NEWTON SEQUENCES AND DIRICHLET CONVOLUTION

Klaudiusz Wójcik
Faculty of Mathematics, Jagiellonian University, Kraków, Poland
Klaudiusz.Wojcik@uj.edu.pl

Received: 12/4/20, Revised: 4/20/21, Accepted: 5/29/21, Published: 6/3/21

Abstract

An integer sequence $a : \mathbb{N} \longrightarrow \mathbb{Z}$ is called a *Newton sequence* generated by the sequence of integers $c : \mathbb{N} \longrightarrow \mathbb{Z}$, if the following *Newton identities* hold

$$a(n) = c(1)\, a(n-1) + \ldots + c(n-1)\, a(1) + n\, c(n).$$

We show that a is a Newton sequence if and only if

$$\sum_{d|n} f(d)\, a(n/d) \equiv 0 \pmod{n}, \quad n \geq 1,$$

for every function $f : \mathbb{N} \longrightarrow \mathbb{Z}$ satisfying the two conditions

$$\sum_{d|n} f(d) \equiv 0 \pmod{n}, \quad f(1) = \pm 1.$$

In particular, f may be the Möbius function, the Euler totient function or the Jordan totient function.

1. Introduction

We recall some basic facts concerning Dirichlet involution (see [2]). Let $\mathcal{A}(\mathbb{C})$ be the set of all complex-valued arithmetical functions, i.e., the set of functions defined on $\mathbb{N}$ with values in $\mathbb{C}$. By $\mathcal{A}(\mathbb{Z}) \subset \mathcal{A}(\mathbb{C})$ we denote the set of all integer-valued sequences. The *Dirichlet convolution* of functions $f, g \in \mathcal{A}(\mathbb{C})$ is the function $f * g \in \mathcal{A}(\mathbb{C})$ defined by

$$(f * g)(n) = \sum_{d|n} f(d) g(n/d) = \sum_{d_1 d_2 = n} f(d_1) g(d_2), \quad n \geq 1.$$

For any non-empty subsets A, B of $\mathcal{A}(\mathbb{C})$ we put

$$A * B := \{a * b : a \in A,\, b \in B\}.$$

We distinguish the following integer-valued sequences:

(ϵ) the *multiplicative identity with respect to Dirichlet convolution*:

$$\epsilon(n) = \left\lfloor \frac{1}{n} \right\rfloor = \begin{cases} 1, & \text{if } n = 1 \\ 0, & \text{if } n > 1, \end{cases}$$

(μ) the *Möbius function* μ:

$$\mu(n) = \begin{cases} 1, & \text{if } n = 1 \\ (-1)^r, & \text{if } n \text{ is a product of } r \text{ different primes} \\ 0, & \text{otherwise.} \end{cases}$$

(I_k) $I_k(n) = n^k$ for $k \geq 0$,

(S_f) the *divisor sum* over $f \in \mathcal{A}(\mathbb{Z})$:

$$S_f(n) := f * I_0(n) = \sum_{d|n} f(d), \quad n \geq 1,$$

(φ) the *Euler totient function* φ:

$$\varphi(n) = \mu * I_1(n) = \sum_{\substack{1 \leq k \leq n \\ (k,n)=1}} 1,$$

(J_k) the *Jordan totient function* J_k:

$$J_k(n) = \mu * I_k(n) = \sum_{\substack{1 \leq a_1, \ldots, a_k \leq n \\ (a_1, \ldots, a_k, n)=1}} 1.$$

The set of arithmetical functions $\mathcal{A}(\mathbb{C})$ is a commutative ring under pointwise addition and Dirichlet convolution. The invertible elements of this ring are the arithmetical functions f with $f(1) \neq 0$. The following well-known facts will be useful later ([2]):

(1) $S_\mu = \mu * I_0 = \epsilon$,

(2) the *Möbius inversion formula*: $S_f = f * I_0$ if and only if $f = \mu * S_f$,

(3) $S_\varphi = I_1$,

(4) $S_{J_k} = I_k$.

Definition 1. Let $a \in \mathcal{A}(\mathbb{Z})$ be a sequence of integers. We say that $a \equiv 0$, if

$$a(n) \equiv 0 \pmod{n},$$

for all $n \geq 1$.

We put

$$\begin{aligned}\mathcal{A}^*(\mathbb{Z}) :=& \big\{a \in \mathcal{A}(\mathbb{Z}) : a(1) = \pm 1\big\},\\ \mathcal{A}_0(\mathbb{Z}) :=& \big\{a \in \mathcal{A}(\mathbb{Z}) : a \equiv 0\big\},\\ \mathcal{A}_0^*(\mathbb{Z}) :=& \mathcal{A}^*(\mathbb{Z}) \cap \mathcal{A}_0(\mathbb{Z}),\\ \mathcal{M}(\mathbb{Z}) :=& \big\{f \in \mathcal{A}(\mathbb{Z}) : S_f \in \mathcal{A}_0^*(\mathbb{Z})\big\}.\end{aligned}$$

Example 2. It follows that $I_k \in \mathcal{A}_0^*(\mathbb{Z})$ and $\mu, \varphi, J_k \in \mathcal{M}(\mathbb{Z})$.

Corollary 3.

(1) Every $a \in \mathcal{A}^*(\mathbb{Z})$ admits an inverse $a^{-1} \in \mathcal{A}(\mathbb{Z})$,

(2) $\mathcal{A}_0(\mathbb{Z}) * \mathcal{A}_0(\mathbb{Z}) \subset \mathcal{A}_0(\mathbb{Z})$,

(3) $\mathcal{A}_0^*(\mathbb{Z}) * \mathcal{A}_0^*(\mathbb{Z}) \subset \mathcal{A}_0^*(\mathbb{Z})$,

(4) $(\mathcal{A}_0^*(\mathbb{Z}), *)$ is the commutative group,

(5) $\mathcal{M}(\mathbb{Z}) = \big\{\mu * g : g \in \mathcal{A}_0^*(\mathbb{Z})\big\}$.

Proof. The conditions (1) and (5) are obvious. If $a, b \in \mathcal{A}_0(\mathbb{Z})$, then

$$a * b(n) = \sum_{d|n} a(d)b(n/d) \equiv 0 \pmod{n},$$

hence (2) follows. We claim that $a^{-1} \equiv 0$ for $a \in \mathcal{A}_0^*(\mathbb{Z})$. We use the induction on n. It is trivial for $n = 1$. For $n > 1$, by [[2], Theorem 2.8] and the inductive step, we get that

$$a^{-1}(n) = \pm \sum_{\substack{d|n\\ d>1}} a(d)a^{-1}(n/d) \equiv 0 \pmod{n}.$$

□

Definition 4 (Newton sequence)**.** A sequence of integers $a \in \mathcal{A}(\mathbb{Z})$ is called a *Newton sequence* generated by the sequence of integers $c \in \mathcal{A}(\mathbb{Z})$, if the following *Newton identities* hold: for all $n \in \mathbb{N}$

$$a(n) = c(1)\, a(n-1) + \ldots + c(n-1)\, a(1) + n\, c(n).$$

Denote by $\mathcal{A}_N(\mathbb{Z})$ the set of Newton sequences, i.e.,

$$\mathcal{A}_N(\mathbb{Z}) = \{a : a \text{ is a Newton sequence generated by a sequence of integers c}\}.$$

Example 5 (Sequence of traces)**.** For a square integer matrix $A \in M_l(\mathbb{Z})$ we define a *sequence of traces* $\operatorname{tr}[A] \in \mathcal{A}(\mathbb{Z})$ by

$$(\operatorname{tr}[A])_n := \operatorname{tr} A^n, \quad n \geq 1.$$

It follows by the classical Newton's identities that a Newton sequence $a \in \mathcal{A}(\mathbb{Z})$ is generated by a finite sequence $c = (c(1), \ldots, c(l)) \in \mathcal{A}(\mathbb{Z})$ (i.e., $c(n) = 0$ for $n > l$) if and only if a is the sequence of traces $\operatorname{tr}[A]$, where A is the *companion matrix* of the monic polynomial $w(x) = x^l - c(1)x^{l-1} - \ldots - c(l-1)x - c(l) \in \mathbb{Z}[x]$, i.e.,

$$A := A[c(1), \ldots, c(l)] := \begin{bmatrix} 0 & 0 & \ldots & 0 & c(l) \\ 1 & 0 & \ldots & 0 & c(l-1) \\ 0 & 1 & \ldots & 0 & c(l-2) \\ \vdots & 0 & \ddots & 0 & \vdots \\ 0 & \ldots & 0 & 1 & c(1) \end{bmatrix} \in M_l(\mathbb{Z}).$$

Since $w(X) = \det(XI_l - A) \in \mathbb{Z}[X]$, the eigenvalues of A are the roots of w.

Definition 6 (Dold-Fermat sequence [6])**.** A sequence $a \in \mathcal{A}(\mathbb{Z})$ is called a *Dold-Fermat sequence*, if $\mu * a \in \mathcal{A}_0(\mathbb{Z})$, i.e.,

$$\sum_{d|n} \mu(d)\, a(n/d) \equiv 0 \pmod{n}, \quad n \geq 1.$$

In combinatorics and number theory, Dold-Fermat sequences have also been called *pre-realizable sequences*, *relatively realizable sequences*, *Gauss sequences* and *generalized Fermat sequences* ([1, 3, 7, 8, 9, 10, 11, 13, 14]).

We prove the following theorem.

Theorem 7. *For $a \in \mathcal{A}(\mathbb{Z})$ the following conditions are equivalent:*

(1) a is a Newton sequence,

(2) a is a Dold-Fermat sequence,

(3) $f * a \in \mathcal{A}_0(\mathbb{Z})$, i.e.,

$$\sum_{d|n} f(d)\, a(n/d) \equiv 0 \pmod{n}, \quad n \geq 1,$$

for every $f \in \mathcal{M}(\mathbb{Z})$.

The equivalence of the conditions (1) and (2) was proved in [8]. On the other hand, it was observed in [1] that in the definition of the Dold-Fermat sequence the Möbius function can be replaced by the Euler totient function φ.

In the last section, we define the unitary analog of the Newton sequences. In particular, we show that a unitary Newton sequence is periodic if and only if it is bounded. We also prove that a p-periodic unitary sequence with prime period has to be constant.

2. Newton Sequences

Lemma 8. *Let $a \in \mathcal{A}(\mathbb{Z})$ and $f \in \mathcal{M}(\mathbb{Z})$. The following conditions are equivalent:*

(1) $\mu * a \in \mathcal{A}_0(\mathbb{Z})$,

(2) $f * a \in \mathcal{A}_0(\mathbb{Z})$.

Proof. We first show that (1) implies (2). We have

$$f * a = \epsilon * f * a = \mu * I_0 * f * a = (\mu * a) * S_f \in \mathcal{A}_0(\mathbb{Z}),$$

by Corollary 3. Assume that (2) holds. We have

$$(\mu * a) * S_f = f * a \in \mathcal{A}_0(\mathbb{Z}).$$

Since S_f belongs to $\mathcal{A}_0^*(\mathbb{Z})$, S_f^{-1} does and by Corollary 3, one has

$$\mu * a = S_f^{-1} * (f * a) \in \mathcal{A}_0(\mathbb{Z}).$$

□

Remark 9. Observe that in the proof of implication (1) $\Longrightarrow$ (2) we need only that $S_f \in \mathcal{A}_0(\mathbb{Z})$ and f does not have to be invertible. In particular, one can take f of the form $f = \mu * g$ for some $g \in \mathcal{A}_0(\mathbb{Z})$.

As a consequence, one has the following result.

Theorem 10. *Assume that $a \in \mathcal{A}(\mathbb{Z})$. The following conditions are equivalent:*

(1) $a \in \mathcal{A}_N(\mathbb{Z})$,

(2) $\mu * a \in \mathcal{A}_0(\mathbb{Z})$,

(3) $f * a \in \mathcal{A}_0(\mathbb{Z})$ *for every* $f \in \mathcal{M}(\mathbb{Z})$.

Proof. The equivalence of the conditions (1) and (2) was proved in [8]. □

Lemma 11. *Let $f \in \mathcal{M}(\mathbb{Z})$. Then*

$$F : \mathcal{A}_0(\mathbb{Z}) \ni b \longmapsto f^{-1} * b \in \mathcal{A}_N(\mathbb{Z})$$

is a bijective map.

Proof. If $b \in \mathcal{A}_0(\mathbb{Z})$ then $f * f^{-1} * b = b \in \mathcal{A}_0(\mathbb{Z})$, hence $f^{-1} * b \in \mathcal{A}_N(\mathbb{Z})$ by Theorem 10, so F is well-defined. Since F is obviously injective, it is sufficient to show its surjectivity. If $a \in \mathcal{A}_N(\mathbb{Z})$ then $f * a \in \mathcal{A}_0(\mathbb{Z})$, hence $f * a = b$ for some $b \in \mathcal{A}_0(\mathbb{Z})$, so $a = f^{-1} * b$. □

Corollary 12. *The following maps are bijective:*

(a) $\mathcal{A}_0(\mathbb{Z}) \ni b \longmapsto \mu^{-1} * b = S_b \in \mathcal{A}_N(\mathbb{Z})$,

(b) $\mathcal{A}_0(\mathbb{Z}) \ni b \longmapsto \varphi^{-1} * b = S_{\mu \cdot I_1} * b \in \mathcal{A}_N(\mathbb{Z})$.

Example 13 (Newton sequences)**.** The following well-known sequences can be interpreted as Newton sequences:

(1) $\sigma_1(n) = S_{I_1}(n) = \sum_{d|n} d$,

(2) $\sigma_k(n) = S_{I_k}(n) = \sum_{d|n} d^k$,

(3) $S_{\mu \cdot I_1} * (n!) = \sum_{d|n} d\mu(d)(n/d)!$,

(4) $S_{\mu \cdot I_1} * I_k(n) = \sum_{d|n} d\mu(d)(n/d)^k = \sum_{d|n} \mu(d) \frac{n^k}{d^{k-1}}$.

Lemma 14. *If* $a \in \mathcal{A}_N(\mathbb{Z})$ *and* $b \in \mathcal{A}_0(\mathbb{Z})$*, then* $a * b \in \mathcal{A}_N(\mathbb{Z})$.

Proof. Since $b, \mu * a \in \mathcal{A}_0(\mathbb{Z})$, we have

$$\mu * (a * b) = b * (\mu * a) \in \mathcal{A}_0(\mathbb{Z}),$$

so $a * b \in \mathcal{A}_N(\mathbb{Z})$. □

Example 15 (Newton sequences)**.** The following sequences are Newton sequences:

(1) $a * I_k(n) = \sum_{d|n} d^k a(n/d)$,

(2) $b(n) = \sum_{d|n} a(n/d)\, d!$.

Corollary 16. *If* $a, b \in \mathcal{A}_N(\mathbb{Z})$*, then* $\mu * a * b \in \mathcal{A}_N(\mathbb{Z})$.

Corollary 17. *The map*

$$\mathcal{A}_0^*(\mathbb{Z}) \times \mathcal{A}_N(\mathbb{Z}) \ni (b, a) \longmapsto b * a \in \mathcal{A}_N(\mathbb{Z})$$

is an action of the group $\mathcal{A}_0^*(\mathbb{Z})$ *on the set* $\mathcal{A}_N(\mathbb{Z})$.

We put

$$\mathcal{A}_{N_*}(\mathbb{Z}) = \{a \in \mathcal{A}_N(\mathbb{Z}) : a(1) \neq 0\}, \quad \mathcal{A}_{N_1}(\mathbb{Z}) = \{a \in \mathcal{A}_{N_*}(\mathbb{Z}) : a(1) = \pm 1\},$$

so $\mathcal{A}_{N_*}(\mathbb{Z})$ is the set of all invertible Newton sequences and for every $a \in \mathcal{A}_{N_1}(\mathbb{Z})$ the inverse of a belongs to $\mathcal{A}(\mathbb{Z})$.

Example 18. We have $I_0 \in \mathcal{A}_{N_1}(\mathbb{Z})$, but $I_0^{-1} = \mu \notin \mathcal{A}_{N_1}(\mathbb{Z})$.

Lemma 19. *The map*

$$\mathcal{A}_0^*(\mathbb{Z}) \times \mathcal{A}_{N_*}(\mathbb{Z}) \ni (b,a) \longmapsto b * a \in \mathcal{A}_{N_*}(\mathbb{Z})$$

is a free but not transitive action of the group $\mathcal{A}_0^*(\mathbb{Z})$ *on the set* $\mathcal{A}_{N_*}(\mathbb{Z})$.

Proof. Since $b*a(1) = b(1)a(1) = \pm a(1) \neq 0$, $b*a \in \mathcal{A}_{N_*}(\mathbb{Z})$. We first show that the action is free. Let $b*a = a$. This implies $b = \epsilon$ because a is invertible. Next, we claim that the action is not transitive. It is obvious that $I_0, 2\cdot I_0 \in \mathcal{A}_{N_*}(\mathbb{Z})$. Suppose that $b * I_0 = 2\cdot I_0$ for some $b \in \mathcal{A}_0^*(\mathbb{Z})$. Then $b = 2\cdot\epsilon$ and $b(1) = 2 \neq \pm 1$. This creates a contradiction because $b \in \mathcal{A}_0^*(\mathbb{Z})$. □

Lemma 20. *The map*

$$\mathcal{A}_0^*(\mathbb{Z}) \times \mathcal{A}_{N_1}(\mathbb{Z}) \ni (b,a) \longmapsto b * a \in \mathcal{A}_{N_1}(\mathbb{Z})$$

is a free and transitive action of the group $\mathcal{A}_0^*(\mathbb{Z})$ *on* $\mathcal{A}_{N_1}(\mathbb{Z})$.

Proof. Since $b*a(1) = b(1)a(1) = \pm 1$, $b*a \in \mathcal{A}_{N_1}(\mathbb{Z})$. The action is free by Lemma 19. We show the transitivity of the action. For this, we consider two different elements a_1 and a_2 of $\mathcal{A}_{N_1}(\mathbb{Z})$. Let $b = a_1^{-1} * a_2$. We have $b * a_1 = a_2$ and $b(1) = \pm 1$, so it is sufficient to show that $b \in \mathcal{A}_0(\mathbb{Z})$. Since $\mu * a_1, \mu * a_2 \in \mathcal{A}_0(\mathbb{Z})$, we have

$$b = a_1^{-1} * I_0 * \mu * a_2 = (\mu * a_1)^{-1} * (\mu * a_2) \in \mathcal{A}_0(\mathbb{Z}).$$

□

Corollary 21. *If* $a_1, a_2 \in \mathcal{A}_{N_1}(\mathbb{Z})$, *then* $a_1^{-1} * a_2 \in \mathcal{A}_0^*(\mathbb{Z})$.

Example 22. For $\sigma_1 \in \mathcal{A}_{N_1}(\mathbb{Z})$, we have $\sigma_1^{-1} = (\mu \cdot I_1) * \mu$, hence $(\mu\cdot I_1) * \mu * a \in \mathcal{A}_0^*(\mathbb{Z})$ for all $a \in \mathcal{A}_{N_1}(\mathbb{Z})$.

Proposition 23. $\mathcal{A}_0(\mathbb{Z}) \cap \mathcal{A}_N(\mathbb{Z}) = \{0^\infty\}$.

Proof. We use the induction with respect to n. Assume that $n = 1$. Since $a \in \mathcal{A}_0(\mathbb{Z}) \cap \mathcal{A}_N(\mathbb{Z})$, for prime p we have $a(p) \equiv 0 \pmod p$ and $a(p) \equiv a(1) \pmod p$. It follows that $a(1) \equiv 0 \pmod p$ for every prime p, i.e., $a(1) = 0$. Let $n \geq 2$ and assume that $a(1) = \ldots = a(n-1) = 0$. We show that $a(n) = 0$. Let $p > n$ be a prime number. We have

$$\sum_{d|pn} \mu(d) a\Big(\frac{pn}{d}\Big) = \sum_{d|n} \mu(d) a\Big(\frac{pn}{d}\Big) + \sum_{d|n} \mu(pd) a\Big(\frac{n}{d}\Big) \equiv 0 \pmod{pn},$$

and consequently,

$$\sum_{d|n} \mu(d) a\Big(\frac{pn}{d}\Big) - a(n) \equiv 0 \pmod{pn}.$$

On the other hand, $a \in \mathcal{A}_0(\mathbb{Z})$ implies that $a\big(\frac{pn}{d}\big) \equiv 0 \pmod{\frac{pn}{d}}$ for all $d|n$, hence $a\big(\frac{pn}{d}\big) \equiv 0 \pmod p$. It follows that $a(n) \equiv 0 \pmod p$ for every prime $p > n$, and $a(n) = 0$. □

3. Unitary Newton Sequences

We recall that d is a *unitary divisor* of the positive integer n if $d|n$ and $(d, n/d) = 1$. It will be denoted by $d\|n$. Obviously, $1\|n$ and $n\|n$. For $f, g \in \mathcal{A}(\mathbb{Z})$ we define their *unitary convolution* $f \circ g$ by the formula

$$f \circ g(n) = \sum_{d\|n} f(d)g(n/d), \quad n \geq 1.$$

Notice that $f \circ g(n) = f * g(n)$ for all square-free $n \geq 1$. We summarize some well-known facts concerning unitary convolution.

- The Dirichlet and the unitary convolution, have the same identity element ϵ.
- If $f \in \mathcal{A}(\mathbb{Z})$ satisfies $f(1) = \pm 1$, then f has the unitary inverse $\overline{f}^{-1} \in \mathcal{A}(\mathbb{Z})$.
- The *unitary sum function* $\overline{S}_f$ is defined as

$$\overline{S}_f(n) = f \circ I_0(n) = \sum_{d\|n} f(d), \quad n \geq 1.$$

- The *unitary Möbius function* $\overline{\mu}$ is defined as the unitary inverse of I_0, i.e., $\overline{\mu} * I_0 = \epsilon$. Since $\overline{\mu}$ is multiplicative, it is determined by its values at the powers of primes. We have

$$0 = \sum_{d\|p^k} \overline{\mu}(d) = \overline{\mu}(p^k) + \overline{\mu}(1),$$

hence $\overline{\mu}(p^k) = -1$ and $\overline{\mu}(n) = (-1)^{\omega(n)}$, where $\omega(n)$ is the number of distinct prime factors of n.

Definition 24 (Unitary Newton sequence)**.** Let $a \in \mathcal{A}(\mathbb{Z})$. We say that a is a *unitary Newton sequence*, if $\overline{\mu} \circ a \in \mathcal{A}_0(\mathbb{Z})$, i.e.,

$$\sum_{d\|n} (-1)^{\omega(d)}\, a(n/d) \equiv 0 \pmod{n}, \quad n \geq 1.$$

By $\mathcal{A}_{UN}(\mathbb{Z})$ we denote the set of all unitary Newton sequences.

Corollary 25. *For $a \in \mathcal{A}(\mathbb{Z})$ the following conditions are equivalent:*

(1) $a \in \mathcal{A}_{UN}(\mathbb{Z})$,

(2) $a = \overline{S}_b = b \circ I_0$ *for some* $b \in \mathcal{A}_0(\mathbb{Z})$.

Proof. Obviously, $\overline{\mu} \circ a = b$ for some $b \in \mathcal{A}_0(\mathbb{Z})$ is equivalent to $a = b \circ I_0 = \overline{S}_b$ for some $b \in \mathcal{A}_0(\mathbb{Z})$. □

Example 26. The sum of unitary divisors function $\overline{\sigma}_1$ given by

$$\overline{\sigma}_1(n) = \sum_{d \| n} d = \overline{S}_{I_1}(n).$$

It follows that $\overline{\sigma}_1 \in \mathcal{A}_{UN}(\mathbb{Z})$, but $\overline{\sigma}_1 \notin \mathcal{A}_N(\mathbb{Z})$. Indeed, for prime p we have

$$\overline{\sigma}_1(p^2) = 1 + p^2, \quad \overline{\sigma}_1(p) = 1 + p,$$

hence

$$\sum_{d | p^2} \mu(d)\,\overline{\sigma}_1(p^2/d) = \overline{\sigma}_1(p^2) - \overline{\sigma}_1(p) = p^2 - p \not\equiv 0 \pmod{p^2}.$$

Example 27. The sum of k-th powers of the unitary divisors of n, i.e.,

$$\overline{\sigma}_k(n) = \sum_{d \| n} d^k = \overline{S}_{I_k}(n), \quad k \geq 1,$$

is a unitary Newton sequence.

Corollary 28. *For $a \in \mathcal{A}_{UN}(\mathbb{Z})$ the following conditions hold:*

(1) $a(p^k) \equiv a(1) \pmod{p^k}$ for all prime p and $k \geq 1$,

(2) if a is bounded and p is prime, then $a(p^k) = a(1)$ for almost all $k \geq 1$,

(3) if n is square-free, then

$$\overline{\mu} \circ a(n) = \sum_{d \| n} (-1)^{\omega(d)}\, a(n/d) = \sum_{d | n} \mu(d)\, a(n/d) \equiv 0 \pmod{n},$$

(4) if $a \in \mathcal{A}_N(\mathbb{Z}) \cap \mathcal{A}_{UN}(\mathbb{Z})$, then $a(p^{k-1}) \equiv a(1) \pmod{p^k}$ for prime p and $k \geq 1$.

Proposition 29. *If $a \in \mathcal{A}_{UN}(\mathbb{Z})$ is p-periodic with a prime p, then a is constant.*

Proof. Since $\overline{\mu} \circ a \in \mathcal{A}_0(\mathbb{Z})$, $a(p) \equiv a(1) \pmod{p}$. We first show that $a(1) = \ldots = a(p-1)$. Let $l \in \{2, \ldots, p-1\}$. We consider the arithmetic progression $p_k = l + kp$. Then, by the Dirichlet theorem, p_k is a prime number for infinitely many $k \geq 1$. If p_k is prime, then $a(1) \equiv a(p_k) = a(l) \pmod{p_k}$. Consequently, $a(1) \equiv a(l) \pmod{p_k}$ for infinitely many primes p_k. This shows that $a(1) = a(l)$. It remains to prove that $a(1) = a(p)$. We have that $a(p^k) = a(p)$ because a is p-periodic. It follows by Corollary 28 that $a(p) \equiv a(1) \pmod{p^k}$ for all $k \geq 1$. This means that $a(p) = a(1)$. □

Example 30. Let $k, l \in \mathbb{Z}$ be such that $k \equiv l \pmod{p}$ for prime p. Let a be a p-periodic sequence such that $a(1) = \ldots = a(p-1) = l$ and $a(p) = k$. If $l \neq k$, then $a \in \mathcal{A}_N(\mathbb{Z})$ and $a \notin \mathcal{A}_{UN}(\mathbb{Z})$.

Example 31. Let $a(n) = 2^n$. Then $a \in \mathcal{A}_N(\mathbb{Z})$ and $a \notin \mathcal{A}_{UN}(\mathbb{Z})$. More generally, let $a(n) = m^n$ for some positive integer $m \geq 1$. One can check that, $a \in \mathcal{A}_{UN}(\mathbb{Z})$ if and only if $m = 1$.

Let $\tau(n) = \sum_{d|n} 1$ be the number of divisors of $n \geq 1$ and $\tau^\circ(n) = \sum_{d\|n} 1$ be the number of unitary divisors of n. Since one of two complementary divisors of n is always not greater than $\sqrt{n}$, one has

$$\tau^\circ(n) \leq \tau(n) \leq 2\sqrt{n}.$$

It follows that

$$\lim_{n\to\infty} \frac{\tau(n)}{n} = 0.$$

Lemma 32. *Let $a \in \mathcal{A}_N(\mathbb{Z})$ ($a \in \mathcal{A}_{UN}(\mathbb{Z})$) be a bounded sequence and let $\|a\|_\infty = \max\{|a_i| : i \geq 1\}$. If $n > 4\|a\|_\infty^2$, then*

$$(\mu * a)(n) = 0 \quad ((\overline{\mu} \circ a)(n) = 0).$$

Proof. We have

$$|(\mu * a)(n)| \leq \sum_{d|n} |a(n/d)| \leq \|a\|_\infty \sum_{d|n} 1 \leq 2\|a\|_\infty \sqrt{n},$$

hence $|(\mu * a)(n)| < n$ for $n > 4\|a\|_\infty^2$. Since $(\mu * a)(n) \equiv 0 \pmod{n}$, $(\mu * a)(n) = 0$ for $n > 4\|a\|_\infty^2$. The proof in the unitary case is exactly the same because

$$\tau^\circ(n) \leq \tau(n) \leq 2\sqrt{n}.$$

□

Lemma 33. *Let $a \in \mathcal{A}_{UN}(\mathbb{Z})$ be p^k-periodic for some prime p and $k \geq 1$. Then $a(p^k) = a(1)$.*

Proof. We have $a(p^k) = a(p^l p^k) = a(p^{l+k}) = a(1)$ for l suficiently large. □

Definition 34. Let $k \geq 1$. We define $\bar{b}_k \in \mathcal{A}_0(\mathbb{Z})$ by

$$\bar{b}_k(n) = \begin{cases} k, & \text{if } n = k \\ 0, & \text{otherwise.} \end{cases}$$

It follows that $\overline{S}_{\bar{b}_k} \in \mathcal{A}_{UN}(\mathbb{Z})$ and

$$\overline{S}_{\bar{b}_k}(n) = \sum_{d\|n} \bar{b}_k(d) = \begin{cases} k, & \text{if } k\|n \\ 0, & \text{otherwise.} \end{cases}$$

Let us observe that $\overline{S}_{\bar{b}_k}$ is k^2-periodic. Indeed, it is easy to check that $k\|n$ if and only if $k\|(n + k^2)$. This shows that $\overline{S}_{\bar{b}_k}(n) = \overline{S}_{\bar{b}_k}(n + k^2)$.

Proposition 35. *Let $a \in \mathcal{A}_{UN}(\mathbb{Z})$. The following conditions are equivalent:*

(1) a is bounded,

(2) there exist $l \geq 1$ and integers $x_k \in \mathbb{Z}$ for $1 \leq k \leq l$ such that

$$a = \sum_{k=1}^{l} x_k \, \overline{S}_{\bar{b}_k},$$

(3) a is periodic.

Proof. Obviously, (2) implies (3) and (3) implies (1). We show that (1) implies (2). Assume that a is bounded and $|a(n)| \leq M$ for $n \geq 1$. Since $a = \overline{S}_b$ with $b \in \mathcal{A}_0(\mathbb{Z})$, $a = \overline{S}_{I \cdot \bar{b}}$ for some $\bar{b} \in \mathcal{A}(\mathbb{Z})$. We have $I \cdot \bar{b} = \overline{\mu} * a$, so

$$|\bar{b}(n)| = \frac{1}{n} \Big| \sum_{d \| n} \overline{\mu}(d) \, a(n/d) \Big| \leq \frac{M}{n} \sum_{d \| n} 1 \leq M \frac{\tau(n)}{n}.$$

Since $\frac{\tau(n)}{n} \to 0$, $\bar{b}(n) \to 0$. On the other hand, $\bar{b}$ is a sequence of integers, so there exists $l \geq 1$ such that $\bar{b}(n) = 0$ for $n > l$. It follows that

$$b = (b(1), \ldots, b(l), 0, \ldots) = \sum_{k=1}^{l} \frac{b(k)}{k} \, \bar{b}_k,$$

and consequently,

$$a = \overline{S}_b = \sum_{k=1}^{l} x_k \, \overline{S}_{\bar{b}_k}, \quad x_k = \frac{b(k)}{k}.$$

□

Remark 36. For $k \geq 1$ we consider the sequence $b_k \in \mathcal{A}_0(\mathbb{Z})$ given as

$$b_k(n) = \begin{cases} k, & \text{if } n = k \\ 0, & \text{otherwise.} \end{cases}$$

It follows that $S_{b_k} \in \mathcal{A}_N(\mathbb{Z})$ and

$$S_{b_k}(n) = \sum_{d | n} b_k(d) = \begin{cases} k, & \text{if } k | n \\ 0, & \text{otherwise.} \end{cases}$$

The proof of Proposition 35 shows the well-known fact that a Newton sequence $a \in \mathcal{A}_N(\mathbb{Z})$ is bounded if and only if there are $l \geq 1$ and integers $x_1, \ldots, x_l$ such that

$$a = \sum_{k=1}^{l} x_k \, S_{b_k}.$$

Lemma 37. *If $a, f \in \mathcal{A}(\mathbb{Z})$ are such that $\overline{\mu} \circ a, \overline{S}_f \in \mathcal{A}_0(\mathbb{Z})$, then $f \circ a \in \mathcal{A}_0(\mathbb{Z})$. In particular, $a \in \mathcal{A}_{UN}(\mathbb{Z})$ implies $f \circ a \in \mathcal{A}_0(\mathbb{Z})$.*

Proof. Corollary 3 implies that

$$f \circ a = \epsilon \circ f \circ a = \overline{\mu} \circ I_0 \circ f \circ a = (\overline{\mu} \circ a) \circ \overline{S}_f \in \mathcal{A}_0(\mathbb{Z}).$$

□

Lemma 38. *If $a, f \in \mathcal{A}(\mathbb{Z})$ are such that $f \circ a \in \mathcal{A}_0(\mathbb{Z})$, $\overline{S}_f \in \mathcal{A}_0^*(\mathbb{Z})$, then $\overline{\mu} \circ a \in \mathcal{A}_0(\mathbb{Z})$. In particular, $f \circ a \in \mathcal{A}_0(\mathbb{Z})$ implies that $a \in \mathcal{A}_{UN}(\mathbb{Z})$ provided that $\overline{S}_f \in \mathcal{A}_0^*(\mathbb{Z})$.*

Proof. We have

$$(\overline{\mu} \circ a) \circ \overline{S}_f = f \circ a \in \mathcal{A}_0(\mathbb{Z}).$$

Since $\overline{S}_f \in \mathcal{A}_0^*(\mathbb{Z})$, $\overline{\overline{S}}_f^{-1} \in \mathcal{A}_0^*(\mathbb{Z})$. Consequently, Corollary 3 shows that

$$\overline{\mu} \circ a = \overline{\overline{S}}_f^{-1} \circ (f \circ a) \in \mathcal{A}_0(\mathbb{Z}).$$

□

Corollary 39. *Assume that $a \in \mathcal{A}(\mathbb{Z})$ and $\overline{S}_f \in \mathcal{A}_0^*(\mathbb{Z})$. The following conditions are equivalent:*

(1) $a \in \mathcal{A}_{UN}(\mathbb{Z})$,

(2) $f \circ a \in \mathcal{A}_0(\mathbb{Z})$.

Proof. It follows by Lemma 37 and Lemma 38. □

Example 40. The *unitary Euler totient function* is defined by $\overline{\phi} := \overline{\mu} \circ I_1$, i.e.,

$$\overline{\phi}(n) = \sum_{d \| n} \overline{\mu}(d) \frac{n}{d}.$$

Obviously,

$$\overline{S}_{\overline{\phi}} = \overline{\phi} \circ I_0 = \overline{\mu} \circ I_1 \circ I_0 = I_1 \in \mathcal{A}_0^*(\mathbb{Z}).$$

Similarly, $\overline{S}_{\overline{\phi}_k} \in \mathcal{A}_0^*(\mathbb{Z})$ for $\overline{\phi}_k := \overline{\mu} \circ I_k$.

It was proved in [7] that $a \in \mathcal{A}_N(\mathbb{Z})$ if and only if

$$a(n) \equiv a(n/p) \pmod{p^k},$$

for any $n \in \mathbb{N}$ and for any prime p with $p^k \| n$ (i.e., $p^k | n$ and $n \not\equiv 0 \pmod{p^{k+1}}$).

Proposition 41. *Let $a \in \mathcal{A}(\mathbb{Z})$. The following conditions are equivalent:*

(1) $a \in \mathcal{A}_{UN}(\mathbb{Z})$*,*

(2) $a(n) \equiv a(n/p^k) \pmod{p^k}$ *for any* $n \geq 1$ *and any prime* p *with* $p^k \| n$*.*

Proof. First, we show that (1) implies (2). We use the induction with respect to $\omega(n)$, i.e., the number of prime factors of n. If $\omega(n) = 1$, then $n = p^k$ and the result follows by Corollary 28. Assume that formula holds for $\omega(n) = r$. We prove it for $\omega(n) = r + 1$. Let $n = p_1^{k_1} p_2^{k_2} \dots p_{r+1}^{k_{r+1}}$ with different primes p_i and $k_i \geq 1$. By symmetry, it is sufficient to show that $a(n) \equiv a(n/p_1^{k_1}) \pmod{p_1^{k_1}}$. We consider the set

$$S = \{d : d \| n,\ d \not\equiv 0 \pmod{p_1^{k_1}}\}.$$

We have

$$\begin{aligned} \overline{\mu} \circ a(n) &= \sum_{d \| n} (-1)^{\omega(d)}\, a(n/d) \\ &= \sum_{d \in S} (-1)^{\omega(d)}\, a(n/d) + (-1)^{\omega(p_1^{k_1} d)}\, a(n/p_1^{k_1} d) \\ &= a(n) - a(n/p_1^{k_1}) + \sum_{\substack{d \in S \\ d \neq 1,\, d \neq p_1^{k_1}}} (-1)^{\omega(d)} (a(n/d) - a(n/p_1^{k_1} d)). \end{aligned}$$

Obviously, $\overline{\mu} \circ a(n) \equiv 0 \pmod{p_1^{k_1}}$ and by the inductive step

$$\sum_{\substack{d \in S \\ d \neq 1,\, d \neq p_1^{k_1}}} (-1)^{\omega(d)} (a(n/d) - a(n/p_1^{k_1} d)) \equiv 0 \pmod{p_1^{k_1}}.$$

It follows that $a(n) - a(n/p_1^{k_1}) \equiv 0 \pmod{p_1^{k_1}}$.

Next, we show that (2) implies (1). We have to show that $\overline{\mu} \circ a(n) \equiv 0 \pmod{n}$. We proceed by induction on $\omega(n)$. If $\omega(n) = 1$, then $n = p^k$ and the result follows by (2). Assume that formula holds for $\omega(n) = r$. We will prove it for $\omega(n) = r + 1$. Let $n = p_1^{k_1} p_2^{k_2} \dots p_{r+1}^{k_{r+1}}$ with different primes p_i and $k_i \geq 1$. We set

$$S_i = \{d : d \| n,\ d \not\equiv 0 \pmod{p_i^{k_i}}\}.$$

We have

$$\overline{\mu} \circ a(n) = a(n) - a(n/p_i^{k_i}) + \sum_{\substack{d \in S_i \\ d \neq 1,\, d \neq p_i^{k_i}}} (-1)^{\omega(d)} (a(n/d) - a(n/p_i^{k_i} d)).$$

By the inductive step

$$\sum_{\substack{d \in S_i \\ d \neq 1,\, d \neq p_i^{k_i}}} (-1)^{\omega(d)} (a(n/d) - a(n/p_i^{k_i} d)) \equiv 0 \pmod{p_i^{k_i}},$$

and $a(n)-a(n/p_i^{k_i}) \equiv 0 \pmod{p_i^{k_i}}$ by (2). We conclude that $\overline{\mu}\circ a(n) \equiv 0 \pmod{p_i^{k_i}}$ for all $i = 1, \ldots, r+1$, and the result follows. □

Corollary 42. *Let $a \in \mathcal{A}(\mathbb{Z})$. The following conditions are equivalent:*

(1) $a \in \mathcal{A}_N(\mathbb{Z}) \cap \mathcal{A}_{UN}(\mathbb{Z})$,

(2) $a(n) \equiv a(n/p) \equiv a(n/p^k) \pmod{p^k}$ *for any* $n \geq 1$ *and all prime* p *with* $p^k \| n$.

In particular, if $a \in \mathcal{A}_N(\mathbb{Z}) \cap \mathcal{A}_{UN}(\mathbb{Z})$, *then*

$$a(p^k) \equiv a(1) \pmod{p^{k+1}},$$

for prime p *and* $k \geq 1$.

Example 43. If $a \in \mathcal{A}(\mathbb{Z})$ is constant, then $a \in \mathcal{A}_N(\mathbb{Z}) \cap \mathcal{A}_{UN}(\mathbb{Z})$.

Example 44. The sequence

$$a_2(n) = \begin{cases} 2^{k+1}, & \text{if } 2^k \| n \text{ for some } k \geq 1 \\ 0, & \text{if } n \equiv 1 \pmod{2}, \end{cases}$$

belongs to $\mathcal{A}_N(\mathbb{Z}) \cap \mathcal{A}_{UN}(\mathbb{Z})$. Indeed, we have

(i) $a_2(n) = a_2(n/p) = a_2(n/p^s) = 0$ if n is odd and $p^s \| n$,

(ii) $a_2(n) = a_2(n/p) = a_2(n/p^s) = 2^{k+1}$ if $n = 2^k m$ $(k \geq 1)$ with m odd and $p^s \| m$,

(iii) for m odd and $k \geq 1$ we have $a_2(2^k m) = 2^{k+1}$, $a_2(2^k m/2^k) = a_2(m) = 0$ and

$$a_2(2^k m/2) = a_2(2^{k-1} m) = \begin{cases} 0, & \text{if } k = 1 \\ 2^k, & \text{if } k > 1. \end{cases}$$

More generally, let p be a fixed prime. Then $a_p \in \mathcal{A}_N(\mathbb{Z}) \cap \mathcal{A}_{UN}(\mathbb{Z})$, where

$$a_p(n) = \begin{cases} p^{k+1}, & \text{if } p^k \| n \text{ for some } k \geq 1 \\ 0, & \text{if } n \not\equiv 0 \pmod{p}. \end{cases}$$

Example 45. We show that the sequence a_2 defined in Example 44 is not a sequence of traces. Let $c \in \mathcal{A}(\mathbb{Z})$ be a sequence of integers generating a_2, i.e.,

$$a_2(n) = c(1)a_2(n-1) + \ldots + c(n-1)a_2(1) + nc(n), \quad n \geq 1.$$

It is sufficient to show that c is infinite, i.e., there is no $l \geq 1$ such that $c(n) = 0$ for $n > l$. We first claim that $c(m) = 0$ for all odd $m \geq 1$. Obviously, we have

$0 = a_2(1) = c(1)$. Assume that $a(s) = 0$ for all odd s less than some odd $m > 1$. Then

$$0 = a_2(m) = c(1)a_2(m-1) + \ldots + c(m-1)a_2(1) + mc(m).$$

Since m is odd, i and $m-i$ have different parity for all $i = 1, \ldots, m-1$. By the inductive step $c(i)a_2(m-i) = 0$. Consequently, $c(m) = 0$. Next, suppose that c is finite, i.e,

$$c = (0, c(2), 0, c(4), \ldots, 0, c(2s), 0, 0, \ldots)$$

for some $s \geq 1$. Then $2s = 2^t m$ for some $t \geq 1$ and odd m. Let $r \geq 1$ be such that $|c(2i)| \leq 2^r$ for $i = 1, \ldots, s$. For all $k > 2s$, we have

$$\begin{aligned} 2^{k+1} &= a_2(2^k) = c(2)a_2(2^k - 2) + \ldots + c(2s)a_2(2^k - 2s) \\ &= c(2)a_2(2(2^{k-1} - 1)) + \ldots + c(2s)a_2(2^t(2^{k-t} - m)) \\ &= c(2)2^2 + \ldots + c(2s)2^{t+1}. \end{aligned}$$

Since

$$\begin{aligned} |a_2(2^k)| &= |c(2)a_2(2^k - 2) + \ldots + c(2s)a_2(2^k - 2s)| \\ &\leq 2^r(2^2 + \ldots + 2^{t+1}) \leq s2^{r+t+1}, \end{aligned}$$

we get a contradiction by taking k sufficiently large.

Problem 46. The following natural questions are worth of consideration:

- describe $\mathcal{A}_N(\mathbb{Z}) \cap \mathcal{A}_{UN}(\mathbb{Z})$,
- characterize the integer matrices $A \in M_l(\mathbb{Z})$ such that $\operatorname{tr}[A] \in \mathcal{A}_N(\mathbb{Z}) \cap \mathcal{A}_{UN}(\mathbb{Z})$ (obviously, $\operatorname{tr}[I] \in \mathcal{A}_N(\mathbb{Z}) \cap \mathcal{A}_{UN}(\mathbb{Z})$),
- characterize the generating sequences $c \in \mathcal{A}(\mathbb{Z})$ for $a \in \mathcal{A}_N(\mathbb{Z}) \cap \mathcal{A}_{UN}(\mathbb{Z})$.

References

[1] S. András, A combinatorial generalizations of Wilson's theorem, *Australas. J. Combin.* **49** (2011), 265-272.

[2] T. M. Apostol, *Introduction to Analytic Number Theory*, Springer-Verlag 1976.

[3] J. Arias de Reyna, Dynamical zeta functions and Krumer congruences, *Acta Arith.* **119** (2005), 39-52.

[4] V. I. Arnold, On the matricial version of Fermat-Euler congruences, *Jpn. J. Math.* **3** (2006), 1-24.

[5] I. K. Babenko, S. A. Bogatyi, The behavior of the index of periodic points under iterations of a mapping, *Math. USSR Izv.* **38** (1992), 1-26.

[6] A. Dold, Fixed point indices of iterated maps, *Invent. Math.* **74** (1983), 419-435.

[7] B.-S. Du, S.-S. Huang, M.-C. Li, Generalized Fermat, Double Fermat and Newton Sequences, *J. Number Theory* **98** (2003), 172-183.

[8] B.-S. Du, S.-S. Huang, M.-C. Li, Newton, Fermat, and exactly realizable sequences, *J. Integer Seq.*, **8** (2005), Article 05.1.2.

[9] F. S. Gillespie, A generalization of Fermat's little theorem, *Fibonacci Quart.* **27** (1989), 109-115.

[10] G. T. Minton, Linear recurrence sequences satisfying congruence conditions, *Proc. Amer. Math. Soc.* **142** (2014), no. 7, 2337-2352.

[11] N. Neumärker, Realizability of integer sequences as differences of fixed point count sequences, *J. Integer Seq.* **12** (2009), Article 09.4.5, 8.

[12] H. Steinlein, Fermat's Little Theorem and Gauss congruence: matrix versions and cyclic permutations, *Amer. Math. Monthly*, **124** (2017), 548-553.

[13] Z.-H.Sun, Linear recursive sequences and powers of matrices, *Fibonacci Quart.* **39** (2001), 339-351.

[14] K. Wójcik, Binomial transform and Dold sequences, *J. Integer Seq.*, **18** (2015), Article 15.1.1.

[15] A. V. Zaruela, On congruences for the traces of powers of some matrices, *Proc. Steklov Inst. Math.*, **263** (2008), 78-98.