Annales Univ. Sci. Budapest., Sect. Comp. 16 (1996) 223-251

RESEARCH PROBLEMS IN NUMBER THEORY II.

I. Kátai (Budapest/Pécs, Hungary)

Dedicated to Professor J. Balázs on his 75-th birthday

1. Number systems and fractal geometry

1.1. Let us fix an integer N ($\neq 0, \pm 1$) and a set $\mathcal{A} = \{a_0 = 0, a_1, \dots, a_{t-1}\}$ ($\subseteq \mathbb{Z}$), which is a complete residue system *mod* N. Then $t = |N|$. For every $n \in \mathbb{Z}$ there is a unique $b \in \mathcal{A}$ and a unique $n_1 \in \mathbb{Z}$, such that $n = b + Nn_1$.

Let $\mathcal{I} : \mathbb{Z} \to \mathbb{Z}$ defined by $\mathcal{J}(n) = n_1$. Let

$$L = \frac{\max_{a \in \mathcal{A}} |a|}{|N| - 1}.$$

One can see immediately that

a) $$|\mathcal{J}(n)| < |n| \quad \text{if} \quad |n| > L,$$

and

b) $$\mathcal{J}(n) \in [-L, L] \quad \text{if} \quad n \in [-L, L].$$

Consequently the sequence n, $\mathcal{J}(n)$, $\mathcal{J}^2(n), \dots$ defined by iterating $\mathcal{J}$ is eventually periodic. An integer π is said to be periodic if $\mathcal{J}^k(\pi) = \pi$ holds for some $k > 0$. The set $\mathcal{P}$ of periodic elements is finite, moreover $\mathcal{P} \subseteq [-L, L]$.

We say that $(\mathcal{A}, N)$ is a number system (NS) if every integer n can be written as

$$n = b_0 + b_1 N + \dots + b_k N^k \quad (b_j \in \mathcal{A})$$

The research has been supported by the GO WEST grant and by the Hungarian National Foundation for Scientific Research under grant OTKA T017412.

in a finite form. (The uniqueness of the representation holds automatically.) It is clear that $(\mathcal{A}, N)$ is a number system if and only if $\mathcal{P} = \{0\}$.

Let $G(\mathcal{P})$ be the directed graph over $\mathcal{P}$ (as the set of nodes) getting by drawing the vertices $\pi \to \mathcal{J}(\pi)$. Then $G(\mathcal{P})$ is a disjoint union of circles (and loops).

Let $H \subseteq \mathbb{R}$ be defined as those x which can be expanded as

$$x = \sum_{\nu=1}^{\infty} \frac{b_\nu}{N^\nu}, \qquad b_\nu \in \mathcal{A}.$$

By using the terminology of Hutchinson (see Barnsley [1]) we say that H is the attractor of the iterated function system $\{f_b \mid b \in \mathcal{A}\}$, where $f_b(z) = \dfrac{z+b}{N}$. The relation

$$H = \bigcup_{b \in \mathcal{A}} \left\{ \frac{1}{N} H + \frac{b}{N} \right\}$$

clearly holds.

In a paper written jointly by Indlekofer, Racskó [2,3] we proved, in a more general setting, that

$$\lambda(H + n_1 \cap H + n_2) = 0 \tag{1.1}$$

(λ is the Lebesgue measure) holds for some pairs of distinct integers n_1, n_2, if and only if $n_1 - n_2 \in \mathcal{M}$, where $\mathcal{M}$ denotes the set of those integers m, which can be written as

$$m = \sum_{\nu=0}^{k} c_\nu \cdot N^\nu, \qquad (c_\nu \in \mathcal{B}),$$

where $\mathcal{B} := \mathcal{A} - \mathcal{A}$. Thus $\mathcal{M}$ is the smallest subset X of $\mathbb{Z}$ containing 0 for which

$$X = \bigcup_{b \in \mathcal{B}} (N \cdot X + b) \tag{1.2}$$

is valid.

One can prove furthermore that

$$\bigcup_{n \in \mathbb{Z}} (H + n) = \mathbb{R}.$$

The base N with the given coefficient set $\mathcal{A}$ is said to be a just touching covering system (JTSC for shorthand) if $\lambda(H + n_1 \cap H + n_2) = 0$ holds for every $n_1 \neq n_2 \in \mathbb{Z}$. According to our cited theorem, $(\mathcal{A}, N)$ is a JTCS if and only if $\mathcal{M} = \mathbb{Z}$.

Similar notions can be introduced in the group $\mathbb{Z}_k$ of integer-vectorials substituting the base N with a subgroup $M\mathbb{Z}_k$ where M $(\mathbb{Z}_k \to \mathbb{Z}_k)$ is an expansive linear mapping and by choosing a complete coset-representative set of $\mathbb{Z}_k/M\mathbb{Z}_k$ (as a coefficient set).

We shall formulate some open problems in the simplest (non-trivial) case, when $k = 1$ and $N = 3$.

1.2. Assume that $N = 3$, $\mathcal{A} = \{0, a_1, a_2\}$, where $a_i \equiv i \pmod 3$, $i = 1, 2$. We would like to give necessary and sufficient conditions for $\mathcal{A}$, which guarantees that $(\mathcal{A}, 3)$ is a JTCS.

If $(a_1, a_2) = e$, $|e| \neq 1$, then $\mathcal{M}$ contains only multiples of e, it is a proper subset of $\mathbb{Z}$, thus $(\mathcal{A}, 3)$ is not a JTCS.

Conjecture 1.1. *If* $(a_1, a_2) = 1$, $a_i \equiv i \pmod 3$, *then* $(\mathcal{A}, 3)$ *is a JTCS.*

This assertion has been proved for all the correspondig values a_1, a_2 in [1,900] by Dr.A.Járai on a SUN S10 workstation in Paderborn.

We can pose the above conjecture in the following equivalent form.

Let $\epsilon_k(n)$ denote the digits of the ternary symmetric expansion of n, i.e.

$$n = \sum_{k=0}^{K} \epsilon_k(n) \cdot 3^k, \qquad \epsilon_k(n) \in \{-1, 0, 1\}.$$

Conjecture 1.1′. *Assume that* $(a_1, a_2) = 1$, $a_i \equiv i \pmod 3$ $(i = 1, 2)$. *Then for every* $n \in \mathbb{Z}$ *there exist suitable* $x, y \in \mathbb{Z}$ *such that* $n = a_1 x - a_2 y$ *and*

$$\begin{bmatrix} \epsilon_\nu(x) \\ \epsilon_\nu(y) \end{bmatrix} \neq \begin{bmatrix} +1 \\ -1 \end{bmatrix}, \quad \begin{bmatrix} -1 \\ +1 \end{bmatrix}$$

holds for every ν.

For each fixed set $\mathcal{A}$ one can decide easily that $\mathcal{M} = \mathbb{Z}$ or not. Since each integer n can be expanded in the symmetric ternary system, and $\{0, b, -b\} \subseteq \mathcal{B}$ if $b \in \mathcal{B}$, thus $b\mathbb{Z} \subseteq \mathcal{M}$ for each $b \in \mathcal{B}$. Furthermore $\mathcal{M} = -\mathcal{M}$, since $\mathcal{B} = -\mathcal{B}$.

Assume that $\mathcal{M}$ is a proper subset of $\mathbb{Z}$ and n_0 is the smallest positive integer which does not belong to $\mathcal{M}$. Observe that

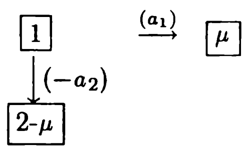
$$n_0 \leq \frac{1}{2} \min(|a_1|,\ |a_2|,\ |d|). \tag{1.3}$$

Indeed, $3 \not| n_0$, consequently for every $0 \neq b \in \mathcal{B}$ one of n_0+b, n_0-b is a multiple of 3, consequently $\frac{n_0 \pm b}{3} \notin \mathcal{M}$ (for at least one sign), whence $\left|\frac{n_0 \pm b}{3}\right| \geq n_0$, which proves (1.3).

Theorem 1.1. *Let* $(a_1, a_2) = 1$, $a_1 \equiv i \pmod 3$, $d = a_2 - a_1 = 4$ *or* 7 *or* 10. *Then* $(\mathcal{A}, 3)$ *is a JTCS.*

Proof. We have to check only that the integers $n \in \left[1, \frac{d}{2}\right]$ belong to $\mathcal{M}$. Let $G(\mathbb{Z})$ be the graph getting by directing an arrow from n to n_1 if $n = b+3\cdot n_1$ with some $b \in \mathcal{B}$. We shall label this arrow by b. If $n \notin \mathcal{M}$, then $n_1 \notin \mathcal{M}$.

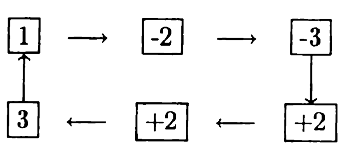
Case d=4. a_1 is odd. Thus $\mu := \frac{1-a_1}{3}$ is even, consequently either μ or $2-\mu$ is a multiple of 4, furthermore



thus $1 \in \mathcal{M}$, and so $-1 \in \mathcal{M}$.

Let $\mathcal{A}_0 = \{0, 4, -4\}$ ($\subseteq \mathcal{B}$). The function $\mathcal{J}$ with respect to $(\mathcal{A}_0, 3)$ maps odd numbers into odd numbers, thus for every odd n, $\mathcal{J}_k(n) \in \{-1, 1\}$ if k is large enough. Thus every odd integer belongs to $\mathcal{M}$. Furthermore, $2 = a_2 + 3 \cdot \frac{2-a_2}{3}$, $\frac{2-a_2}{3}$ is odd, thus $2 \in \mathcal{M}$, consequently $-2 \in \mathcal{M}$. Due to (1.3), we are ready.

Case d=7. Now $\mathcal{B} = \{0, \pm 7, \pm a_1, \pm a_2\}$. Let $\mathcal{A}_0 = \{-7, 0, 7\}$. For the expansion $(\mathcal{A}_0, 3)$ the nonzero periodic elements form a circle



Due to (1.3) it is enough to prove that at least one of the elements -2, -1, 1, 2 belong to $\mathcal{M}$.

The numbers in $7\mathbb{Z}$ have finite expansions in $(\mathcal{A}_0, 3)$. Thus $7\mathbb{Z} \subseteq \mathcal{M}$, consequently $b + 21\mathbb{Z} \subseteq \mathcal{M}$ if $b \in \mathcal{B}$.

Let $a_1 = l + 21A$, $l \in \{1, 4, 10, 13, 16, 19\}$. $l = 7$ implies $7|a_1$, so it is excluded.

Let $\mu := \frac{1 - a_1}{3}$. Then $\frac{1 + a_2}{3} = 3 - \mu$. Thus

To prove that $\mathcal{M} = \mathbb{Z}$, it is enough to show that one of μ, $\mu - 1$, $\mu - 2$, $\mu - 3$ is either a multiple of 7 or belongs to the set $\bigcup_{b \in \mathcal{B}} (b + 21\mathbb{Z})$.

We can find a multiple of 7 if $l = 1, 13, 16, 19$. For the remaining cases $l = 4, 10$, let $A_0 = \epsilon + 3A_1$, $\epsilon_0 \in \{-1, 0, 1\}$.

Let $l = 4$. Then the arithmetic progressions $n = 4, 10, 11, 17 \pmod{21}$ belong to $\mathcal{M}$. Furthermore $\mu - \delta \equiv -1 - \delta - 7\epsilon_0 \pmod{21}$.

If $\epsilon_0 = 0$, the $\mu - 3 \equiv 17 \pmod{21}$, if $\epsilon_0 = 1$, then $\mu - 2 \equiv 11 \pmod{21}$, if $\epsilon_0 = -1$, then $\mu - 2 \equiv 4 \pmod{21}$.

Finally, let $l = 10$. Then $n \equiv 4, 10, 11, 17 \pmod{21}$ belong to $\mathcal{M}$. Furthermore, $\mu \equiv 11 \pmod{21}$ if $\epsilon_0 = 1$; $\mu - 1 \equiv 17 \pmod{21}$, if $\epsilon_0 = = 0$; $\mu \equiv 4 \pmod{21}$, if $\epsilon_0 = -1$.

Case d=10. Let $\mathcal{A}_0 = \{0, 10, -10\}$. Then the graph $\mathcal{G}(\mathcal{P})$ to the expansion $(\mathcal{A}_0, 3)$ consists of three circles G_1, G_2, G_3 and the loop $0 \to 0$, where

$$G_1 = \{1 \to -3 \to -1 \to 3\ (\to 1)\},$$
$$G_2 = \{2 \to 4 \to (-2) \to (-4)\ (\to 2)\},$$
$$G_3 = \{5 \to -5 \to (5)\}.$$

Observe that under the mapping $\mathcal{J}$ the orbit $n, \mathcal{J}(n), \ldots$ goes to C_1 if $(\mu, 10) = = 1$; to C_2 if $(n, 5) = 1$ and $2|\mu$; to C_3 if $(\mu, 2) = 1$ and $5|n$; and to 0 if $10|n$.

Let us consider now the whole graph consisting of $\mathbb{Z}$ as nodes, and the edges of which are determined by $n \overset{(b)}{\rightarrow} n_1$ for $n = b + 3n_1$ for all possible values $b \in \mathcal{B}$. We shall prove that the components C_1, C_2, C_3 are strongly connected. Since

$$\boxed{5} \overset{(-a_1)}{\longrightarrow} \boxed{\frac{5+a_1}{3}}$$

is even, and it is not a multiple of 5, thus $C_3 \rightarrow \ldots \rightarrow C_2$. Furthermore, since

$$\begin{array}{ccc} \boxed{2} & \overset{(-a_1)}{\longrightarrow} & \boxed{\frac{2+a_1}{3}} \\ \downarrow (a_2) & & \\ \boxed{\frac{2-a_2}{3}} & & \end{array}$$

and one of the odd numbers $\frac{2+a_1}{3}$, $\frac{2-a_2}{3}$ is not a multiple of 5, thus

$$\boxed{C_2} \longrightarrow \cdots \longrightarrow \boxed{C_1}$$

Since $5 \not| a_1$, therefore one of $2 + a_1$, $2 - a_2$, $4 - a_1$, $4 + a_2$ is a multiple of 5 and odd, furthermore

$$\begin{array}{ccc} \boxed{2} & \longrightarrow & \boxed{\frac{2+a_1}{3}} \\ \downarrow & & \\ \boxed{\frac{2-a_2}{3}} & & \end{array} \qquad \begin{array}{ccc} \boxed{4} & \longrightarrow & \boxed{\frac{4-a_1}{3}} \\ \downarrow & & \\ \boxed{\frac{4+a_2}{3}} & & \end{array}$$

therefore we can reach C_3 from C_2:

$$\boxed{C_2} \longrightarrow \cdots \longrightarrow \boxed{C_3}$$

Let $\mu = \dfrac{1-a_1}{3}$, we have

$$\begin{array}{ccc} \boxed{1} & \xrightarrow{(a_1)} & \boxed{\mu} \\ \downarrow{\scriptstyle(-a_2)} & & \\ \boxed{4\text{-}\mu} & & \end{array}$$

Since μ is even, one of $\mu, 4-\mu$ is coprime to 5, thus

$$\boxed{C_1} \longrightarrow \cdots \longrightarrow \boxed{C_2}$$

Consequently, it is enough to prove that at least one of the elements of $C_1 \cup C_2 \cup C_3$ can be transformed to 0.

Let $a_1 = l + 30A$, $1 \leq l \leq 30$, $l \equiv \pmod 3$, $(l, 10) = 1$. Then $n \in \mathcal{M}$, if $n \equiv \pm l$, $\pm(l+10) \pmod{30}$. Since $10|\mu$ for $l = 1$, $10|4-\mu$ for $l = 19$, we have to consider only the cases $l = 7, 13$.

The case $l = 13$. Then $n \in \mathcal{M}$ if $n = \pm 7$, $\pm 13 \pmod{30}$. Assume that $A = \epsilon_0 + 3A_1$, $\epsilon_0 \in \{-1, 0, 1\}$. Then $a_1 = 13 + 30\epsilon_0 + 3 \cdot 30A_1$. We have

$$\mu + 1 = -3 - 10\epsilon_0 - 30A_1 \text{ and } \mu + 1 \in \mathcal{M} \text{ if } \epsilon_0 = 1 \text{ or } \epsilon_0 = -1,$$
$$\mu - 3 = -7 - 10\epsilon_0 - 30A_1 \text{ and } \mu - 3 \in \mathcal{M} \text{ if } \epsilon_0 = 0.$$

Since $\mu + 1$ or $\mu - 3 \in \mathcal{M}$, therefore $4 \in \mathcal{M}$ and we are ready.

The case $l = 7$. We have $n \in \mathcal{M}$, if $n \equiv \pm 7$, $\pm 13 \pmod{30}$. Let $a_1 = 7 + 30\epsilon_0 - 30A_1$. Then $\mu = -2 - 10\epsilon_0 - 30A_1$.

If $\epsilon_0 = -1$, then $\mu - 1 \equiv 7 \pmod{30}$, $\mu - 1 \in \mathcal{M}$.

If $\epsilon_0 = 1$, then $\mu - 5 = -7 - 10 - 30A_1$, $\mu - 5 \in \mathcal{M}$.

If $\epsilon_0 = 0$, then $\mu - 5 \equiv -7 \pmod{30}$, $\mu - 5 \in \mathcal{M}$.

Since $4 = -a_2 + 3 \cdot (5 - \mu)$, therefore $4 \in \mathcal{M}$, we are ready.

The proof is completed.

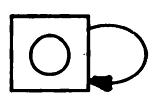
1.3. To explain the background of our conjecture let us consider the structure of $G(\mathcal{P})$ for $\mathcal{A}_{\mathcal{D}} = \{0, \mathcal{D}, -\mathcal{D}\}$ with $N = 3$. Let $\mathrm{ord}(\mathcal{D})$ denote the smallest positive t for which $3^t \equiv 1 \pmod{\mathcal{D}}$ holds. From the Euler-Fermat theorem $\mathrm{ord}(\mathcal{D}) | \varphi(\mathcal{D})$. Let $\mathcal{F}_{\mathcal{D}}$ denote the set of integers $k \in \left(-\frac{\mathcal{D}}{2}, \frac{\mathcal{D}}{2}\right]$ coprime to $\mathcal{D}$. If $k_0 \in \mathcal{F}_{\mathcal{D}}$, $k_0 = \epsilon_0 \mathcal{D} + 3k_1$, $\epsilon_0 = 1$ or -1, then $k_1 \in \mathcal{F}_{\mathcal{D}}$. Its value can be computed from the cogruence relation $k \equiv 3k_1 \pmod{\mathcal{D}}$. Repeating this, we get $k_j \equiv 3k_{j-1} \pmod{\mathcal{D}}$ $(j = 1, 2, \ldots, \mathrm{ord}(\mathcal{D}))$, $k_{\mathrm{ord}(\mathcal{D})-1} = k_0$. On $G(\mathcal{P})$ they are located on a circle, $k_0 \to k_1 \to \ldots \to k_{\mathrm{ord}(\mathcal{D})-1}$ $(\to k_0)$.

Thus the elements of $\mathcal{F}_{\mathcal{D}}$ are subdivided on $G(\mathcal{P})$ into $\frac{\varphi(\mathcal{D})}{\mathrm{ord}(\mathcal{D})}$ disjoint circles, each of which has $\mathrm{ord}(\mathcal{D})$ elements.

Let $\mathcal{D} = \mathcal{D}_1 \cdot \mathcal{D}_2$. If $= \epsilon_0 \mathcal{D} + 3n_1$, then $\mathcal{D}_1 | n$ implies that $\mathcal{D}_1 | n_1$ and vice versa, furthermore $\left(\frac{n}{\mathcal{D}_1}, \mathcal{D}_2\right) = \left(\frac{n_1}{\mathcal{D}_1}, \mathcal{D}_2\right)$.

Hence we obtain that, if $\mathcal{D}_1$ is a unitary divisor of n then it is a unitary divisor of $\mathcal{J}^k(n)$ for every k.

Let $\mathcal{D}_1 l \in \left[-\frac{\mathcal{D}}{2}, \frac{\mathcal{D}}{2}\right]$, $(l, \mathcal{D}_2) = 1$. Let $\mathcal{J}(\mathcal{D}_1 l) = \mathcal{D}_1 l_1$, $\mathcal{D}_1 l = \epsilon \mathcal{D} + 3\mathcal{D}_1 l_1$, whence $l = \epsilon \mathcal{D}_2 + 3l_1$. Thus $l \equiv 3l_1 \pmod{\mathcal{D}}$. Repeating the argument used above we get that $\varphi(\mathcal{D}_2)$ elements $\mathcal{D}_1 l$ are located on $G(\mathcal{P})$ on $\frac{\varphi(\mathcal{D}_2)}{\mathrm{ord}(\mathcal{D}_2)}$ disjoint circles each of which is of length $\mathrm{ord}(\mathcal{D}_2)$. By this we determined completely $G(\mathcal{P})$ for $\mathcal{A}_{\mathcal{D}}$. The structure of $G(\mathcal{P})$ is very simple if $\mathcal{D}$ =prime and 3 is a primitive root mod 3. Then it consists of a loop



and a circle of length $\mathcal{D} - 1$. The following theorem is clear.

Theorem 1.2. *If a_1 (or a_2) is a prime and 3 is a primitive root mod a_1 (or mod a_2), then for $|d| < \frac{|a_1|}{2}$ $\left(|d| < \frac{|a_2|}{2}\right)$ $(\{0, a_1, a_2\}, 3)$ is a JTCS.*

Proof. Since d can be reached from each $0 \neq \nu$, $|\nu| < \frac{|a_1|}{2}$ on the graph $G(\mathcal{P})$ costructed with $\mathcal{A}_{a_1}$, and $d \in \mathcal{M}$, thus $\nu \in \mathcal{M}$, and by (1.3) we are ready.

1.4. Let K be a finite extension field of $\mathbb{Q}$, I be the ring of integers in K. Let $\alpha \in I$ and $\mathcal{A} = \{a_0 = 0, a_1, \ldots, a_{t-1}\}$ $(\subseteq I)$ be a complete residue system mod α. We say that $(\mathcal{A},\alpha)$ is a NS in I, if each $\beta \in I$ can be written in finite form

$$\beta = b_0 + b_1\alpha + \ldots + b_k\alpha^k \qquad (b_\nu \in \mathcal{A}).$$

(The unicity of the expansion is a consequence of the assumption that each residue class mod α contains a unique element in $\mathcal{A}$ (see our paper [4])). One can easily see that α can be a candidate for a base of a NS only if all the conjugates α_j of α satisfy $|\alpha_j| > 1$, and furthermore, if $1-\alpha$ is not a unit. The sufficiency of these conditions has been proved for K = Gaussian integers by G.Steidl [5] and for each imaginary quadratic extension field by the author in [6].

Theorem 1.3. *Let K be a quadratic imaginary extension field of $\mathbb{Q}$, $\alpha \in I$, $|\alpha| > 1$, $|1-\alpha| > 1$. Then there is a suitable coefficient set $\mathcal{A}$ such that $(\mathcal{A},\alpha)$ is a NS.*

$\mathcal{A}$ was given explicitly in [6].

Conjecture 1.2. *If K is a real quadratic extension field, $\alpha \in K$ is an algebraic integer, furthermore $|\alpha_j| > 1$, $|1-\alpha_j| > 1$ holds for $\alpha = \alpha_1$ and for the conjugate α_2, then $(\mathcal{A},\alpha)$ is a NS with a suitable coefficient set $\mathcal{A}$.*

The conjecture has been tested for several values of α for which $\min(|\alpha|, |1-\alpha|, |\alpha_2|, |1-\alpha_2|)$ is not too close to 1.

I do not know how to extend this conjecture for higher degree extension fields.

2. Characterization of arithmetical functions

For an arbitrary additively written Abelian group G let $\mathcal{A}_G$, resp. $\mathcal{A}_G^*$ denote the classes of additive, resp. completely additive functions. A function $f : \mathbb{N} \to G$ belongs to $\mathcal{A}_G$ if $f(mn) = f(m) + f(n)$ holds for each coprime m, n and it belongs to $\mathcal{A}_G^*$ if the above equation holds for all pairs $m, n \in \mathbb{N}$. If G is written multiplicatively, then we write $\mathcal{M}_G$, $\mathcal{M}_G^*$ instead of $\mathcal{A}_G$, $\mathcal{A}_G^*$ and the corresponding functions are called multiplicative, completely multiplicative ones. If $G = \mathbb{R}$, then we write $\mathcal{A}$, $\mathcal{A}^*$ instead of $\mathcal{A}_G$, $\mathcal{A}_G^*$, and for $G + \mathbb{C}$ we write $\mathcal{M}$, $\mathcal{M}^*$ instead of $\mathcal{M}_G$, $\mathcal{M}_G^*$.

Let S be an R-module, containing at least two elements, defined over an integral domain R which has an identity. In the set of all doubly infinite sequences $(\ldots, s_{-1}, s_0, s_1, \ldots)$ of elements of S we define the shift operator E

whose action takes a typical sequence $\{s_n\}$ to the new sequence $\{s_{n+1}\}$. For an arbitrary polynomial $P(x) = \sum_{j=0}^{r} c_j x^j$, $P(E)\{s_n\}$ is defined as

$$P(E)s_n = \sum_{j=0}^{r} c_j s_{n+j}.$$

In this way we define a ring of operators which is isomorphic to the ring of polynomials over $\mathbb{R}$. Let I be the identity operator, and $\Delta := E - I$.

Let $\mathbb{Q}_x$, resp. $\mathbb{R}_x$ be the multiplicative group of positive rationals and positive reals.

If $f : R_x \to G$ satisfies the Cauchy equation $f(xy) = f(x) + f(y)$, then restricting the domain to N, f is a completely additive function.

If $f \in \mathcal{A}_G^*$ $(\mathbb{N} \to G)$, then its domain can be extended to $\mathbb{Q}_x$ by $f\left(\frac{m}{n}\right) :=$ $:= f(m) - f(n)$. If f is continuous in $\mathbb{Q}_x$ (it is enough to require the continuity at the point 1), then it can be continuously extended to $\mathbb{R}_x$.

Our main question is the following: what further properties along with (complete) additivity will ensure that an arithmetic function f is in fact a restriction of a continuous homomorphism $R_x \to G$?

The first result of this type was found by P.Erdős [7] in 1946: If $f \in \mathcal{A}$ and $\Delta f(n) \geq 0$ for all n, or $f(n) \to 0$ $(n \to \infty)$, then $f(n)$ is a constant multiple of $\log n$.

A survey paper on this topic was written recently [8]. The book of Elliott [9] contains a lot of important results. We are concentrating on unsolved problems.

2.1. Additive functions: $G = \mathbb{R}$

Conjecture 2.1. *If $f_1, \ldots, f_k \in \mathcal{A}$, and*

$$l_n := f_1(n+1) + f_2(n+2) + \ldots + f_k(n+k) \to 0 \tag{2.1}$$

as $n \to \infty$, then there exist suitable contants $c_1, \ldots, c_k$ and additive functions $v_1, \ldots, v_k$ of finite support such that $f_i(n) = c_i \log n + v_i(n)$,

$$\sum_{i=1}^{k} c_i = 0,$$

$$\sum_{i=1}^{K} v_i(n+i) = 0 \qquad (n = 0, 1, 2, \ldots).$$

We say that $f \in \mathcal{A}$ ($\in \mathcal{A}_G$) is of finite support, if it vanishes on the set of prime powers p^α for all but at most finitely many primes p.

Assuming that each $f_i(n)$ has the special form $f_i(n) = \lambda_i f(n)$ ($i = 1, \ldots, k$) with some constants λ_i, the conjecture was proved by Elliott [11], and by myself [10], independently.

An infinite sequence $\{U_n\}_{n\in N}$ of real (or complex) numbers is called a tight sequence if for every $\delta > 0$ there exists a number $c < \infty$, such that

$$\sup_{n\geq 1} x^{-1}\sharp\{n \leq x \mid |U_n| > c\} < \delta.$$

Let $\mathcal{T}$ be the set of tight sequences.

Let $\mathcal{T}'$ denote the set of those sequences $\{U_n\}_{n\in N}$ for which the relation

$$\sup_{x\geq 1} x^{-1}\sharp\{n \leq x \mid |U_n - \alpha(x)| > c\} < \delta$$

holds for every $\delta > 0$ with a suitable constant $c = c(\delta)$ and with a suitable function $\alpha(x)$.

It would be important to characterize those $f_i \in \mathcal{A}$ ($i = 1, \ldots, k$) for which the sequence l_n defined in (2.1) belongs to $\mathcal{T}$ or $\mathcal{T}'$. Perhaps the following assertion is true.

Conjecture 2.2. *If $f_1, \ldots, f_k \in \mathcal{A}$ such $\{l_n\} \in \mathcal{T}$, then there exist constants $\lambda_1, \ldots, \lambda_k$ such that $\sum_{j=1}^{k} \lambda_j = 0$, furthermore for the functions $h_j(n) := f_j(n) - \lambda_j \log n$ the conditions hold*

$$\sum_{j=1}^{k} \sum_{\substack{|h_j(p)|\leq 1\\ p\leq x}} h_j(p) \quad \textit{is bounded in } x, \tag{2.2}$$

$$\sum_{j=1}^{k}\sum_{p} \frac{\min(1, h_j^2(p))}{p} < \infty. \tag{2.3}$$

Remarks.

1. If (2.2), (2.3) are satisfied, then $\{l_n\} \in \mathcal{T}$. This can be proved in a routine way.

2. A.Hildebrand made an important step [12] by showing that $\{l_n := \Delta f(n)\} \in \mathcal{T}$ implies that f has the decomposition $f = \lambda \log + h$, where h is finitely distributed.
3. Some further results have been proved in [13].

2.2. *Characterization of n^s as a multiplicative function $\mathbb{N} \to \mathbb{C}$*

In a series of papers [14-19] I considered functions $f \in \mathcal{M}$ under the conditions that $\Delta f(n)$ tends to zero in some sense. There were determined all the functions $f, g \in \mathcal{M}$ for which the relation

$$\sum_{n=1}^{\infty} \frac{1}{n} |g(n+k) - f(n)| < \infty \tag{2.4}$$

with some fixed $k \in \mathbb{N}$ holds. In the special case $k = 1$, $f, g \in \mathcal{M}^*$ implies that either

$$\sum_{n=1}^{\infty} \frac{|f(n)|}{n} < \infty, \qquad \sum_{n=1}^{\infty} \frac{|g(n)|}{n} < \infty,$$

or $f(n) = g(n) = n^{\sigma + i\tau}$, $\quad \sigma, \tau \in \mathbb{R}, \ 0 \le \sigma < 1$.

Hence it follows especially that

$$\sum_{n=1}^{\infty} \frac{|\lambda(n+1) - \lambda(n)|}{n} = \infty,$$

where λ is the Liouville function, which shows that the size of integers n for which $\lambda(n+1) \ne \lambda(n)$ is not too small.

A more explicit estimation from below for

$$\sharp\{n \le x \mid f(n+1) \ne f(n)\},$$

where $f \in \mathcal{M}$, $f(n) \in \{-1, 1\}$ was given by A.Hildebrand [20].

In our joint papers written together with K.-H.Indlekofer [21-24] we deduced: if $f, g \in \mathcal{M}^*$ and

$$\sum_{n \le x} |g(n+1) - f(n)| = O(x),$$

then either $\sum_{n \le x} |f(n)| = O(x)$, $\sum_{n \le x} |g(n)| = O(x)$, or

$$f(n) = g(n) = n^s, \qquad 0 \le \operatorname{Re} s \le 1.$$

Conjecture 2.3. *Let $f, g \in \mathcal{M}$, $k \in N$ such that* $\liminf \frac{1}{x} \sum_{n \le x} |f(n)| > 0$, *and*

$$\frac{1}{x} \sum_{n \le x} |g(n+k) - f(n)| \to 0.$$

Then there exists $U, V \in \mathcal{M}$ and $s \in C$ with $0 \le \operatorname{Re} s < 1$ such that $f(n) = U(n)n^s$, $g(n) = V(n)n^s$, and

$$V(n+k) = U(n) \qquad (n = 1, 2, \ldots) \tag{2.5}$$

holds.

Even a complete characterization of the couples $U, V \in \mathcal{M}$ satisfying (2.5) seems to be hard. One can assume always that $U(p^\alpha) = V(p^\alpha) = 0$ for $p|k$. If $U, V \in \mathcal{M}^*$ is assumed, then all the solutions are Dirichlet characters (see [14-19]).

Assume only the multiplicativity, and let us restrict ourselves to the case $U(n) \in \{0, 1\}$ $(n = 1, 2, \ldots)$. As the example $k = 3$, $U(2) = V(5) = 1$, $U(4) = V(7) = 1$, $U(32) = V(35) = 1$ and $U(p^\beta) = 0$ for all the prime powers $p^\beta \notin \{2, 2^2, 2^5\}$ shows, there could be other solutions which are expected: $U(n) = 1$ for every n coprime to k.

Conjecture 2.4. *Let $U, V \in \mathcal{M}$, $U(\mathbb{N}), V(\mathbb{N}) \subseteq \{0, 1\}$ such that $U(n) = V(n+k)$ $(n = 1, 2, \ldots)$, and $U(1) = 1$ and $U(p^\alpha) = V(p^\alpha) = 0$ for all primes $p|k$. Let $N_0 = \{n \mid U(n) = 0\}$, $N_1 = \{n \mid U(n) = 1\}$. If N_0 contains an n, $(n, k) = 1$, then N_1 is a finite set.*

This conjecture has been proved, and all the solutions of $V(n+k) = U(n)$ were given for all the odd values k in the interval $1 \le k \le 201$ by R.Styer. He observed furthermore that N_1 was a set consisting only some of powers of a unique prime. Perhaps it is always true.

I think furthermore that the existence of a prime power p^β with the property $p|k+1$, $U(p^\beta) = 1$ implies that $U(n) = 1$ for $(n, k) = 1$. Perhaps the more general assertion is true: if there exists a prime q, and positive exponents α, β such that $U(q^\alpha) = V(q^\beta) = 1$, then $U(n) = 1$ holds for all n coprime to k.

In 1984 E.Wirsing proved that $f \in \mathcal{M}$, $\Delta f(n) \to 0$ implies that either $f(n) \to 0$ or $f(n) = n^s$, $0 \le \operatorname{Re} s < 1$ [25]. As an immediate consequence we get that if $F(n) \in \mathcal{A}$, then $\|\Delta F(n)\| \to 0$ implies that either $\|F(n)\| \to 0$ or $F(n) - \tau \log n \equiv 0 \pmod 1$ for every n, with a suitable $\tau \in \mathbb{R}$.

Assume we would like to find all couples $f, g \in \mathcal{M}$ for which $g(n+k) - f(n) \to 0$ $(n \to \infty)$, where k is a fixed integer. Trying to reduce this problem to Wirsing's case $(k = 1,\ f = g)$, the first problem is to determine the set of those integers n for which $f(n) = 0$ (or $g(n) = 0$). Excluding the case $f(n) \to 0$

(which implies $g(n) \to 0$) one can deduce that (f, g) is a solution if $g(n) = n^s$, $f(n) = n^s U(n)$, (2.5) holds and $0 \le \text{Re } s < 1$. The proof of this assertion is not quite easy, it can be done by the method which was used in a joint paper of N.L. Bassily and the author [26]. Namely in [26] the following theorem was proved:

Let $f, g \in \mathcal{M}$, $c \neq 0$ such that $g(2n+1) - cf(n) \to 0$ $(n \to \infty)$. Assume that $f(n) \not\to 0$ $(n \to \infty)$. Then $f(n) = n^s$ $0 < \text{Re } s <$ and $g(n) = f(n)$ for odd n.

2.3. Additive functions mod 1

T is considered here as the additive group $\mathbb{R}/\mathbb{Z}$.

We say that $F \in \mathcal{A}_T$ is of finite support if $F(p^\alpha) = 0$ for every large prime p.

For $F_\nu \in \mathcal{A}_T$ $((= 0, 1, \dots, k-1)$ let

$$L_n(F_0, \dots, F_{k-1}) := F_0(n) + \dots + F_{k-1}(n + k - 1). \tag{2.6}$$

Conjecture 2.5. *Let $\mathcal{L}_0$ be the space of those k-tuples $(F_0, \dots, F_{k-1})$, $F_\nu \in \mathcal{A}_T$ $(\nu = 0, 1, \dots, k-1)$ for which*

$$L_n(F_0, \dots, F_{k-1}) = 0 \qquad (n \in \mathbb{N}) \tag{2.7}$$

holds. Then each F is of finite support, and $\mathcal{L}_0$ is a finite dimensional $\mathbb{Z}$ module.

The domain of the functions $F(n) := \tau \log n$ (mod 1) can be extended to $\mathbb{R}_x$ continuously, where $\mathbb{R}_x$ is the multiplicative group of positive reals. Thus $F(n)$ are called restrictions of continuous homomorphisms from $\mathbb{R}_x$ to T.

It is clear that for each choice of $\tau_0, \dots, \tau_{k-1}$ such that $\tau_0 + \dots + \tau_{k-1} = 0$ we have

$$L_n(\tau_0 \log ., \ \tau_1 \log ., \dots, \tau_{k-1} \log .) \to 0 \qquad (n \to \infty).$$

Conjecture 2.6. *If $F_\nu \in \mathcal{A}_T$ $(\nu = 0, \dots, k-1)$,*

$$L_n(F_0, \dots, F_{k-1}) \to 0 \qquad (n \to \infty),$$

then there exist suitable real numbers $\tau_0, \dots, \tau_{k-1}$ such that $\tau_0 + \dots + \tau_{k-1} = 0$, and if $H_j(n) := F_j(n) - \tau_j \log n$, then

$$L_n(H_0, \dots, H_{k-1}) = 0 \qquad (n = 1, 2, \dots).$$

Remarks.

(1) Conjecture 2.6 for $k = 1$ can be deduced easily from Wirsing's theorem.
(2) Conjecture 2.5 was proved under the more strict assumption that F_ν are completely additive for $k = 3$ [27].
(3) Conjecture 2.5 for $k = 2$ has been proved by R.Styer [28].
(4) Marijke van Rossum-Wijsmuller treated similar problems for functions defined on the set of Gaussian integers. See [29], [30].

Let K be the closure of the set $\{L_n(F_0, \dots, F_{k-1}) \mid n \in \mathbb{N}\}$.

Conjecture 2.7. *If $F_0, \dots, F_{k-1} \in \mathcal{A}_T^*$ and K contains an element of infinite order, then $K=T$.*

Remarks.

(1) This assertion is clearly true for $k = 1$.
(2) The conjecture fails for the wider class $F_0 \in \mathcal{A}_T$ even in the case $k = 1$.

2.4. Characterizations of continuous homomorphisms as elements of $\mathcal{A}_G$ for compact groups G

We investigated this topic in a series of papers written jointly by Z.Daróczy [31-36].

Assume in this section that G is a metrically compact Abelian group supplied with some translation invariant metric ρ. An infinite sequence $\{x_n\}_{n=1}^\infty$ in G is said to belong to $\mathcal{E}_\mathcal{D}$, if for every convergent subsequence $x_{n_1}, x_{n_2}, \dots$ the "shifted subsequence" $x_{n_1+1}, x_{n_1+2}, \dots$ is convergent, too. Let $\mathcal{E}_\Delta$ be the set of those sequences $\{x_n\}_{n=1}^\infty$ for which $\Delta x_n \to 0$ $(n \to \infty)$ holds. Then $\mathcal{E}_\Delta \subseteq \mathcal{E}_\mathcal{D}$. We say that $f \in \mathcal{A}_G^*$ belongs to $\mathcal{A}_G^*(\Delta)$ (resp. $\mathcal{A}_G^*(\mathcal{D})$) if the sequence $\{f(n)\}_{n=1}^\infty$ belongs to $\mathcal{E}_\Delta$ (resp. $\mathcal{E}_\mathcal{D}$).

We proved the following results:

(1) $\mathcal{A}_G^*(\Delta) = \mathcal{A}_G^*(\mathcal{D})$.
(2) If $f \in \mathcal{A}_G^*(\mathcal{D})$, then there exists a continuous homomorphism $\Phi : \mathbb{R}_x \to G$ such that $f(n) = \Phi(n)$ for every $n \in \mathbb{N}$.

The proof of (2) was based upon the theorem of Wirsing in [25].

The set of all limit points of $\{f(n)\}_{n=1}^\infty$ form a compact subgroup in G which is denoted by S_f.

(3) $f \in \mathcal{A}_G^*(\mathcal{D})$ if and only if there exists a continuous function $H : S_f \to S_f$ such that $f(n+1) - H(f(n)) \to 0$ as $n \to \infty$.

The main problem we are interested in is the following one:

Let $f_j \in \mathcal{A}_{G_j}$ $(j = 0, 1, \dots, k-1)$, and consider the sequence $e_n :=$ $:= \{f_0(n), f_1(n+1), \dots, f_{k-1}(n+k-1)\}$.

Then $e_n \in S_{f_0} \times \ldots \times S_{f_{k-1}}$. What can we say about the functions f_j, if the set of the limit points of e_n is not everywhere dense in U? We shall formulate our guesses only for special cases.

Conjecture 2.8. *Let $f \in \mathcal{A}_T^*$, $S_f = T$, $e_n := (f(n), \ldots, f(n+k-1))$. Then either $\{e_n \mid n \in N\}$ is everywhere dense in $T_k = T \times \ldots \times T$, or $f(n) = = \lambda \log n \pmod{\mathbb{Z}}$ with some $\lambda \in \mathbb{R}$.*

Conjecture 2.9. *Let $f, g \in \mathcal{A}_T^*$, $S_f = S_g = T$, $e_n := (f(n), g(n+1))$. If e_n is not everywhere dense in T^2, then f and g are rationally dependent continuous characters, i.e. there exists $\lambda \in \mathbb{R}$, $s \in \mathbb{Q}$ such that $g(n) = sf(n) \pmod{\mathbb{Z}}$, $f(n) = \lambda \log n \pmod{\mathbb{Z}}$.*

3. On prime divisors

3.1. Let $P(n)$ be the largest and $p(n)$ be the smallest prime divisor of n.

Conjecture 3.1. *For every integer k (≥ 1) there always exists a constant c_k such that for every prime p greater than c_k*

$$\min_{\substack{1 \leq j \\ P(j) < p}} \max_{\substack{l = -k, \ldots, k \\ l \neq 0}} P(jp + l) < p$$

holds.

Some heuristical arguments support my opinion that this assertion is true. Hence it would follow that the dimension of the space $\mathcal{L}_0$ defined in Conjecture 2.5 is finite.

The problem is unsolved even for $k = 2$.

3.2. We say that p^α is a unitary prime-power factor of n if $p^\alpha \mid n$, and $\left(\frac{n}{p^\alpha}, p^\alpha\right) = 1$. We use the notation $p^\alpha \| n$. Let furthermore $(a, b) =$ the greatest common divisor of a and b.

Conjecture 3.2. *Let a be an odd positive integer and $\mathcal{M}(\subseteq \mathbb{N})$ be defined by the following properties:*

(1) $\{1, 2, 2^2, 2^3, \ldots\} \subseteq \mathcal{M}$.

(2) If $P_0 \in \mathcal{M}$, *then* $P_1 := 4P_0 + a \in \mathcal{M}$.

(3) If $Q_1, Q_2 \in \mathcal{M}$ *and* $(Q_1, Q_2) = 1$, *then* $Q_1 Q_2 \in \mathcal{M}$.

(4) If $Q \in \mathcal{M}$ *and* $p^\alpha \| Q$, *then* $p^\alpha \in \mathcal{M}$.

(5) If $(n, a) > 1$, *then* $n \notin \mathcal{M}$.

Then $\mathcal{M} = \{n \mid (n,a) = 1\}$.

Remarks.

(1) The conjecture is true for small positive integers a.

(2) Let $a = p_1^{\alpha_1} \dots p_r^{\alpha_r}$. One can give a function L_a explicitly, L_a depends only on the primes $p_1, \dots, p_r$, such that if $\{n \le L_a \wedge (n,a) = 1\} \subseteq \mathcal{M}$, the $\mathcal{M} = \{n,\ (n,a) = 1\}$.

(3) J. Fehér proved the conjecture for a =prime.

3.3. Let ϑ be a completely multiplicative function, taking values on $\mathbb{N}$. Let ϑ_k denote the k-fold iterates of it. We define a directed graph called G_ϑ on the set of primes by leading an edge from p to q, if $q|\vartheta(p)$. For each p let E_p denote the set of those primes q which can be reached from p walking on G_ϑ. Let furthermore K be the set of that primes which are located on some circles.

The properties of K and E_p were investigated in [37], [38], [39] for the case $\vartheta(p) = p + a$, where a is a constant. It was proved that K is a finite set, and that for every prime p there is a k such that all the prime factors of $\vartheta_k(p)$ belong to K.

Conjecture 3.3. *Let* $\vartheta \in \mathcal{M}^*$ *be defined at prime places* p *by* $\vartheta(p) = ap+b$, *where* $a \ge 2$, $2a + b \ge 1$, a, b *integers*, $(a,b) = 1$. *Then*

(1) E_p *is a finite set for every prime* p.

(2) K *is an infinite set.*

Conjecture 3.4. *If* ϑ *is defined by* $\vartheta(p) = p^2 + 1$, *then there is a prime* q *for which* E_q *is an infinite set.*

Perhaps E_2 is infinite, and then E_q is infinite for every prime q.

3.4. We are interested in to estimate the longest interval on which a suitable multiplicative function taking values ± 1 does not change its sign.

For an integer x let L_x be the largest integer for which there exists $f \in \mathcal{M}^*$, $f(n) \in \{+1, -1\}$, $f(2) = -1$ such that $f(x + j) = 1$ $(j = 1, \dots, L_x)$. It is clear that $L_x < \min_{2m^2 > x} \{2m^2 - x\}$; since $f(2m^2) = -1$ always holds, therefore $L_x < 2\left(\left[\sqrt{\frac{x}{2}}\right] + 1\right) - x \le 2\sqrt{2}\sqrt{x} + 1$. Furthermore, $L_{2m^2} = 0$, $L_{2m^2-1} = 1$. On the other hand, if for all the integers $x+j$ $(j = 0, \dots, k)$ one can find prime divisors $p_j | x+j$ such that $p_j > k$ and $p_j^2 \nmid x+j$, the $L_x \ge k$. In a paper written jointly with Erdős [40] we proved that for a suitable sequence of $x = x_\nu$ can be found such a $k = k_\nu$ for which

$$k_\nu > \exp\left(\left(\frac{1}{2} - \epsilon\right) \frac{(\log x_\nu) \log\log\log x_\nu}{\log\log x_\nu}\right),$$

more exactly, from our Theorem 3, in [40], it comes out immediately from the following

Conjecture 3.5. $L_x/\sqrt{x} \to 0$ *as* $x \to \infty$.

Probably $\log L_x/\log x \to 0$ is true as well.

4. Values of multiplicative functions on some special subsequences of integers

4.1. Let $\mathcal{P}_k$ be the set of integers $n \geq 2$ the number of distinct prime factors of which is $\leq k$. Let furthermore $\mathcal{P}_{k,+1} := \mathcal{P}_k + 1$; $\mathcal{P}_1 = \mathcal{P}$. Let furthermore $\tilde{\mathcal{M}}_0$ be the class of those complex valued (completely) multiplicative functions which are nowhere zero.

Several years ago, in [41] I formulated the conjecture that $\lambda(p+1)$ takes on both the values 1 and -1 infinitely often, if p runs over $\mathcal{P}$. Here λ is the Liouville-function. If the equation $p-2q = 1$ has infinitely many solutions in primes, then the same is true for $p+1 = 2(q+1)$. Since $\lambda(p+1) = \lambda(2)\lambda(q+1) = -\lambda(q+1)$, the conjecture hence it would follow.

By using this simple observation and Chen's method in sieve (see [42]) one can prove the following assertion: For every $a \in \mathbb{N}$ there exists an infinite sequence of pairs of integers $P_2^{(\nu)}+1$, $Q_2^{(\nu)}+1 \in \mathcal{P}_{2,+1}$ ($\nu = 1, 2, \ldots$), such that

$$P_2^{(\nu)} + 1 = a(Q_2^{(\nu)} + 1) \tag{4.1}$$

holds true.

This implies the following assertion, evidently.

If $f \in \tilde{\mathcal{M}}_0$, then either $f(a) = 1$ identically, or it takes on at least two distinct values on the set $\mathcal{P}_{2,+1} \cap [t, \infty)$ for every $t > 0$.

Conjecture 4.1. *If* $f \in \tilde{\mathcal{M}}_0$ *and* f *is not identically 1, then* $f(p+1)$ ($p \in \mathcal{P}$) *takes on at least two distinct values.*

4.2. In [41] we mentioned that $\lambda(n^2+1)$ ($n \in \mathbb{N}$) changes its value infinitely often, which is a straightforward consequence of the fact that the Pell-equation $n^2 + 1 = 2(m^2 + 1)$ has infinitely many solutions. This elementary observation can be extended to $n^2 + a$, and for more general quadratic polynomials.

Let $F(n) := n^2 + An + B$, A, B integers, F be irreducible over $\mathbb{Q}$. Since $F(n+x) = F(n) + F'(n)x + \frac{F''(n)}{2}x^2$, $F(n+x) = F(n) + (2n+A)x + x^2$, therefore

$$F(n + tF(n)) = \Phi(n,t)F(n), \tag{4.2}$$

where

$$\Phi(n,t) := 1 + (2n + A)t + t^2(n^2 + An + B).$$

Let us observe that

$$\Phi(n,-1) = F(n-1), \qquad \Phi(n,1) = F(n+1),$$

which, by (4.2), leads to the equations

$$F(n + F(n)) = F(n+1)F(n), \tag{4.3}$$

$$F(n - F(n)) = F(n-1)F(n). \tag{4.4}$$

Let η_F be the smallest positive integer for which $F(x) > 0$ for all $x \geq \eta_F$. Let

$$M^{(s)} = MF^s := \{F(n) \mid n = s, s+1, \ldots\}.$$

Theorem 4.1. *Let $f \in \widetilde{\mathcal{M}}_0$. Then either $f[M^{(\eta_F)}] = 1$ or $f[M^{(s)}]$ contains at least two elements for every $s \geq \eta_F$.*

Proof. Assume that there exists an s for which $f[M^{(s)}]$ contains only one element. We denote it by c. From (4.3) we have

$$f(F(n + F(n))) = f(F(n+1))f(F(n)), \tag{4.5}$$

which implies that $c = 1$. Consequently, if $f[M^{(\eta_F)}]$ is a singleton, then $f[M^{(\eta_F)}] = 1$.

Assume that our theorem is not true. Then there exists a largest integer $n = n_0$ ($\geq \eta_F$) such that $f(F(n)) \neq f(F(n+1))$. Then from (4.5) we have

$$1 = f(F(n_0 + 1)) = f(F(n_0 + 2)) = \ldots,$$

$f(F(n_0)) = d$, $d \neq 1$. Consider now (4.3) for $n = n_0$. Since $F(n_0) > 0$, therefore $n_0 + F(n_0) > n_0$, $f(F(n_0 + F(n_0))) = 1$, $f(F(n_0 + 1)) = 1$, whence $d = 1$ follows. This contradicts to our assumption. The proof is finished.

Let especially $F(n) = P_a(n) = n^2 + a$, $a \in \mathbb{N}$. Then $\eta_F = 1$. We can rewrite $\Phi(n,t)$ in the form

$$\Phi(n,t) = (1+tn)^2 + at^2. \tag{4.6}$$

Corollary 1. *Let $f \in \mathcal{M}_0^*$ such that $f(\Phi(n_0,t_0)) \neq 1$ for a suitable choice of $n_0 \in \mathbb{N}$, $t_0 \in \mathbb{Z}$. Then*

$$f(P_a(n)) \neq f(P_a(n+1))$$

holds for infinitely many $n \in \mathbb{N}$.

Proof. From (4.2) we deduce that $\{f(F(n)) \mid n = 0, \pm 1, \pm 2, \ldots\}$ contains at least two distinct values. Observe that $F(-n) = F(n)$. If there is an $n_0 > 0$ such that $f(F(n_0+1)) \neq f(F(n_0))$, then we can apply Theorem 4.1 directly. Assume that $f(F(0)) = d$, $f(F(n)) = c = 1$ $(n \in \mathbb{N})$, $d \neq 1$. From (4.3) we get that $f(F(0)) = 1$. Consequently $\{f(F(n)) \mid n = 0, \pm 1, \ldots\} = \{1\}$, which is a contradiction. It is clear that

$$\{F(n) \mid \ = 0,1,2,\ldots\} \subseteq \{\Phi(n,1) \mid n \in \mathbb{N}\} \cup \{\Phi(n,-1) \mid n \in \mathbb{N}\}.$$

So we have

Corollary 2. *Let $a \in \mathbb{N}$. If $\lambda(n^2+a) = -1$ has at least one solution $n \in \mathbb{Z}$, then $\lambda(n^2+a)$ $(n \in \mathbb{Z})$ takes on both values $+1$, -1 infinitely often.*

We can prove a similar result for $a < 0$.

Corollary 3. *Let $a < 0$, where $-a$ is not a square number. Assume that $\lambda(n^2+a) = -1$ holds for some $n = n_0$ satisfying $n_0^2 + a > 0$. Then $\lambda(n^2+a)$ takes on both the values $+1$, -1 infinitely often.*

Conjecture 4.2. *Assume that $a \in \mathbb{Z}$ and $-a$ is not a square. If $f \in \widetilde{\mathcal{M}}_0$ satisfies $f(n^2+a) = 1$ $(n \in \mathbb{Z})$, then $f(u^2+av^2) = 1$ holds for every $u, v \in \mathbb{Z}$ for which $u^2 + av^2 > 0$.*

5. q-additive and q-multiplicative functions

Let $q \geq 2$, $q \in \mathbb{N}$, $A = \{0, 1, \ldots q-1\}$, the digits in the q-ary expansion of a nonnegative integer $n \in \mathbb{N} \cup \{0\}$ are denoted by $e_j(n)$,

$$n = \sum_{j=0}^{\infty} e_j(n) q^j, \qquad e_j(n) \in A. \tag{5.1}$$

A function $f : \mathbb{N} \cup \{0\} \to \mathbb{R}$ is said to be q-additive function, if $f(0) = 0$ and

$$f(n) = \sum_{j=0}^{\infty} f(e_j(n)q^j) \tag{5.2}$$

holds for every $n \in \mathbb{N}$. A function $g : \mathbb{N} \cup \{0\} \to \mathbb{C}$ is q-multiplicative, if $g(0) = 1$ and

$$g(n) = \prod_{j=0}^{\infty} g(e_j(n)q^j). \tag{5.3}$$

Let $\mathcal{A}_q$, resp. $\mathcal{M}_q$ be the sets of q-additive and q-multiplicative functions. The sum of digit function $\alpha(n) := \sum_{j=0}^{\infty} e_j(n)$ is a typical q-additive function.

It is clear furthermore, that if $f \in \mathcal{A}q$ and $z \in \mathbb{C}$, then $g(n) := z^{f(n)}$ belongs to $\mathcal{M}_q$. Thus e^{inx} as a function in n belongs to $\mathcal{M}_q$ for every $x \in \mathbb{R}$, and the sequence $w_n(x) = g(n)$, w_n is the n-th Walsh function, belongs to $\mathcal{M}_2$.

Questions for the value distributions of q-additive functions are somewhat easier to solve than in the case of additive functions. Nevertheless this field is rich in nice and important open problems.

5.1. Distribution of q-additive functions

As H.Delange proved [43], $g \in \mathcal{M}_q$ under the condition $|g(n)| \leq 1$ has a nonzero mean value $M(g)$, i.e.

$$\frac{1}{x} \sum_{n \leq x} g(n) \to M(g),$$

if and only if $\sum_{j=0}^{\infty} \sum_{a \in \mathcal{A}} (g(aq^j) - 1)$ is convergent, $\sum_{a \in \mathcal{A}} g(aq^j) \neq q$ $(j = 0, 1, \ldots)$, and then

$$M(g) = \prod_{j=0}^{\infty} \left\{ \sum_{j=0}^{q-1} (g(aq^j) - 1) \right\}.$$

As a consequence he deduced that a function $f \in \mathcal{A}_q$ has a limit distribution, if and only if

$$\sum_{j=0}^{\infty} \left(\sum_{a \in \mathcal{A}} f(aq^j) \right) \quad \text{is convergent,} \tag{5.4}$$

and

$$\sum_{j=0}^{\infty} \sum_{a \in \mathcal{A}} f^2(aq^j) < \infty. \tag{5.5}$$

In [44] the following assertion is proved.

Theorem 5.1. *Let $f \in \mathcal{A}_q$. Assume that there is a suitable function $\alpha(x)$ such that*

$$\lim_{x \to \infty} \frac{1}{\pi(x)} \sharp\{p \le x,\ f(p) - \alpha(x) < y\} = F(y), \tag{5.6}$$

where F is a distribution function. Then (5.5) is convergent.

Let $N = N_x = \left[\frac{\log x}{\log q}\right]$,

$$\mu(x) := \sum_{j=0}^{N} \sum_{a \in \mathcal{A}} f(aq^j). \tag{5.7}$$

Then $\alpha(x) - \mu(x)$ tends to a finite limit as $x \to \infty$. Especially, if $\alpha(x) = 0$ identically, then (5.4) is convergent.

On the other hand, the convergence of (5.4), (5.5) are sufficient for the existence of the limit distribution F with $\alpha(x) \equiv 0$; the fulfilment of (5.5) implies the existence of $\alpha(x)$ ($\alpha(x) = \mu(x)$ is suitable) by which (5.6) holds true.

The proof goes back to nontrivial estimates of exponential sums with prime variables.

5.2. Mean values of q-multiplicative functions over the set $\mathcal{P}$ of primes

Conjecture 5.1. *If $g \in \mathcal{M}_q$, $|g(n)| \le 1$ and*

$$\lim_{x \to \infty} \frac{1}{\pi(x)} \sum_{p \le x} g(p)\ (=: M_g)$$

exists, then

$$\sum_j \sum_{a \in A} (g(aq^j) - 1)$$

is convergent.

Remark. The opposite assertion, the sufficiency is proved in [44]. Assume from now on that $g \in \mathcal{M}_q$, $|g(n)| = 1$ for $n \in \mathbb{N} \cup \{0\}$. Let

$$S(x|\alpha) := \sum_{\substack{l<x \\ (l,q)=1}} g(l)e(\alpha l), \quad e(\beta) := \exp(2\pi i\beta), \tag{5.8}$$

$$P(x) := \sum_{p \le x} g(p). \tag{5.9}$$

We are interested in to give necessary and sufficient conditions for g to satisfy

$$\frac{P(x)}{\pi(x)} \to 0 \qquad (x \to \infty). \tag{5.10}$$

Conjecture 5.2. *(5.10) holds if and only if*

$$x^{-1}S(x|r) \to 0 \qquad (x \to \infty) \tag{5.11}$$

for every $r \in \mathbb{Q}$.

Remark. In [44] we proved that (5.10) implies the fulfilment of (5.11).

Let

$$T_{l_1,l_2}^{(M)} = T_{l_1,l_2} = \tag{5.12}$$

$$= \sharp\{p_1, p_2 \in \mathcal{P},\ p_2 - p_1 = l_2 - l_1,\ \ p_1 \equiv l_1 \pmod{q^M},\ \ p_1 \le x\}.$$

Conjecture 5.3. *There exists a constant* $0 < \delta < 1/2$ *such that for* $M = [\delta N]$, $N = \left[\frac{\log x}{\log q}\right]$ *we have*

$$\sum_{\substack{l_1,l_2<q^M \\ (l_1,q)=1 \\ l_1 \ne l_2}} \left| T_{l_1,l_2}^{(M)} - \frac{x}{\varphi(q^M)\log^2 x} H(l_2 - l_1) \right| < \frac{\epsilon(x) x q^M}{\log^2 x}, \tag{5.13}$$

with a suitable function $\epsilon(x) \to 0$ $(x \to \infty)$, *where*

$$H(d) := \prod_{\substack{p|d \\ p\nmid q}} \left(1 + \frac{1}{p-2}\right). \tag{5.14}$$

In [44] we proved that Conjecture 5.3 implies the fulfilment of Conjecture 5.2.

Let $Y(x)$ be a monotically increasing function such that $Y(x) \to \infty$ and $\frac{\log Y(x)}{\log x} \to 0$ as $x \to \infty$. Let $\mathcal{N}_x := \{n \in [0,x],\ p(n) > Y(x)\}$, where $p(n)$ is the smallest prime factor of n. Let $N(x) = \text{card}\ \mathcal{N}_x$. Let L be the strongly multiplicative function defined on primes p with the relation

$$L(p) = \begin{cases} \frac{1}{p-2} & \text{if } p > 2 \text{ and } p \not| q, \\ 0 & \text{otherwise.} \end{cases}$$

In [44] we proved the following assertion:

If $g \in \mathcal{M}_q$, $|g(n)| = 1$ for $n \in \mathbb{N} \cup \{0\}$,

$$U(x) := \sum_{n \in \mathcal{N}_x} g(n), \tag{5.15}$$

then

$$\left|\frac{U(x)}{N(x)}\right|^2 \le \sum_{d<\mathcal{D}} \frac{L(d)}{d} \sum_{a=0}^{d-1} \left|q^{-M} S\left(q^M \,\middle|\, \frac{a}{d}\right)\right|^2 + \frac{c_1}{\mathcal{D}} + o_x(1), \tag{5.16}$$

where M is an arbitrary integer in the interval $q^{-1}x^{1/4} \le q^M < qx^{1/4}$, c_1 is a positive constant which depends only on q, the constant standing implicitly in $o_x(1)$ depends only on the choice of $Y(x)$ (and does not depend on g), furthermore $\mathcal{D} \ge 1$ is an arbitrary real number.

Remark. As a consequence of the above assertion we have that (5.11) implies that $U(x) = o(1)N(x)$ as $x \to \infty$.

5.3. The distribution of q-ary digits on some subsets of integers

Let $\mathcal{B}$ be an infinite subset of $\mathbb{N} \cup \{0\}$ with cardinality function $B(x) = \sharp\{b \le x,\ b \in \mathcal{B}\}$. For $0 \le l_1 < l_2 < \dots l_h\ (\le n)$, $b_1, \dots, b_h \in A$ let $A_{\mathcal{B}}\left(x \,\middle|\, \begin{matrix} l \\ b \end{matrix}\right)$ be the size of the set of integers $n \le x$ for which $n \in \mathcal{B}$, and $e_{l_j}(n) = b_j$ $(j = 1, \dots, h)$ simultaneously hold.

Conjecture 5.4. *For each choice of* $(1\le)l_1<\ldots<l_h$ *and* $b_1,\ldots,b_h\in A$, *such that* $h\le c_1\log N$, *we have*

$$\sup_{1\le h\le c_1\log N}\ \sup_{\substack{l_1,\ldots,l_h\\ b_1,\ldots,b_h}}\left|\frac{q^h A_{\mathcal{P}}\left(x\,\middle|\,\begin{matrix} l\\ b\end{matrix}\right)}{\pi(x)}-1\right|\to 0 \tag{5.17}$$

as $x\to\infty$. *Here* $\mathcal{P}$ *is the set of primes.*

Remark. Perhaps (5.17) remains valid extending the supremum for $h<\frac{1}{3}N$, say. It is known to be true for both of the extremal cases $l_h<N/3$, $l_l>N-N/3$. The first assertion is proved by R. Heath-Brown, the second follows from the prime-number theorem for short intervals.

5.4. Distribution of integers with missing digits in arithmetical progressions

Let $\mathcal{H}$ denote the set of those integers n the digits $e_j(n)$ of which belong to $\{0,1\}$ in their ternary expansions. How they are distributed in arithmetical progressions?

Let $g\in\mathcal{M}_3$ be defined by $g(0)=g(1\cdot 3^j)=1$, $g(2\cdot 3^j)=0$ $(j=0,1,2,\ldots)$. Then $g(n)=1$ or 0 according to $n\in\mathcal{H}$ or not.

Let

$$E(x,d,l)=\sum_{\substack{n<x\\ n\equiv l \pmod d}} g(n),\qquad E(x)=\sum_{n<x} g(n),$$

$$U(x;d,f)=\sum_{n<x} g(n)e\left(\frac{fn}{d}\right).$$

Then

$$E(x,d,l)-\frac{E(x)}{d}=\frac{1}{d}\sum_{f=1}^{d-1} e\left(-\frac{fl}{d}\right)U(x,d,f).$$

Let us restrict ourselves to the subsequence $x=3^N$ $(N=1,2,\ldots)$. Then

$$\left|\frac{E(3^N,d,l)}{2^N}-\frac{1}{d}\right|\le\frac{1}{d}\sum_{f=1}^{d-1}\hat{T}_f,$$

where

$$T_f = \prod_{j=0}^{N-1} \frac{\left|1 + e\left(\frac{f \cdot 3^j}{d}\right)\right|}{2}.$$

Assume that $(d, 3) = 1$. Let $\frac{f}{d} = \frac{F}{\mathcal{D}}$, $(F, \mathcal{D}) = 1$. If $\left\|\frac{F \cdot 3^j}{\mathcal{D}}\right\| < \frac{1}{6}$, then $\left\|\frac{F \cdot 3^{j+1}}{\mathcal{D}}\right\| = 3 \cdot \left\|\frac{F \cdot 3^j}{\mathcal{D}}\right\|$. Hence it follows that

$$\max_{j=t,\dots,t+s-1} \left\|\frac{F \cdot 3^j}{\mathcal{D}}\right\| > \frac{1}{6},$$

where $s = \left[\frac{\log d}{\log 3}\right] + 1$, and t is an arbitrary integer. Since $\frac{|1 + e(\alpha)|}{2} \le \frac{1}{\sqrt{2}}$ if $||\alpha|| \ge \frac{1}{6}$, therefore

$$|T_f| \le \left(\frac{1}{\sqrt{2}}\right)^{[N/s]}$$

Hence

$$\left|\frac{E(3^N, d, l)}{2^N} - \frac{1}{d}\right| \le \frac{c_1}{d} \cdot \left(\frac{1}{2}\right)^{\frac{1}{2}\frac{N \log 3}{\log d} - \frac{\log d}{\log 3}}$$

The exponent on the right hand side is positive if d is not too large, i.e. if

$$\log d < \left(\frac{(\log 2) \cdot (\log 3)}{2}\right)^{1/2} N^{1/2}$$

Conjecture 5.5. *Let $\epsilon_x \to 0$ arbitrarily, d be an arbitrary positive integer coprime to 3, $d \le x^{\epsilon_x}$. Then*

$$\max_{l \pmod d} \left|\frac{dE(x, d, l)}{E(x)} - 1\right| \to 0$$

uniformly as $x \to \infty$.

Conjecture 5.6. *For a given $q \ge 3$ let $\mathbb{B} = \{b_0, \dots, b_{k-1}\}$ be a proper subset of A, $b_0 = 0$. Let $k \ge 2$. Let $\mathcal{H}$ be the set of those integers n the q-ary digits of which belong to $\mathbb{B}$. Let*

$$E(x, d, l) = \sharp\{n \le x, \quad n \equiv l \pmod d, \quad n \in \mathcal{H}\},$$

$$E(x) = \sharp\{n \leq x, \quad n \in \mathcal{H}\}.$$

Let $\epsilon_x \to 0$ arbitrarily, d run over those integers up to x^{ϵ_x}, for which $(d,q)=1$, and $fb_l \not\equiv 0 \pmod d$ holds for at least one $b_l \in \mathbb{B}$ for each $f \in \{1, \ldots, d-1\}$. Then

$$\max_{l \pmod d} \left| \frac{dE(x,d,l)}{E(x)} - 1 \right| \to 0$$

uniformly as $x \to \infty$.

References

[1] **Barnsley H.**, *Fractals everywhere*, Academic Press, 1988.

[2] **Indlekofer K.-H., Kátai I. and Racskó P.**, Number systems and fractal geometry, *Probability theory and applications*, eds. J.Galambos and I.Kátai, Kluwer, 1992, 319-334.

[3] **Indlekofer K.-H., Kátai I. and Racskó P.**, Some remarks on generalized number systems, *Acta Sci. Math.*, **57** (1993), 543-553.

[4] **Kátai I. and Környei I.**, On number systems in algebraic fields, *Publ. Math. Debrecen*, **41** (1992), 289-294.

[5] **Steidl G.**, On symmetric representation of Gaussian integers, *BIT*, **29** (1989), 563-571.

[6] **Kátai I.**, Number systems in imaginary quadratic fields, *Annales Univ. Sci. Bud. Sect. Comp.*, **14** (1994), 91-103.

[7] **Erdős P.**, On the distribution function of additive functions, *Annals of Math.*, **47** (1946), 1-20.

[8] **Kátai I.**, Characterization of arithmetical functions, some problems and results, *Proc. of Number Theory Conference held at Université Laval in 1987*, W.Gruyter Co., 1987, 544-545.

[9] **Elliott P.D.T.A.**, *Probabilistic number theory I-II.*, Springer, 1979.

[10] **Kátai I.**, Characterization of $\log n$, *Studies in Pure Math., To the memory of P.Turán*, Akadémiai Kiadó, 1984, 415-421.

[11] **Elliott P.D.T.A.**, On sums of an additive arithmetic function with shifted arguments, *J.London Math. Soc.*, **22** (1980), 25-38.

[12] **Hildebrand A.**, An Erdős-Wintner theorem for differences of additive functions, *Trans. Amer. Math. Soc.*, **310** (1988), 257-276.

[13] **Indlekofer K.H. and Kátai I.**, On the distribution of translates of additive functions, *Acta Math. Hungar.*, **61** (1993), 343-356.

[14-19] **Kátai I.**, Multiplicative functions with regularity properties I-VI., *Acta Math. Hungar.*, **42** (1983), 295-308, **43** (1984), 105-130, **43** (1984) 259-272, **44** (1984), 125-132, **45** (1985), 379-380, **58** (1991), 343-350.

[20] **Hildebrand A.**, Multiplicative functions at consecutive integers I-II., *Math. Proc. Cambridge Phil. Soc.*, **100** (1986), 229-236, **103** (1988), 389-398.

[21-24] **Indlekofer K.-H. and Kátai I.**, Multiplicative functions with small increments I-III., *Acta Math. Hungar.*, **55** (1990), 97-101, **56** (1990), 159-164, **58** (1991), 121-132.

[25] **Wirsing E.**, The proof was presented in a Number Theory meeting in Oberwolfach, 1984.

[26] **Bassily N.L. and Kátai I.**, On the pairs of multiplicative functions satisfying some relations (manuscript)

[27] **Kátai I.**, On additive functions satisfying a congruence, *Acta Sci. Math.*, **47** (1984), 85-92.

[28] **Styer R.**, A problem of Kátai on sums of additive functions, *Acta Sci. Math.*, **55** (1991), 269-286.

[29] **van Rossum-Wijsmuller M.**, Additive functions on the Gaussian integers, *Publ. Math. Debrecen*, **38** (3-4) (1991), 255-262.

[30] **Kátai I. and van Rossum-Wijsmuller M.**, Additive functions satisfying congruences, *Acta Sci. Math.*, **56** (1992), 63-72.

[31] **Daróczy Z. and Kátai I.**, On additive numbertheoretical functions with values in a compact Abelian group, *Aequationes Math.*, **28** (1985), 288-292.

[32] **Daróczy Z. and Kátai I.**, On additive arithmetical functions with values in the circle group, *Publ. Math. Debrecen*, **34** (1984), 307-312.

[33-34] **Daróczy Z. and Kátai I.**, On additive arithmetical functions with values in topological groups I-II., *Publ. Math. Debrecen*, **33** (1986), 287-292, **34** (1987), 65-68.

[35] **Daróczy Z. and Kátai I.**, On additive functions taking values from a compact group, *Acta Sci. Math.*, **53** (1989), 59-65.

[36] **Daróczy Z. and Kátai I.**, Characterization of additive functions with values in the circle group, *Publ. Math. Debrecen*, **36** (1991), 1-7.

[37] **Kátai I.**, Some problems on the iteration of multiplicative numbertheoretical functions, *Acta Math. Acad. Sci. Hungar.*, **19** (1968), 441-450.

[38] **Pollack R.M., Shapiro H.N. and Sparer G.H.**, On the graphs of I.Kátai, *Communicatons on Pure and Applied Math.*, **27** (1974), 669-713.

[39] **Kátai I.**, On the iteration of multiplicative functions, *Publ. Math. Debrecen*, **36** (1989), 129-134.

[40] **Erdős P. and Kátai I.**, On the growth of some additive functions on small intervals, *Acta Math. Acad. Sci. Hungar.*, **33** (1979), 345-359.

[41] **Kátai I.**, Research problems in number theory, *Publ. Math. Debrecen*, **24** (1977), 263-276.

[42] **Halberstam H. and Richert H.**, *Sieve methods*, Academic Press, 1974.

[43] **Delange H.**, Sur les fonctions q-additives ou q-multiplicatives, *Acta Arithm.*, **21** (1972), 285-298.

[44] **Kátai I.**, Distribution of q-additive functions, *Probability theory and applications*, eds. J.Galambos and I.Kátai, Kluwer, 1992, 309-318.

I. Kátai
Department of Computer Algebra
Eötvös Loránd University
VIII. Múzeum krt. 6-8.
H-1088 Budapest, Hungary

Department of Applied Mathematics
Janus Pannonius University
Ifjúság u. 6.
H-7624 Pécs, Hungary