldots$ *is not automatic?*

3.1. Results on power sums

Let $0 \notin \mathcal{A}, \mathcal{B} \subset \mathbb{Z}_{\mathbb{K}}$ 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: $\mathbb{K} = \mathbb{Q}, \mathcal{A} = \{1\}, \mathcal{B} = \{2, 3\}$ then

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

Theorem 1. *Let $s \geq 1$ and $\mathcal{A}, \mathcal{B}$ as above. Assume that $c_n \in S(\mathcal{A}, \mathcal{B}, s)$ and (c_n) has infinitely many distinct terms. If $(\gamma, \mathcal{D})$ is a GNS in $\mathbb{Z}_{\mathbb{K}}$ and the elements of $\{\gamma \cup \mathcal{B}\}$ are multiplicatively independent then the infinite word $(c_1)_\gamma (c_2)_\gamma \ldots$ is not periodic.*

With $\mathbb{K} = \mathbb{Q}, \mathcal{A} = \{1\}, \mathcal{B} = \{h\}, \gamma = g$ we get Mahler's result, when g, h are multiplicatively independent.

The proof of Theorem 1 is based on the following

Lemma 1. *Let $(\gamma, \mathcal{D})$ be a GNS in $\mathbb{Z}_{\mathbb{K}}$ and $w, w_1 \in \mathcal{D}^*$. Assume that the elements of $\{\gamma \cup \mathcal{B}\}$ are multiplicatively independent. There are only finitely many $U \in S(\mathcal{A}, \mathcal{B}, s)$ such that $(U)_\gamma = w_1 w^k$, and $(U)_\gamma = w^k w_1$.*

Problem 2. *Let $\mathcal{A}, \mathcal{B}, \gamma, \mathcal{D}, w_1$ as in Lemma 1. There are only finitely many $U \in S(\mathcal{A}, \mathcal{B}, s)$ and $w \in \mathcal{D}^*$ such that $(U)_\gamma = w_1 w^k$ with $k \geq k_0$.*

This is true if $\mathbb{K} = \mathbb{Q}, \mathcal{A} = \{1\}, \mathcal{B} = \{h\}$ and k is fixed. The equation $(h^x)_g = w_1 w^k$ has only finitely many solutions in $w \in \{0, 1, \ldots, g-1\}^*$ and $x \geq 0$ integer.

Corollary 1. *Let γ be an algebraic integer. Let $\mathbb{K} = \mathbb{Q}(\gamma)$ and $\mathcal{D} \subset \mathbb{Z}$ and assume that $(\gamma, \mathcal{D})$ is a GNS in $\mathbb{Z}_{\mathbb{K}}$. For any $m \in \mathbb{Z}$ and $w, w_1 \in \mathcal{D}^*$ there exist only finitely many $\beta \in \mathbb{Z}_{\mathbb{K}}$ of norm m such that $(\beta)_\gamma = w_1 w^k$ or $w^k w_1$.*

Proof. If γ is rational or imaginary quadratic then there are in $\mathbb{Z}_{\mathbb{K}}$ only finitely many elements with given norm, hence the statement holds automatically.

Otherwise 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 $\varepsilon_1, \ldots, \varepsilon_r$ such that every unit of infinite order of $\mathbb{Z}_{\mathbb{K}}$ can be written in the form $\varepsilon_1^{m_1} \cdots \varepsilon_r^{m_r}$. Set $\mathcal{B} = \{\varepsilon_1, \ldots, \varepsilon_r\}$ and apply Theorem 1. □

3.2. 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 $\alpha_1 = 1, \alpha_2, \ldots, \alpha_k \in \mathbb{Z}_{\mathbb{K}}$ be $\mathbb{Q}$-linear independent elements and $L(\mathbf{X}) = \alpha_1 X_1 + \cdots + \alpha_k X_k$. Consider the norm form equation

$$N_{\mathbb{K}/\mathbb{Q}}(L(\mathbf{X})) = \prod_{j=1}^{k} (\alpha_1^{(j)} X_1 + \cdots + \alpha_k^{(j)} X_k) = t, \qquad (2)$$

where $0 \neq t \in \mathbb{Z}$, which solutions are searched in $\mathbb{Z}$. Notice that $N_{\mathbb{K}/\mathbb{Q}}(L(\mathbf{X})) \in \mathbb{Z}[\mathbf{X}]$.

If $k = 2, \alpha_2 = \sqrt{d}, 0 < d \neq \square$ then $N_{\mathbb{K}/\mathbb{Q}}(X_1 + \sqrt{d}X_2) = X_1^2 - dX_2^2$ $\Rightarrow$ (2) is a Pell equation.

Theorem 2. *Let* $(\mathbf{x}_n) = ((x_{n1}, \ldots, x_{nk}))$ *be a sequence of different solutions of* (2). *Let* $1 \le j \le k$ *be fixed,* $g \ge 2$ *and* $w, w_1 \in \{0, 1, \ldots, g-1\}^*$. *If* (x_{nj}) *is finite or has infinitely many nonzero terms then the equation* $(|x_{nj}|)_g = w_1 w^u$ *has only finitely many solutions in* n, u.

Outline of the proof If $\mathbb{K}$ is $\mathbb{Q}$ or an imaginary quadratic number field then (2) has finitely many solutions $\Rightarrow$ we are done.

By a deep theorem of W.M. Schmidt (1982) there exist a finite set $\mathcal{A} \subset \mathbb{Z}_{\mathbb{K}}$ such that

$$\alpha_1 x_{n1} + \cdots + \alpha_k x_{nk} = \mu u_n$$

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

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

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 non-zero for infinitely many n implies that (x_{nj}) is not bounded. Now we can apply Theorem 1.□

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

3.3. Results on rational integers

Van der Poorten and Schlickewei, 1982: the elements of $S(\mathcal{A}, \mathcal{B}, s)$ are growing exponentially. Now we show 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.

Theorem 3. *Let $\mathbb{K}$ be an algebraic number field of degree $k \geq 2$, $(\gamma, \mathcal{D})$ be a GNS 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 1. *Assume that* $\gamma^\ell = m$ *for some integers* $\ell \geq 1$, *and* $m\mathbb{Z}$. *As* $(\gamma, \mathcal{D})$ *is a GNS in* $\mathbb{Z}_\mathbb{K}$ *we have* $\mathbb{K} = \mathbb{Q}(\gamma)$, *i.e., the degree of* γ *is exactly* 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, as* $\gamma^\ell = m, \ell = 1, \ldots, k$, *hence* γ^ℓ/γ^j *are roots of unity. Thus our assumption is necessary.*

Scats of the proof of Theorem 3. Let $w_1 \in \mathcal{D}^*$ be given. By unicity of expansions there is exactly one U with $(U)_\gamma = w_1$. Thus our statement is true if $w = \lambda$.

Let $w = d_0 \dots d_{h-1}$ and $q = d_0 + d_1\gamma + \dots + d_{h-1}\gamma^{h-1}$. Set $q_0 = 0$ if $w_1 = \lambda$, and $q_0 = f_0 + f_1\gamma + \dots + f_{g-1}\gamma^{g-1}$ provided $w_1 = f_0 \dots f_{g-1}$.

Let $n \in \mathbb{Z}$ and assume that $(t(n))_\gamma = w_1 w^u$ holds for some $k > 0$.

It means that

$$\begin{aligned} t(n) &= q_0 + \gamma^g \sum_{i=0}^{u-1} \gamma^{ih} \sum_{j=0}^{h-1} d_j \gamma^j \\ &= q_0 + \gamma^g \sum_{i=0}^{u-1} q\gamma^{ih} \\ &= q_0 + q\gamma^g \frac{\gamma^{hu} - 1}{\gamma^h - 1} \\ &= \frac{q\gamma^g}{\gamma^h - 1}\gamma^{hu} + q_0 - \frac{q\gamma^g}{\gamma^h - 1}. \end{aligned}$$

Setting

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

we get the system of equations

$$\begin{aligned} t^{(1)}(n) - \alpha^{(1)}(\gamma^{(1)h})^u + \beta^{(1)} &= 0, \\ t^{(2)}(n) - \alpha^{(2)}(\gamma^{(2)h})^u + \beta^{(2)} &= 0 \end{aligned}$$

in the unknown integers n, u. Computing the resultant of the polynomials on the LHS's with respect to the variable n we get the necessary condition

$$\left(\alpha_1(\gamma^{(1)h})^u + \alpha_2(\gamma^{(2)h})^u\right)^v + F_3\left((\gamma^{(1)h})^u, (\gamma^{(2)h})^u\right) = 0, \quad (3)$$

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

$$\left|F_3\left((\gamma^{(1)h})^u, (\gamma^{(2)h})^u\right)\right| \leq c_1|\gamma^{(1)}|^{hu(v-1)} \quad (4)$$

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.

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 Shorey and Tijdeman (1986) 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

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

Comparing this lower bound with (4) implies our statement.

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

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

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

whenever $|u| \geq c_6$. $\square$

Corollary 3. *Let $\mathbb{K}$ be an algebraic number field of degree $k \geq 2$ and $(\gamma, \mathcal{D})$ be a GNS in $\mathbb{Z}_{\mathbb{K}}$. Let $t(X) \in \mathbb{Z}_{\mathbb{K}}[X]$. Assume that γ has two conjugates whose quotient is not a root of unity. Then the infinite word $W = (t(1))_\gamma (t(2))_\gamma (t(3))_\gamma \ldots$ is not ultimately periodic.*

Idea of the proof. Omitting, if necessary, some starting members of $(t(n))$ we may assume that W is periodic, i.e. $W = H^\infty$ with $H \in \mathcal{D}^h$.

We have $(t(n))_\gamma = c_{n0} H^{e_n} c_{n1}$ for all $n \geq 1$, where c_{n0} is a a suffix and c_{n1} is a a prefix of H and $e_n \geq 0$. As $|t(n)| \to \infty$ the length of $(t(n))_\gamma, n = 1, 2, \ldots$, thus e_n is not bounded. There exists an infinite sequence $k_1 < k_2 < \ldots$ of integers such that $l((t(k_{n+1)})_\gamma) > l((t(k_n))_\gamma)$.

Write $(t(k_n))_\gamma = c_{k_n 0} H^{e_{k_n}} c_{k_n 1}$. 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 $c_{k_n 0}$ and $c_{k_n 1}$ are fixed, say $c_{k_n 0} = C_0$ and $c_{k_n 1} = C_1$. In the sequel 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 $(c_n)_\gamma = C_0 H^{e_n}$ for infinitely many n. Contradition to Theorem 3. $\square$

Conjecture 1. *Let $\mathbb{K}$ be an algebraic number field and $(\gamma, \mathcal{D})$ be a GNS in $\mathbb{Z}_{\mathbb{K}}$. Let $t(X) \in \mathbb{Z}_{\mathbb{K}}[X]$. Then the infinite word $(t(1))_\gamma (t(2))_\gamma (t(3))_\gamma \ldots$ is not automatic.*

If $\mathbb{K} = \mathbb{Q}$ and $t(x) = x$ then $C_\gamma = 0.(1)_\gamma (2)_\gamma (3)_\gamma \ldots$ is the Champernowne number. He proved in 1933 that C_{10} is normal. Nakai and Shiokawa (1962): C_γ in base γ is normal. Mahler (1937): C_{10} is transcendental.

Generalization: Let $(t(1))_\gamma (t(2))_\gamma (t(3))_\gamma \ldots = s_1 s_2 \ldots$, which is a word over $\mathcal{D}$. The series $\sum_{j=1}^{\infty} s_j \gamma^{-j}$ defines a complex number. Is it always transcendental?

4. Rational integers with fixed representation word

Fix $w \in \mathbb{Z}^*$. Search for number systems $(\gamma, \mathcal{D})$ and rational integers n such that $(n)_{(\gamma,\mathcal{D})} = w$. The underlying idea: 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, thus $\alpha \in \mathbb{Z}$ is only possible if $w_2, \dots, w_\ell = 0$ and $\alpha = w_1$.

What about if $k < \ell - 1$? Search γ as a root of the polynomial $X^k + g_{k-1}X^{k-1} + \ldots + g_0$. Then $\gamma^j = \sum_{i=0}^{k-1} g_{ij}\gamma^i$ holds for all $j \geq 0$ where g_{ij} are polynomials of $g_0, \ldots, g_{k-1}$ with integer coefficients. Thus

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

As $1, \gamma, \ldots, \gamma^{k-1}$ are $\mathbb{Q}$-linearly independent $\alpha \in \mathbb{Z}$ holds if and only if $\sum_{j=0}^{\ell-1} w_{j+1} g_{ij} = 0$ for $i = 1, \ldots, k-1$. These are systems of diophantine equations.

For example for $k = 2$ we have

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

The same data for $k = 3$.

j	0	1	2	3	4	5	6
g_{0j}	1	0	0	$-g_0$	$g_0 g_2$	$-g_0 g_2^2 + g_0 g_1$	$g_0 g_2^3 - g_0 g_1^2 - g_0 g_1 g_2 + g_0^2$
g_{1j}	0	1	0	$-g_1$	$g_1 g_2 - g_0$	$-g_1 g_2^2 + g_0 g_2 + g_1^2$	$g_1 g_2^3 - g_0 g_2^2 - 2 g_1^2 g_2 + 2 g_0 g_1$
g_{2j}	0	0	1	$-g_2$	$g_2^2 - g_1$	$-g_2^3 + 2 g_1 g_2 - g_0$	$g_2^4 - 3 g_1 g_2^2 + 2 g_0 g_2 + g_1^2$

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. $S \leftarrow \emptyset$; $\mathcal{D} \leftarrow \{w_1, \dots, w_\ell\}$;
2. for $k \leftarrow 2$ to ℓ do $\{$
3. for $i \leftarrow 1$ to $k-1$ do $L_i \leftarrow \sum_{j=0}^{\ell-1} w_{j+1} g_{ij}$;
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 $\underline{\mathrm{g}} = (g_0, \ldots, g_{k-1}) \in S_1$ do $\{$

7. $S_1 \leftarrow S_1 \setminus \{\underline{\mathrm{g}}\}$;

8. if $g_0 | x - y$ for all $x, y \in \mathcal{D}_w$ and $P(X) = X^k + g_{k-1}X^{k-1} + \ldots + g_0$ is irreducible then

9. $S \leftarrow \{(\gamma, \mathcal{D}, n)\}$, where γ is a zero of $P(X)$, $\mathcal{D} \supseteq \mathcal{D}_w$ is a complete residue system modulo g_0 and $n = \sum_{j=0}^{\ell-1} w_{j+1} g_{0j}$

$\}$ (* end of the $\underline{\mathrm{g}}$ cycle*)

$\}$ (* end of the k cycle*)

Example Search for all algebraic integer γ such that $(n)_\gamma = 0202$, i.e,

$$2\gamma^3 + 2\gamma = n \to n = 2m.$$

Plainly $\deg \gamma \leq 3$.

$\deg \gamma = 3 \to \gamma^3 + \gamma - m = 0$ and $|m| \geq 3, \{0, 2\} \subset \mathcal{D}$.

$\deg \gamma = 2 \to (g_1^2 - g_0 + 1)\gamma + g_0 g_1 - m = 0$ thus $m = g_1^3 + g_1, \quad g_0 = g_1^2 + 1, |g_1| \geq 1$.

$\deg \gamma = 2 \to m = g^3 + g$.

5. Repunits in number systems

If $(\gamma, \mathcal{D})$ is fixed then there there are by Theorem 3 only finitely many rational integers, which are repunits in $(\gamma, \mathcal{D})$.

Similarly, 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 more precise description. For $i \geq 0$ let

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

Proposition 1. *Let $\mathbb{K}$ be a number field of degree $k \geq 2$. 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 $Q_m(X) = \sum_{i=1}^{k} X^i + m$, $0, \pm 1 \neq m \in \mathbb{Z}$ and $\mathcal{D}$ is a complete residue system modulo m including* $0, 1$ *then* $(1-m)_{(\gamma,\mathcal{D})} = 1^{k+1}$.

• *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* $(G_{k+1}(m))_{(\gamma,\mathcal{D})} = 1^{k+2}$.

Proof. Only the third assertion. The recursion $G_{i+1}(X) = (X-1)G_i(X) + 1$, $i \geq 0$ is easy to verify. Thus

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

hence

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

which means

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

Remark 2. *By the Algorithm, there is no rational integer, which is a repunit of length five in a quadratic number field.*

Theorem 4. *If $\mathbb{K}$ 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. Let $\gamma \in \mathbb{Z}_{\mathbb{K}}$ 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. Then

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

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, then $f(x)$ 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. $\square$

Imre Kátai and Júlia Szabó (1975) characterized the CNS in the imaginary, and Kátai and Kovács (1980) in the real quadratic number fields. Their results is

Theorem 5. *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 $(\gamma, \{0, 1, \ldots, |b| - 1\})$ is a CNS in $\mathbb{Z}_{\mathbb{K}}$ if and only if $1 \leq a \leq b$, and $b \geq 2$.*

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.

If $1 \leq a \leq b, b \geq 2$ be fixed then, by Theorem 3, there are only finitely many rational integer repunits in the CNS $\left(\frac{-a+\sqrt{a^2-4b}}{2}, \{0, 1, \ldots, b - 1\}\right)$. We did not found any other CNS, in which some rational integer is a repunit.

Conjecture 2. *The only rational integer repunits in*

$$\left(\frac{-1+\sqrt{1-4m}}{2}, \{0, 1, \ldots, m-1\}\right)$$

and

$$\left(\frac{-m+\sqrt{-3m^2+4m-4}}{2}, \{0, 1, \ldots, m^2-m\}\right)$$

are $1-m$ *and* m^3-2m^2+2m *respectively.*

Probably the following much stronger conjecture is still true.

Conjecture 3. *Apart from the examples of Conjecture 2 there are no CNS in quadratic number fields in which there are rational integer repunits.*

6. GNS with given digit set

Problem 3. *Let $\mathcal{D} \subset \mathbb{Z}$ be given. How many $\gamma \in \mathbb{Z}_{\mathbb{K}}$ exist such that $(\gamma, \mathcal{D})$ is a GNS in $\mathbb{Z}_{\mathbb{K}}$?*

For $\mathbb{K} = \mathbb{Q}$ the answer is: at most two, $g = \pm|\mathcal{D}|$!
Same if $\mathbb{K}$ is imaginary quadratic, except when $\mathbb{K} = \mathbb{Q}(i)$ and $\mathbb{K} = \mathbb{Q}\left(\frac{\pm 1 \pm \sqrt{-3}}{2}\right)$.

Theorem 6 (Evertse, Győry, Pethő and Thuswaldner (2019))**.** *Let $\mathbb{K}$ be number field and $0 \in \mathcal{D} \subset \mathbb{Z}$. Then there exist only finitely many, effectively computable $\gamma \in \mathbb{Z}_{\mathbb{K}}$ such that $(\gamma, \mathcal{D})$ is a GNS.*

Proof. Let $\gamma \in \mathbb{Z}_{\mathbb{K}}$ 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 $\mathbb{Z}_{\mathbb{K}}$ modulo γ, which is only possible if $|N(\gamma)| = |\mathcal{D}|$. If there is no such γ then we are done. If $\mathbb{K} = \mathbb{Q}$ or an imaginary quadratic number field then there are only finitely many γ with $|N(\gamma)| = |\mathcal{D}|$ and our assertion holds again.

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

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

hence $\mathbb{Z}_{\mathbb{K}} = \mathbb{Z}[\gamma]$. By a deep theorem of Győry (1978) there exist only finitely many $\mathbb{Z}$-equivalence classes of $\beta \in \mathbb{Z}_{\mathbb{K}}$ such that $\mathbb{Z}_{\mathbb{K}} = \mathbb{Z}[\beta]$. 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. □

In fact Evertse, et al (2019) proved the above theorem for number systems in general orders.

Thank you for your attention!

I wish everybody refreshing summer holidays!