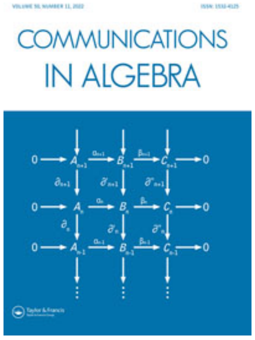

Communications in Algebra

ISSN: (Print) (Online) Journal homepage: https://www.tandfonline.com/loi/lagb20

The ring of polyfunctions over $\mathbb{Z}/n\mathbb{Z}$

Ernst Specker, Norbert Hungerbühler & Micha Wasem

COMMUNICATIONS IN ALGEBRA®
https://doi.org/10.1080/00927872.2022.2092628

The ring of polyfunctions over $\mathbb{Z}/n\mathbb{Z}$

Ernst Specker[a], Norbert Hungerbühler[a], and Micha Wasem[b,c]

[a]Department of Mathematics, ETH Zürich, Zürich, Switzerland; [b]HTA Freiburg, HES-SO University of Applied Sciences and Arts Western Switzerland, Freiburg, Switzerland; [c]UniDistance Suisse, Brig, Switzerland

ABSTRACT

We study the ring of *polyfunctions* over $\mathbb{Z}/n\mathbb{Z}$. The ring of polyfunctions over a commutative ring R with unit element is the ring of functions $f: R \to R$ which admit a polynomial representative $p \in R[x]$ in the sense that $f(x) = p(x)$ for all $x \in R$. This allows to define a ring invariant s which associates to a commutative ring R with unit element a value in $\mathbb{N} \cup \{\infty\}$. The function s generalizes the number theoretic Smarandache function. For the ring $R = \mathbb{Z}/n\mathbb{Z}$ we provide a unique representation of polynomials which vanish as a function. This yields a new formula for the number $\Psi(n)$ of polyfunctions over $\mathbb{Z}/n\mathbb{Z}$. We also investigate algebraic properties of the ring of polyfunctions over $\mathbb{Z}/n\mathbb{Z}$. In particular, we identify the additive subgroup of the ring and the ring structure itself. Moreover we derive formulas for the size of the ring of polyfunctions in several variables over $\mathbb{Z}/n\mathbb{Z}$, and we compute the number of polyfunctions which are units of the ring.

ARTICLE HISTORY
Received 23 July 2021
Revised 25 May 2022
Communicated by Alfred Geroldinger

KEYWORDS
Polynomial functions; ring invariant;
Smarandache function

2020 MATHEMATICS SUBJECT CLASSIFICATION
13M10; 13B25;
13F20; 13M05

1. Introduction

In a finite field F, every function $f: F \to F$ can be represented by a polynomial, i.e., there exists a polynomial $p \in F[x]$ such that $f(x) = p(x)$ for all $x \in F$. Such a polynomial is, e.g., given by the Lagrange interpolation polynomial for f. Among the commutative rings with unit element, the finite fields are actually characterized by this representation property (see [18]):

Theorem 1 (Rédei, Szele). *If R is a commutative ring with unit element then R is a finite field if and only if every function $f: R \to R$ can be represented by a polynomial in $R[x]$.*

If a commutative ring R with unit element is *not* a field, it is natural to ask what can be said about the functions from R to R which *can* be represented by a polynomial in $R[x]$. These functions are called polynomial functions or *polyfunctions* for short. The set of polyfunctions

$$\{f: R \to R \mid \exists p \in R[x] \quad \forall x \in R: p(x) = f(x)\},$$

equipped with pointwise addition and multiplication, is a subring of R^R. This ring of polyfunctions over R will be denoted by $G(R)$. Of particular interest are the polynomials which correspond to the zero element in $G(R)$, they will be called *null-polynomials* (see, e.g., [19]). It is the objective of this article to investigate the algebraic structure and combinatorial properties of the ring of polyfunctions $G(\mathbb{Z}/n\mathbb{Z})$.

CONTACT Norbert Hungerbühler norbert.hungerbuehler@math.ethz.ch Department of Mathematics, ETH Zürich, Rämistrasse 101, 8092 Zürich, Switzerland.
Dedicated to the memory of the first author.

More generally, one can study the ring of multivariate polyfunctions in $d \in \mathbb{N}$ variables—this ring is defined as the set

$$\{f : R^d \to R \mid \exists p \in R[x_1, x_2, ..., x_d] \quad \forall x = (x_1, ..., x_d) \in R^d : p(x) = f(x)\},$$

equipped with pointwise addition and multiplication. We denote this ring by $G_d(R)$ and write $G(R) = G_1(R),$ in accordance with the notation introduced above.

Polyfunctions in one variable over $\mathbb{Z}/n\mathbb{Z}$ were already discussed by Kempner [12, 13], who gave a formula for the number $\Psi(n)$ of polyfunctions over $\mathbb{Z}/n\mathbb{Z},$ which was subsequently simplified by Keller and Olson in [10] (see also the work of Carlitz [4] in the case where n is a power of a prime). Regarding polyfunctions in d variables we refer to Mullen [16] and more recently to [9]: In [9, Theorem 2, p. 5], a characterization theorem is proved which allows to tell whether a given function $f : (\mathbb{Z}/n\mathbb{Z})^d \to \mathbb{Z}/n\mathbb{Z}$ is a polyfunction or not. Furthermore, a formula for the number of polyfunctions $\Psi_d(n)$ in d variables over $\mathbb{Z}/n\mathbb{Z}$ is obtained. In the present work, we provide an alternative formula for $\Psi(n)$ and a new proof of the formula for $\Psi_d(n)$ given in [9].

Polyfunctions from $\mathbb{Z}/n\mathbb{Z}$ to $\mathbb{Z}/m\mathbb{Z}$ have been discussed by Chen [5, 6] and Bhargava [3]. The focus there is to find conditions on the pair (m, n) such that all functions (or certain subclasses) from $\mathbb{Z}/n\mathbb{Z}$ to $\mathbb{Z}/m\mathbb{Z}$ are polyfunctions. These results have been generalized to polynomial functions in the residue class rings of Dedekind domains by Li and Sha in [14]. Dueball in [7] considered polynomials mod p^n with integer coefficients. He showed that the values of such a polynomial $f(x)$ are already determined when x runs through a certain subset of residues. He also provided a formula to generate polynomials which vanish mod p^n for all integral values of x.

To each commutative ring R with unit element, we can associate a number $s(R) \in \mathbb{N} \cup \{\infty\}$ which is defined to be the minimal degree m such that the function $x \mapsto x^m$ can be represented by a polynomial in $R[x]$ of degree strictly smaller than m, i.e.

$$s(R) := \min\{m \in \mathbb{N} \mid \exists p \in R[x], \deg(p) < m, \forall x \in R : p(x) = x^m\} \tag{1}$$

if such an m exists, and $s(R) = \infty$ otherwise.

If $s(R)$ is finite, the monomial $x^{s(R)}$ can be represented by a polynomial p of degree less than $s(R)$. Therefore, the normed polynomial $q(x) = x^{s(R)} - p(x)$ represents the zero-function. Vice versa, if $r(x)$ is a normed null-polynomial of minimal degree m, then $m = s(R)$. Hence, $s(R)$ can be interpreted as the minimal degree of a normed null-polynomial over R.

An alternative and, for reasons that will become clear later, preferable way to view the function defined by (1) is as follows: The building blocks of polynomials are the monomials $x^0, x^1, x^2, ...$ We say, a monomial x^m is *reducible*, if the function $x \mapsto x^m$ can be represented by a polynomial in $R[x]$ of degree strictly smaller than m. Then, $s(R)$ is the number of non-reducible monomials.

The function s is a ring invariant which generalizes the classical number theoretic Smarandache function $s : \mathbb{N} \to \mathbb{N}$,

$$n \mapsto s(n) := \min\{k \in \mathbb{N} : n | k!\}, \tag{2}$$

which is named after the Romanian mathematician Florentin Smarandache, but which has been originally introduced by Lucas in [15] (for prime powers) and Kempner in [11] (for general n). The function s defined in (1) will be called *Smarandache function* because $n \mapsto s(\mathbb{Z}/n\mathbb{Z})$ coincides with the usual Smarandache function $n \mapsto s(n)$ (see Theorem 2). In the context of general commutative rings with unit element, this function will be studied in a forthcoming paper [20]. We also refer to [17], where polyfunctions over general rings are discussed.

The article is organized as follows: Section 2 establishes a unique representation theorem for null-polynomials (Theorem 8). This provides a new formula for the number $\Psi(n)$ of polyfunctions over $\mathbb{Z}/n\mathbb{Z}$ (Corollary 9 and Proposition 11). In Section 3, we investigate algebraic properties of the ring of polyfunctions over $\mathbb{Z}/n\mathbb{Z}$. In particular, we identify the additive subgroup of the ring (Theorem 14) and the ring structure itself (Theorem 18). We also investigate the multiplicative subgroup U_n of units in the ring (Propositions 22 and 27). Section 4 comprises a description of the ring of polyfunctions in several variables over $\mathbb{Z}/n\mathbb{Z}$. In particular, we give a new formula for the size of this ring (Proposition 26).

1.1. Notational conventions

Unless stated otherwise, n will denote a natural number $\geqslant 2$ and $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ is the ring of integers modulo n. We adopt the notation (a, b) for the greatest common divisor of the integer numbers a and b, and we write $a|b$ if b is an integer multiple of a. Furthermore, for $f, g \in \mathbb{Z}_n[x]$ we will write $f \equiv g \mod n$ to mean the equality of polynomials and we will write $f(x) \equiv g(x) \mod n$ if the functions defined by f and g agree.

2. Combinatorial aspects of polyfunctions over $\mathbb{Z}_n$

2.1. The Smarandache function

In this section, we want to determine the minimal degree of a normed null-polynomial in $\mathbb{Z}_n[x]$. We call a polynomial *normed*, if its leading coefficient is 1. The answer is given in the following theorem:

Theorem 2. *$s(\mathbb{Z}_n)$ equals the Smarandache function s(n) defined in (2).*

Remark 3. According to our conventions, $n \geqslant 2$ as the case $n = 1$ should formally be excluded since $\mathbb{Z}_1$ is not a ring with unit element. However, if $n = 1$ we can still make sense of $s(\mathbb{Z}_1)$ if we view $\mathbb{Z}_1$ as $\{0\}$ and it holds that $s(\mathbb{Z}_1) = 0$ but $s(1) = 1$. Kempner originally defined $s(1) = 1$ in [11] but changed it to $s(1) = 0$ later on in [12, 13]. By defining

$$s(n) := \min\{k \in \mathbb{N}_0 : n|k!\},$$

this ambiguity can be avoided (see also [9, p. 7]) and the theorem might be stated for every $1 \leqslant n \in \mathbb{N}$. Another proof of Theorem 2 also appears in [8, Theorem 7, p. 126].

In order to prove Theorem 2 for $n \geqslant 2$, we first show that $s(\mathbb{Z}_n) \leqslant s(n)$. This is established by giving a normed null-polynomial of degree $s(n)$. In fact, we have

$$p(x) := \prod_{i=1}^{s(n)} (x+i) = \binom{x+s(n)}{s(n)} s(n)! \equiv 0 \mod n$$

for all $x \in \mathbb{Z}_n$.

The second step consists in proving the reverse inequality $s(\mathbb{Z}_n) \geqslant s(n)$. This follows easily from the combinatorial identity which connects the binomial and the Stirling numbers of the second kind (see, e.g., [1, 3.39, p. 97] or [8, Lemma 3]): For all $r, j \in \mathbb{N}_0$ there holds

$$\sum_{i=0}^{r} (-1)^{r-i} \binom{r}{i} i^j = r! \left\{ {j \atop r} \right\}$$

(with the convention $0^0 := 1$). In particular, it follows that

$$\sum_{i=0}^{r} (-1)^{i+r} \binom{r}{i} i^k = \delta_{kr} r! \tag{3}$$

for $k \in \{0, 1, ..., r\}$. Now, we consider a null-polynomial p over $\mathbb{Z}_n$, i.e., we assume

$$p(i) = \sum_{k=0}^{r} a_k i^k \equiv 0 \mod n$$

for all $i \in \mathbb{Z}_n$. Then, it follows from (3) that modulo n

$$\begin{aligned} 0 &\equiv \sum_{i=0}^{r}\sum_{k=0}^{r}(-1)^{i+r}\binom{r}{i}a_k i^k \\ &= \sum_{k=0}^{r}a_k\sum_{i=0}^{r}(-1)^{i+r}\binom{r}{i}i^k \\ &= \sum_{k=0}^{r}a_k\delta_{kr}r! = a_r r! \end{aligned}$$

This establishes the desired inequality $s(\mathbb{Z}_n) \geqslant s(n)$ and the proof of Theorem 2 is complete. □

In order to gain more insight in the ideal of null-polynomials in $\mathbb{Z}_n[x]$, we need a stronger version of Theorem 2. First we consider the following simple lemma:

Lemma 4. *Let A and C denote matrices with integer coefficients, y a vector with integer components and $\mathbb{I}$ the identity matrix. If $A^tC \equiv m\mathbb{I} \mod n$, then $Ay \equiv 0 \mod n$ implies $my \equiv 0 \mod n$.*

Proof. Modulo n we have

$$0 \equiv C^tAy = (y^tA^tC)^t \equiv (y^tm\mathbb{I})^t = my.$$ □

Lemma 4 allows to prove the following stronger form of Theorem 2. This will be the technical key to the understanding of the null-polynomials in Section 2.2, the structure of the additive group of the polyfunctions in Section 3.1, and of their ring structure in Section 3.2.

Theorem 5. *If $p(x) = a_0 + a_1x + \cdots + a_rx^r$ vanishes in $\mathbb{Z}_n$ on the set $x \in \{\alpha, \alpha+1, \ldots, \alpha+r\}$ (in particular, if p is a null-polynomial over $\mathbb{Z}_n$), then $a_kr! \equiv 0 \bmod n$ holds for all $k \in \{0, 1, \ldots, r\}$.*

Proof. For $\alpha \in \{0, 1, \ldots, n-1\}$ and $j \in \{\alpha, \alpha+1, \ldots, \alpha+r\}$, we consider the polynomials

$$g_{j,\alpha}(x) := \prod_{\substack{k=\alpha \\ k\neq j}}^{\alpha+r}(x-k) = \sum_{k=0}^{r}g_{j\alpha k}x^k.$$

Obviously, we have $g_{j,\alpha}(i) = 0$ whenever $i \in \{\alpha, \alpha+1, \ldots, \alpha+r\}$ is different from j, and $g_{j,\alpha}(j) = (j-\alpha)!(-1)^{\alpha+r-j}(\alpha+r-j)!$. Hence, we obtain for $i, j \in \{\alpha, \alpha+1, \ldots, \alpha+r\}$

$$(-1)^{\alpha+r-j}\binom{r}{j-\alpha}g_{j,\alpha}(i) = \delta_{ij}r!$$

This identity can be read as $AD = r!\mathbb{I}$ for the matrix $(A)_{ik} = i^k$, $i \in \{\alpha, \alpha+1, \ldots, \alpha+r\}$, $k \in \{0, 1, \ldots, r\}$, and the matrix

$$(D)_{kj} = (-1)^{\alpha+r-j}\binom{r}{j-\alpha}g_{j\alpha k},$$

$k \in \{0, 1, \ldots r\}$, $j \in \{\alpha, \alpha+1, \ldots \alpha+r\}$. Finally, from it follows $A^tC = r!\mathbb{I}$ for $C = D^t$. Thus, the hypotheses of Lemma 4 are fulfilled with $m = r!$.

From the hypothesis of Theorem 5 it follows moreover, that $Ay \equiv 0 \mod n$ for the vector $y = (a_0, a_1, \ldots, a_r)^t$ and hence, the conclusion of Lemma 4 gives the desired result. □

2.2. Decomposition of null-polynomials

In this section we analyze the null-polynomials in $\mathbb{Z}_n[x]$, i.e. the polynomials which vanish as a function from $\mathbb{Z}_n$ to $\mathbb{Z}_n$. In particular we will determine the number of null-polynomials which then allows to compute the number of polyfunctions over $\mathbb{Z}_n$.

We introduce the following notation for $2 \leqslant n \in \mathbb{N}$: $q(n)$ denotes the smallest prime divisor of n, $t(n) := \text{card}\{s((n, \alpha!)) | s((n, \alpha!)) \geqslant q(n), \alpha \in \mathbb{N}\}$ and

$$\{s((n, \alpha!)) | s((n, \alpha!)) \geqslant q(n), \alpha \in \mathbb{N}\} =: \{\beta_1, \beta_2, ..., \beta_{t(n)}\},$$

where the numbers β_k are numbered in descending order, i.e.

$$s(n) = \beta_1 > \beta_2 > \cdots > \beta_{t(n)} = q(n). \tag{4}$$

Here, s continues to denote the number-theoretic Smarandache function. We have

$$\beta_{l+1} = s((n, (\beta_l - 1)!))$$

for $l = 1, ..., t(n) - 1$: To see this, let $\alpha \in \{q(n), q(n) + 1, ..., s(n)\}$ be such that $\beta_l = s((n, \alpha!))$. If $k = (n, \alpha!)$, then $s(k)$ is the smallest number such that $k | s(k)!$. If $\alpha > s(k)$ we might replace α by $s(k)$ and obtain $(n, \alpha!) = (n, s(k)!) = (n, \beta_l!)$. Therefore $\beta_l = s((n, \beta_l!))$ and $\beta_{l+1} = s((n, (\beta_l - 1)!)) < \beta_l$, as claimed.

Furthermore, we define

$$\alpha_k := \frac{n}{(n, \beta_k!)} \tag{5}$$

and consider the *basic null-polynomials* in $\mathbb{Z}_n[x]$:

$$b_k(x) := \alpha_k \prod_{i=1}^{\beta_k} (x + i) \tag{6}$$

Why the null-polynomials are important becomes clear in Theorem 8 below. But first we consider an example and give some computational remarks.

Example 6. The smallest prime divisor of $n = 90$ is $q(90) = 2$, and $s(90) = 6$. In order to compute the degrees β_k according to (4), notice that we only need to consider values $\alpha \in \{q(n), q(n) + 1, ..., s(n)\}$. For these values, we have

α	$(90, \alpha!)$	$s((90, \alpha!))$
2	2	2
3	6	3
4	6	3
5	30	5
6	90	6

From this table, we read off $t(90) = 4$ and

$$\beta_1 = 6, \quad \beta_2 = 5, \quad \beta_3 = 3, \quad \beta_4 = 2.$$

The coefficients α_k are now computed by (5):

$$\alpha_1 = 1, \quad \alpha_2 = 3, \quad \alpha_3 = 15, \quad \alpha_4 = 45.$$

The basic null-polynomials for $n = 90$ are therefore

$$\begin{aligned} b_1(x) &= (1 + x)(2 + x)(3 + x)(4 + x)(5 + x)(6 + x) \\ b_2(x) &= 3(1 + x)(2 + x)(3 + x)(4 + x)(5 + x) \\ b_3(x) &= 15(1 + x)(2 + x)(3 + x) \\ b_4(x) &= 45(1 + x)(2 + x) \end{aligned}$$

□

Remark 7. It is useful to note, that by construction we have

$$(n, (k+1)!) = (n, \beta_j!)$$

for all $k+1 \in \{\beta_j, \beta_j + 1, ..., \beta_{j-1} - 1\}$.

Note that Kempner [12, 13] also introduces basic null-polynomials of the form

$$\tilde{b}(x) = \frac{n}{d} \prod_{i=0}^{s(d)-1} (x-i)$$

where $d > 1$ is a divisor of n. If $d > 1$ runs through all divisors of n in decreasing order, we only list polynomials which are not multiples of polynomials that already appeared. In the present case, when $n = 90$, one obtains in this way the basic null-polynomials

$$\begin{aligned}
\tilde{b}_1(x) \quad &= x(x-1)(x-2)(x-3)(x-4)(x-5) \\
\tilde{b}_2(x) \quad &= 3x(x-1)(x-2)(x-3)(x-4) \\
\tilde{b}_3(x) \quad &= 15x(x-1)(x-2) \\
\tilde{b}_4(x) \quad &= 45x(x-1)
\end{aligned}$$

The difference stems from the fact, that we introduced a normed null-polynomial of minimal degree by defining

$$p(x) = \prod_{i=1}^{s(n)} (x+i),$$

whereas Kempner uses

$$\tilde{p}(x) = \prod_{i=0}^{s(n)-1} (x-i).$$

Notice that the basic null-polynomial $b_{t(n)}$ is a non-zero polynomial of minimal degree $q(n)$ (see, e.g., [8, Theorem 8]). This fact is used in the following decomposition theorem. With the notations above we have:

Theorem 8. *Every null-polynomial p in $\mathbb{Z}_n[x]$ has a unique decomposition of the form*

$$p(x) = \sum_{k=1}^{t(n)} q_k(x) b_k(x),$$

where $q_k \in \mathbb{Z}_{n/\alpha_k}[x]$ has degree strictly less than $\beta_{k-1} - \beta_k$ if $k > 1$ and where $\deg(q_1) = \deg(p) - \beta_1$.

Proof. We start by proving the existence of a decomposition of the desired type.

In a first step, we can write

$$p(x) = q_1(x) b_1(x) + p_1(x)$$

with $q_1 \in \mathbb{Z}_n[x]$, $\deg(q_1) = \deg(p) - \beta_1$, and $\deg(p_1) < \beta_1$, by dividing the polynomials with remainder (observe that b_1 is normed).

Now, we assume by induction that the decomposition has the form

$$p(x) = \sum_{k=1}^{l} q_k(x) b_k(x) + p_l(x)$$

with $\deg(p_l) < \beta_l$. Then, the next step is carried out as follows: p_l is a null-polynomial in $\mathbb{Z}_n[x]$ of the form

$$p_l(x) = a_0 + a_1x + \cdots + a_{\beta_l-1}x^{\beta_l-1}.$$

Hence, by Theorem 5, it follows that

$$a_i(\beta_l - 1)! \equiv 0 \mod n$$

for all $i \in \{0, 1, ..., \beta_l - 1\}$. Since $\beta_{l+1} = s((n, (\beta_l - 1)!)) < \beta_l$, this implies

$$\alpha_{l+1} \mid a_i$$

for all $i \in \{0, 1, ..., \beta_l - 1\}$. Hence, we can divide the polynomial p_l by b_{l+1} with remainder and obtain

$$p_l(x) = q_{l+1}(x)b_{l+1}(x) + p_{l+1}(x)$$

with $\deg(p_{l+1}) < \beta_{l+1}$, $\deg(q_{l+1}) < \beta_l - \beta_{l+1}$ and $q_{l+1} \in \mathbb{Z}_{n/\alpha_{l+1}}[x]$. This iterative process ends as soon as $\deg(p_{l+1}) < q(n)$, since then, it follows that $p_{l+1} \equiv 0 \mod n$ by [8, Theorem 8].

Now, we assume by contradiction that there exist two different decompositions of p, say

$$0 \equiv \sum_{k=1}^{t(n)} b_k(q_k - \tilde{q}_k) \mod n \tag{7}$$

with a smallest index k_0 with $q_{k_0} \neq \tilde{q}_{k_0}$. Let i denote the highest power i in q_{k_0} and $\tilde{q}_{k_0}$ with different coefficients $a_i \neq \tilde{a}_i$ in $\mathbb{Z}_{n/\alpha_{k_0}}$. Then, according to the construction of the basic null-polynomials b_k, the coefficient of the highest power of x on the right-hand side of (7) is $\alpha_{k_0}(a_i - \tilde{a}_i)$. By (7), we have

$$\alpha_{k_0} \underbrace{(a_i - \tilde{a}_i)}_{\in \mathbb{Z}_{n/\alpha_{k_0}}} \equiv 0 \mod n$$

which implies that $a_i \equiv \tilde{a}_i \mod (n/\alpha_{k_0})$, and this is a contradiction. □

2.3. The number of polyfunctions

The result of the previous section allows now to compute the cardinality of the ring $G(\mathbb{Z}_n)$.

Corollary 9. *The number $\Psi(n)$ of polyfunctions over $\mathbb{Z}_n$ is given by*

$$\Psi(n) = \prod_{k=1}^{t(n)} (n, \beta_k!)^{\beta_k - \beta_{k-1}}$$

with the convention $\beta_0 := 0$.

Proof. We consider the additive group $F(n)$ of polynomials in $\mathbb{Z}_n[x]$ of degree strictly less than $s(n)$ and the normal subgroup $N(n)$ of all null-polynomials in $F(n)$. The additive group of polyfunctions over $\mathbb{Z}_n$ is then isomorphic to the quotient $F(n)/N(n)$. All cosets have the cardinality of the set of null-polynomials of degree strictly less than $s(n)$, namely, according to Theorem 8,

$$|N(n)| = \prod_{i=2}^{t(n)} \left(\frac{n}{\alpha_i}\right)^{\beta_{i-1} - \beta_i}.$$

On the other hand, the number of polynomials of degree strictly less than $s(n)$ is $|F(n)| = n^{\beta_1}$. Division $|F(n)|/|N(n)|$ gives the claimed formula. □

Example 10. Let us come back to Example 6 with $n = 90$: The formula in Corollary 9 gives $\Psi(90) = (90, 6!)^6 (90, 5!)^{-1} (90, 3!)^{-2} (90, 2!)^{-1} = 246037500$ for the number of polyfunctions over $\mathbb{Z}_{90}$. □

In the case when n equals the power of a prime number the formula for Ψ takes a particularly simple form. Since Ψ will be shown to be multiplicative, it is actually enough to know the values of $\Psi(p^m)$ for p prime (see Section 2.3.1).

2.3.1. The case $n = p^m$, p prime

At this point it is useful to include a general remark on rings of polyfunctions: If R and S are commutative rings with unit element, then $G(R \oplus S)$ and $G(R) \oplus G(S)$ are isomorphic as rings in the obvious way. In particular, since $\mathbb{Z}_n \oplus \mathbb{Z}_m \cong \mathbb{Z}_{nm}$ if m and n are relatively prime, we have that

$$G(\mathbb{Z}_{nm}) \cong G(\mathbb{Z}_n) \oplus G(\mathbb{Z}_m)$$

if $(m, n) = 1$. Therefore, we may confine ourselves to the case $n = p^m$, p prime, without loss of generality.

This observation gives rise to the following version of Corollary 9, see also [10].

Proposition 11. *Let $\Psi(n)$ denote the number of polyfunctions over $\mathbb{Z}_n$ and s the Smarandache function. Then,*

(i) *the function Ψ is multiplicative, i.e. if $(m, n) = 1$ then $\Psi(mn) = \Psi(m)\Psi(n)$, and*
(ii) *for a prime number p and $m \in \mathbb{N}$ there holds*

$$\Psi(p^m) = \exp_p\left(\sum_{k=1}^{m} s(p^k)\right),$$

where we write $\exp_p a := p^a$ for typographical reasons.

Example 12. Before we prove Proposition 11, we come back to Example 10, where $n = 90$. By (i) in Proposition 11, we have

$$\Psi(90) = \Psi(2)\Psi(3^2)\Psi(5)$$

and the factors are by (ii) $\Psi(2) = 2^2$, $\Psi(3^2) = 3^{3+6}$ and $\Psi(5) = 5^5$. The product of these numbers is $\Psi(90) = 4 \cdot 19683 \cdot 3125 = 246037500$ in accordance with the calculation in Example 10.

At this point, it is useful to introduce one more quantity which will play a role in the proof of Proposition 11 and which is going to be used in the description of the algebraic structure of the ring of polyfunctions over $\mathbb{Z}_n$ (see Section 3.2). For prime numbers p and integers $k \geqslant 0$, we define

$$e_p(k) := \max\{x \in \mathbb{N}_0 \ : \ p^x | k!\}.$$

Notice that $e_p(k) = j$ for $jp \leqslant k < (j+1)p$ if $k < p^2$. But the next number is $e_p(p^2) = p + 1$.

Proof of Proposition 11.
(i) The multiplicativity follows immediately from the remark preceding the proposition.
(ii) The basic null-polynomials of degree strictly less than $s(p^m)$ are in this case (see (6)) given by

$$b_k(x) = p^{m - e_p(k)} \prod_{i=1}^{k} (x - i)$$

for $k = p, 2p, 3p, \dots, s(p^m) - p$. Thus the number of null-polynomials in $\mathbb{Z}_{p^m}[x]$ of degree strictly less than $s(p^m)$ is

$$\prod_{k=1}^{\frac{s(p^m)}{p}-1} p^{pe_p(pk)},$$

and the total number of polynomials in $\mathbb{Z}_{p^m}[x]$ of degree strictly less than $s(p^m)$ is

$$p^{ms(p^m)}.$$

Division of both numbers yields the number of polyfunctions over $\mathbb{Z}_{p^m}$, namely

$$\Psi(p^m) = \exp_p\left(p\sum_{k=0}^{\frac{s(p^m)}{p}-1}(m - e_p(pk))\right).$$

Hence, the claim is proved if we verify that for all $m \in \mathbb{N}$ there holds

$$p\sum_{k=0}^{\frac{s(p^m)}{p}-1}(m - e_p(pk)) = \sum_{k=1}^{m} s(p^k). \tag{8}$$

Obviously, (8) is true for $m=1$. Moreover $s(p^{m+1}) - s(p^m)$ is either 0 or p. Using this, it is easy to see, that (8) holds for $m+1$ if it is correct for m, and the claim follows by induction. □

Remark 13.

(i) The formula in (ii) above is particularly simple in the case $m \leqslant p$: We observe that $s(p^k) = kp$ for $k \leqslant p$. Thus

$$\sum_{k=1}^{m} s(p^k) = p\binom{m+1}{2} \text{ and } \Psi(p^m) = \exp_p\left(p\binom{m+1}{2}\right)$$

for $m \leqslant p$.

(ii) While the present approach for counting the number of polyfunctions in $\mathbb{Z}_n$ consists in finding a unique representative for each null-polynomial, in [9, Theorem 5, p. 8], each polyfunction is shown to have a unique representative. An alternative proof of Theorem 11 is then given in [9, Theorem 6, p. 9] by counting these representatives. Moreover, a very short formula for $\Psi(n)$ is given in [9, Theorem 9, p. 10] in terms of the Smarandache function, the Mangoldt function, and the Dirichlet convolution.

(iii) Not only the formula for $\Psi(n)$ looks particularly pleasant for $n = p^m$, also the decomposition of the additive group $F(n)$ takes its simplest form for powers of prime numbers. As mentioned earlier in this section, it is sufficient to know the structure of $F(n)$ for $n = p^m$. In this case, the decomposition in Theorem 14 simplifies to

$$F(p^m) \cong p\bigoplus_{k=0}^{s(p^m)/p-1} \mathbb{Z}_{p^{m-e_p(pk)}}.$$

Here and throughout Section 3, we will use the notation

$$nG = \bigoplus_{i=1}^{n} G$$

for the n-fold direct product of a group G with itself, where $n \in \mathbb{N}$.

3. Algebraic properties of the ring of polyfunctions

3.1. The additive group of polyfunctions

Let $F(n)$ denote the additive group of polyfunctions over $\mathbb{Z}_n$ and $F_k(n)$ the subgroup of polyfunctions which have a representative of degree less than or equal to k. Using the notation of Section 2.2, we have the following result:

Theorem 14. *The group $F(n)$ is isomorphic to*

$$\bigoplus_{j=1}^{t(n)} (\beta_j - \beta_{j+1})\mathbb{Z}_{\alpha_{j+1}}$$

with the convention $\beta_{t(n)+1} := 0$ and $\alpha_{t(n)+1} := n$.

We prepare the proof by the following lemma:

Lemma 15. *Let $\beta_j \leqslant k+1 < \beta_{j-1}$, $k \geqslant 0$, $2 \leqslant j \leqslant t(n)+1$. Then there holds:*

(i) *Every element in the quotient $F(n)/F_k(n)$ has order less than or equal to α_j.*
(ii) *The polyfunction represented by x^{k+1} has the order α_j in $F(n)/F_k(n)$.*

Proof of the Lemma.

(i) We have, that in $F(n)/F_k(n)$

$$\alpha_j x^{k+1} = \alpha_j x^{\beta_j} x^{k+1-\beta_j} = \underbrace{b_j(x)}_{=0 \text{ for all } x \in \mathbb{Z}_n} x^{k+1-\beta_j} = 0$$

since $\beta_j \leqslant k+1$. Here, b_j is a basic null-polynomial (see Section 2.2). Now, every $f \in F(n)/F_k(n)$ contains x^{k+1} as a factor and hence $\text{ord}(f) \leqslant \alpha_j$.

(ii) Suppose $\alpha x^{k+1} = 0$ in $F(n)/F_k(n)$ for some α in $\mathbb{Z}_n$. Then, by Theorem 5, $\alpha(k+1)! \equiv 0 \mod n$. Hence, α is a multiple of

$$\frac{n}{(n,(k+1)!)} > \frac{n}{(n,\beta_{j-1}!)} = \alpha_{j-1}$$

since $k+1 < \beta_{j-1}$. Thus we have

$$\frac{n}{(n,(k+1)!)} \geqslant \alpha_j$$

(see Remark 7) and hence $\alpha \notin \{1,2,\ldots,\alpha_j - 1\}$. □

Now, Theorem 14 follows from Lemma 15 by iteration: First, we observe that $1 \in F(n)$ has the (maximal) order $n = \alpha_{t(n)+1}$. Thus

$$F(n) \cong \mathbb{Z}_n \oplus F(n)/F_0(n)$$

since finite Abelian groups split off a maximal cyclic subgroup. Now, we proceed iteratively and split in each step

$$F(n)/F_k(n) \cong \mathbb{Z}_{\alpha_j} \oplus F(n)/F_{k+1}(n)$$

by using Lemma 15. The process stops as soon as $k+1 = s(n)$, and by collecting the quotients we obtain the claimed decomposition. □

Example 16. We revisit Examples 6, 10, and 12 respectively in order to compute the decomposition of $F(90)$. With the notational conventions of Theorem 14 we have:

j	1	2	3	4	5
α_j	1	3	15	45	90
β_j	6	5	3	2	0

In a first step, we decompose

$$F(90) \cong \mathbb{Z}_{90} \oplus F(90)/F_0(90).$$

If $k=0$, we have $\beta_5 < k+1 < \beta_4$ and hence $F(90)/F_0(90)$ splits off a cyclic subgroup of order $\alpha_5 = 90$ and hence $F(90)/F_0(90) \cong \mathbb{Z}_{90} \oplus F(90)/F_1(90)$.

If $k=1$, we have $\beta_4 \leqslant k+1 < \beta_3$ and hence $F(90)/F_1(90)$ splits off a cyclic subgroup of order α_4 and hence $F(90)/F_1(90) \cong \mathbb{Z}_{45} \oplus F(90)/F_2(90)$.

If $k=2,\ 3$, we have $\beta_3 \leqslant k+1 < \beta_2$ so we might split off twice the subgroup $\mathbb{Z}_{15}$ and hence $F(90)/F_2(90) \cong \mathbb{Z}_{15} \oplus \mathbb{Z}_{15} \oplus F(90)/F_4(90)$.

Finally, if $k=4$, it holds that $\beta_2 \leqslant k+1 < \beta_1$ and we find $F(90)/F_4(90) \cong \mathbb{Z}_3$ and the process ends. This leads to the desired decomposition

$$F(90) \cong \mathbb{Z}_3 \oplus 2\mathbb{Z}_{15} \oplus \mathbb{Z}_{45} \oplus 2\mathbb{Z}_{90}$$

and we find again $|F(90)| = 3 \cdot 15^2 \cdot 45 \cdot 90^2 = 246037500$ in accordance with Examples 10 and 12.

Remark 17. Since it turns out that it is sufficient to know the structure of $F(p^m)$ for prime numbers p (see Section 2.3.1), observe that in this case, the decomposition described in Theorem 14 takes a particularly simple form (see Remark 13, item (iii)).

3.2. The ring of polyfunctions

In this section, we use the shorthand notation $G(n)$ for $G(\mathbb{Z}_n)$, i.e. the ring of polyfunctions over $\mathbb{Z}_n$. We recall that $G(mn) \cong G(m) \oplus G(n)$ if $(m,n)=1$, and hence we may restrict ourselves to investigate the structure of $G(n)$ in the case $n = p^m$ for p prime. Let $I_{p,m}$ be the ideal of polynomials in $\mathbb{Z}_{p^m}[x]$ defined by

$$I_{p,m} = \{f \in \mathbb{Z}_{p^m}[x] \ : \ f(kp) = 0 \text{ for all } k\}.$$

Then, we have the following decomposition:

Theorem 18.
(i) $G(p^m) \cong p\ \mathbb{Z}_{p^m}[x]/I_{p,m}$.
(ii) $\mathbb{Z}_{p^m}[x]/I_{p,m}$ *is not decomposable.*

Proof. We proceed in several steps:
Step 1: For $j \in \{0, 1, \dots, p-1\}$ let

$$R_j(p^m) := \{f \in G(p^m) \ : \ f(k) = 0 \ \text{if} \ k \not\equiv j \mod p\}.$$

It is clear that $R_j(p^m)$ is an ideal of $G(p^m)$ and that $R_i(p^m) \cap R_j(p^m) = \{0\}$ if $i \neq j$.

Step 2: We show that $G(p^m) \cong \bigoplus_{j=0}^{p-1} R_j(p^m)$.

To see this, we define

$$\varepsilon_0(x) := 1 - x^{m\varphi(p^m)},$$

where φ denotes Euler's φ-function. Then we have

$$\varepsilon_0(k) \equiv \begin{cases} 0 & \text{if } k \not\equiv 0 \mod p \\ 1 & \text{if } k \equiv 0 \mod p \end{cases} \mod p^m.$$

Moreover, for $\varepsilon_j(x) := \varepsilon_0(x-j),$ we have similarly

$$\varepsilon_j(k) \equiv \begin{cases} 0 & \text{if } k \not\equiv j \mod p \\ 1 & \text{if } k \equiv j \mod p \end{cases} \mod p^m.$$

Hence, for $f \in G(p^m),$ we have $f\varepsilon_j \in R_j(p^m)$ and

$$f = \sum_{j=0}^{p-1} f\varepsilon_j.$$

Then,

$$\Phi_0 : G(p^m) \to \bigoplus_{j=0}^{p-1} R_j(p^m), f \mapsto (f\varepsilon_0, f\varepsilon_1, \ldots, f\varepsilon_{p-1})$$

is a ring isomorphism (the ring operations $+$ and $\cdot$ are, as usual, defined componentwise).
Step 3: We show that $R_j(p^m) \cong R_0(p^m)$ for $j \in \{0, 1, \ldots, p-1\}.$

The map

$$\Phi_1 : R_0(p^m) \to R_j(p^m), f \mapsto g,$$

where $g(x) := f(x-j)$, $x \in \mathbb{Z}_{p^m}$ is a ring isomorphism. Hence, according to the second step, we have that

$$G(p^m) \cong pR_0(p^m).$$

Step 4: We show that $R_0(p^m) \cong \mathbb{Z}_{p^m}[x]/I_{p,m}.$

To see this, we consider the map

$$\Phi_2 : \mathbb{Z}_{p^m}[x] \to R_0(p^m), f \mapsto f\varepsilon_0.$$

Φ_2 is a surjective ring homomorphism. If $f \in \ker(\Phi_2),$ then $\Phi_2(f)(k) = 0$ for all $k \in \mathbb{Z}_{p^m}$ and hence $f(jp)\varepsilon_0(jp) = f(jp) = 0$ for all j. This implies that $f \in I_{p,m}$. Arguing in the opposite direction, we conclude that $f \in I_{p,m}$ implies that $f \in \ker(\Phi_2)$.

Now, (i) follows from the third and the fourth step and it remains to prove (ii). This is done in the last step:
Step 5: We show, that $R_0(p^m)$ is not decomposable:

Let $f \in R_0(p^m)$ be such that $f^2 = f$. In particular, this means $f^2(jp) = f(jp)$ for all j. Hence, $f(jp) \in \{0, 1\}$ for all j. Observe, that

$$f(jp) \equiv f(0) \mod p$$

and hence

$$f(k) = 0 \qquad \text{for all } k \in \mathbb{Z}_{p^m}$$

or

$$f(k) = \begin{cases} 0 & \text{if } k \not\equiv 0 \mod p, \\ 1 & \text{if } k \equiv 0 \mod p. \end{cases}$$

It follows that only two elements $f \in R_0(p^m)$ with the property $f^2 = f$ exist. In a decomposable ring there are at least four elements with $f^2 = f$. This completes the proof. □

We now want to investigate the structure of the ideal $I_{p,m}$ in more detail. First, for $m \in \mathbb{N}$ and a prime number p, we define

$$s^*(p^m) := \min\{x \in \mathbb{N} \;:\; p^m | p^x x!\}.$$

Then, for $r \in \{1, 2, \dots, s^*(p^m) - 1\}$ let

$$e^*(r) := \max\{x \in \mathbb{N} \;:\; p^x | p^r r!\}$$

and

$$e^*(s^*(p^m)) := m.$$

Remark 19. s^* is connected with the Smarandache function by

$$p\ s^*(p^m) = s(p^m).$$

Let us assume, that $f \in I_{p,m}$:

$$f(x) = a_1 x + a_2 x^2 + \cdots + a_r x^r.$$

Then, $f(jp) \equiv 0 \mod p^m$ for all j and hence, the polynomial

$$g(x) := a_1 p x + a_2 p^2 x^2 + \cdots + a_r p^r x^r$$

is a null-polynomial over $\mathbb{Z}_{p^m}$. Hence, it follows from Theorem 5 that

$$a_k p^k r! \equiv 0 \mod p^m$$

for all $k \in \{1, 2, \dots, r\}$. From, this congruence, we immediately obtain the following conclusion.

Proposition 20.

(i) *If $f \in I_{p,m}$ is normed, then* $\deg(f) \geqslant s^*(p^m)$.

(ii) *If $f \in I_{p,m}$, $f(x) = a_1 x + a_2 x^2 + \cdots + a_r x^r$, with $r \leqslant s^*(p^m)$, then*

$$p^{m - e^*(r) + r - k} | a_k$$

holds for all $k \in \{1, 2, \dots, r\}$.

Now, the polynomials in $I_{p,m}$ can be decomposed similarly as the null-polynomials (see Section 2.2 and (6)). The basic polynomials are in this case

$$b_k^*(x) := p^{m - e^*(k)} \prod_{j=1}^{k} (x + jp)$$

for $k \in \{1, 2, \dots, s^*(p^m)\}$. In fact, we have:

Lemma 21. $b_k^* \in I_{p,m}$ *for all* $k \in \{1, 2, \dots, s^*(p^m)\}$.

Proof. We have

$$\begin{aligned} b_k^*(ip) &= p^{m - e^*(k)} \prod_{j=1}^{k} (ip + jp) \\ &= p^{m - e^*(k)} p^k \binom{i+k}{k} k! \end{aligned} \tag{9}$$

The right-hand side of (9) is congruent 0 modulo p^m for all j as is easily seen by treating separately the cases $k < s^*(p^m)$ and $k = s^*(p^m)$. □

3.3. The units in $G(\mathbb{Z}_n)$

The previous results on the algebraic structure of the ring of polyfunctions over $\mathbb{Z}_n$ allow now to answer more specific questions. As an example, we consider the multiplicative subgroup U_n of units in $G(\mathbb{Z}_n)$ and ask for the size of U_{3^k}.

For this, we consider the set Q of polynomials in $\mathbb{Z}_{3^k}[x]$ with degree strictly less than $s(3^k) =: r+1$. A polynomial $q \in Q$, $q(x) = a_0 + a_1x + a_2x^2 + \cdots + a_rx^r$ with $a_i \in \mathbb{Z}_{3^k}$, represents according to [9, Proposition 3, p. 5] an invertible polyfunction (i.e. a unit in $G(\mathbb{Z}_{3^k})$) if and only if its image is contained in the multiplicative subgroup of units in $\mathbb{Z}_{3^k}$, that is

$$q(i) \not\equiv 0 \mod 3 \quad \text{for } i = 0, 1, 2. \tag{10}$$

(Observe that $q(x+3j) \equiv q(x) \mod 3$ for all integers x and j.) Let

$$\Sigma_1 := \sum_{\substack{i=1 \\ i \text{ odd}}}^{r} a_i$$

and

$$\Sigma_2 := \sum_{\substack{i=2 \\ i \text{ even}}}^{r} a_i.$$

Then, we can rewrite (10) in the form

$$\left.\begin{array}{lcll} a_0 & \not\equiv & 0 & \mod 3 \\ a_0 + \Sigma_1 + \Sigma_2 & \not\equiv & 0 & \mod 3 \\ a_0 + \Sigma_1 + 2\Sigma_2 & \not\equiv & 0 & \mod 3 \end{array}\right\} \tag{11}$$

It is then easy to determine the total number X of solutions $(a_0, a_1, \ldots, a_r) \in \mathbb{Z}_{3^k}^{r+1}$ of (11):

$$X = 8 \cdot 3^{k(r+1)-3}.$$

Now, two polynomials in Q represent the same unit in $G(\mathbb{Z}_{3^k})$ if and only if their difference is a null-polynomial of degree strictly less than $s(3^k)$. The number Y of such null-polynomials is according to Proposition 11 given by

$$Y = \frac{3^{ks(3^k)}}{\Psi(3^k)}.$$

Division of X by Y yields the following result:

Proposition 22.

$$|U_{3^k}| = \left(\frac{2}{3}\right)^3 \Psi(3^k) = \left(\frac{2}{3}\right)^3 \exp_3\left(\sum_{i=1}^{k} s(3^i)\right).$$

In other words, the fraction of units among all polyfunctions in $G(\mathbb{Z}_{3^k})$ is $\frac{8}{27}$, independently of k.

Proposition 22 gives a flavor of a more general result: In Section 4.2, we will determine the number of units in the ring $G_d(\mathbb{Z}_{p^m})$ of multivariate polyfunctions.

4. Polyfunctions in several variables

In order to keep the formulas short, we use the following multi-index notation: For $\boldsymbol{k} = (k_1, k_2, \ldots, k_d) \in \mathbb{N}_0^d$ and $\boldsymbol{x} := (x_1, x_2, \ldots, x_d) \in \mathbb{N}_0^d$ let

$$\boldsymbol{x}^{\boldsymbol{k}} := \prod_{i=1}^{d} x_i^{k_i}, \quad \boldsymbol{k}! := \prod_{i=1}^{d} k_i!, \quad |\boldsymbol{k}| := \sum_{i=1}^{d} k_i, \quad \text{and} \quad \binom{\boldsymbol{x}}{\boldsymbol{k}} := \prod_{i=1}^{d} \binom{x_i}{k_i}.$$

Recall that

$$G_d(R) = \{f : R^d \to R \mid \exists p \in R[x_1, x_2, ..., x_d] \quad \forall x \in R^j \Rightarrow p(x) = f(x)\},$$

equipped with pointwise addition and multiplication denotes the ring of polyfunctions in d variables, whenever R is a commutative ring with unit element.

An alternative (but equivalent) construction is to define $G_d(R)$ recursively as the ring of polyfunctions in one variable from R to $G_{d-1}(R)$ by

$$G_d(R) = \{f : R \to G_{d-1}(R) \mid \exists p \in G_{d-1}(R)[x] \quad \forall x \in R \Rightarrow p(x) = f(x)\}.$$

4.1. The number of multivariate polyfunctions on $\mathbb{Z}_n$

We recall a few facts and definitions from [9] in order to count the number of polyfunctions on $\mathbb{Z}_n$ in d variables, and again it is enough to find a formula for $n = p^m$ since we have the natural decomposition $G_d(\mathbb{Z}_{ab}) \cong G_d(\mathbb{Z}_a) \oplus G_d(\mathbb{Z}_b)$ if $(a, b) = 1$. We define the set

$$S_d(n) := \{\boldsymbol{k} \in \mathbb{N}_0^d : n \nmid \boldsymbol{k}!\} \tag{12}$$

and let $s_d(n) := |S_d(n)|$ be the generalization of the Smarandache function introduced in [9]. As for the case of one variable we define

$$e_p(\boldsymbol{k}) := \max\{x \in \mathbb{N}_0 \quad : \quad p^x | \boldsymbol{k}!\}.$$

Definition 23. Let a be an element of $\mathbb{Z}_n$. We say, the polynomial $a\boldsymbol{x}^{\boldsymbol{k}} \in \mathbb{Z}_n[\boldsymbol{x}]$ is reducible (modulo n) if a polynomial $p(\boldsymbol{x}) \in \mathbb{Z}_n[\boldsymbol{x}]$ exists with $\deg(p) < |\boldsymbol{k}|$ such that $a\boldsymbol{x}^{\boldsymbol{k}} \equiv p(\boldsymbol{x}) \mod n$ for all $\boldsymbol{x} \in \mathbb{Z}_n^d$. Moreover, we say that $a\boldsymbol{x}^{\boldsymbol{k}}$ is weakly reducible if $a\boldsymbol{x}^{\boldsymbol{k}} \equiv p(\boldsymbol{x}) \mod n$ for all $\boldsymbol{x} \in \mathbb{Z}_n^d$, where $p \in \mathbb{Z}_n[\boldsymbol{x}]$ is such that $\deg(p) \leqslant |\boldsymbol{k}|$ (instead of $\deg(p) < |\boldsymbol{k}|$) and such that $\boldsymbol{x}^{\boldsymbol{k}}$ (or a multiple of it) does not appear as a monomial in p.

We will need the following lemma (see also [9, Lemma 4, p. 6]) which characterizes tuples $\boldsymbol{k}$ for which $a\boldsymbol{x}^{\boldsymbol{k}}$ is (weakly) reducible in $\mathbb{Z}_n[\boldsymbol{x}]$.

Lemma 24.
(i) *If $a\boldsymbol{x}^{\boldsymbol{k}}$ is weakly reducible modulo n, then $n | a\boldsymbol{k}!$.*
(ii) *If $n | a\boldsymbol{k}!$, then $a\boldsymbol{x}^{\boldsymbol{k}}$ is reducible modulo n.*

Proof.
(i) We assume, that $p(\boldsymbol{x})$ reduces $a\boldsymbol{x}^{\boldsymbol{k}}$ weakly. Hence, $q(\boldsymbol{x}) := a\boldsymbol{x}^{\boldsymbol{k}} - p(\boldsymbol{x})$ is a null-polynomial in d variables over $\mathbb{Z}_n$. Let us define the following "integral" for functions $f : \mathbb{Z}_n \to \mathbb{Z}_n$:

$$\int_0^m f(x) d\mu(x) := \sum_{j=0}^{m} (-1)^{m-j} \binom{m}{j} f(j).$$

Now, we write q in the form

$$q(\boldsymbol{x}) = \sum_{\substack{\boldsymbol{l} \in \mathbb{N}_0^d \\ |\boldsymbol{l}| \leqslant |\boldsymbol{k}|}} q_{\boldsymbol{l}} \boldsymbol{x}^{\boldsymbol{l}}$$

for suitable coefficients $q_{\boldsymbol{l}} \in \mathbb{Z}_n$, with $q_{\boldsymbol{k}} = a$. Then, modulo n, we have

$$0 = \int_0^{k_d} \int_0^{k_{d-1}} \dots \int_0^{k_1} q(\boldsymbol{x}) d\mu(x_1)\dots d\mu(x_{d-1}) d\mu(x_d) =$$
$$= \sum_{\substack{\boldsymbol{l} \in \mathbb{N}_0^d \\ |\boldsymbol{l}| \leqslant |\boldsymbol{k}|}} q_{\boldsymbol{l}} \int_0^{k_d} \int_0^{k_{d-1}} \dots \int_0^{k_1} \boldsymbol{x}^{\boldsymbol{l}} d\mu(x_1)\dots d\mu(x_{d-1}) d\mu(x_d).$$

Observe that the only term which does not vanish in the above sum is

$$q_{\boldsymbol{k}} \int_0^{k_d} \int_0^{k_{d-1}} \dots \int_0^{k_1} \boldsymbol{x}^{\boldsymbol{k}} d\mu(x_1)\dots d\mu(x_{d-1}) d\mu(x_d) = a\boldsymbol{k}!.$$

In fact all other terms vanish by (3), since $|\boldsymbol{l}| \leqslant |\boldsymbol{k}|$ and $\boldsymbol{l} \neq \boldsymbol{k}$ implies that for some $i \in \{0, 1, \dots, d\}$ we have $l_i < k_i$ and therefore the integral with respect to x_i gives zero. This completes the proof of (i).

(ii) We assume, that $n | a\boldsymbol{k}!$. Then, the polynomial

$$q(\boldsymbol{x}) := a \prod_{i=1}^{d} \prod_{l=1}^{k_i} (x_i + l) = a\boldsymbol{k}! \prod_{i=1}^{d} \binom{x_i + k_i}{k_i} = a\boldsymbol{k}! \binom{\boldsymbol{x} + \boldsymbol{k}}{\boldsymbol{k}}$$

is a null-polynomial over $\mathbb{Z}_n$ and the term of maximal degree is $a\boldsymbol{x}^{\boldsymbol{k}}$. Hence, $q(\boldsymbol{x}) - a\boldsymbol{x}^{\boldsymbol{k}}$ reduces $a\boldsymbol{x}^{\boldsymbol{k}}$. □

As an immediate consequence, we have:

Corollary 25. *A monomial $\boldsymbol{x}^{\boldsymbol{k}}$ is reducible modulo n if and only if it is weakly reducible.*

Furthermore it is proved in [9, Proposition 5, p. 8] that every polyfunction $f \in G_d(\mathbb{Z}_{p^m})$ has a unique representative of the form

$$f(\boldsymbol{x}) = \sum_{\substack{\boldsymbol{k} \in \mathbb{N}_0^d \\ e_p(\boldsymbol{k}) < m}} \alpha_{\boldsymbol{k}} \boldsymbol{x}^{\boldsymbol{k}},$$

where $\alpha_{\boldsymbol{k}} \in \{0, 1, \dots, p^{m - e_p(\boldsymbol{k})} - 1\}$. Notice, that $e_p(\boldsymbol{k}) < m$ if and only if $\boldsymbol{k} \in S_d(p^m)$ and hence this representative can be written as

$$f(\boldsymbol{x}) = \sum_{\boldsymbol{k} \in S_d(p^m)} \alpha_{\boldsymbol{k}} \boldsymbol{x}^{\boldsymbol{k}}. \tag{13}$$

In the case of one variable, what the Smarandache function really does is counting the number of monomials x^k, $k \in \mathbb{N}_0$, which are not reducible. Using the unique representative of a polyfunction above we can count the number of monomials $\boldsymbol{x}^{\boldsymbol{k}}$, $\boldsymbol{k} \in \mathbb{N}_0^d$, which are not reducible and hence to find a formula for $\Psi_d(n)$ which counts the number of polyfunctions in $G_d(\mathbb{Z}_n)$. In view of (13), we have for every coefficient $\alpha_{\boldsymbol{k}}$ exactly $p^{m - e_p(\boldsymbol{k})}$ choices and therefore we obtain:

Proposition 26. *The number of polyfunctions in $G_d(\mathbb{Z}_{p^m})$ is given by*

$$\Psi_d(p^m) = \prod_{\substack{\boldsymbol{k} \in \mathbb{N}_0^d \\ e_p(\boldsymbol{k}) < m}} p^{m - e_p(\boldsymbol{k})}. \tag{14}$$

On the other hand it is shown in [9, Theorem 6, p. 9] that

$$\Psi_d(p^m) = \exp_p\left(\sum_{k=1}^{m} s_d(p^k)\right). \tag{15}$$

The equivalence of the two formulas (14) and (15) can be established by a similar induction argument as in the proof of Proposition 11. However, it is much more instructive, to give a direct algebraic argument: We consider the surjective homomorphism H of rings defined by

$$H : G_d(\mathbb{Z}_{p^{m+1}}) \to G_d(\mathbb{Z}_{p^m}), \quad f \mapsto H(f) := h \circ f \circ h^*. \tag{16}$$

Here,

$$h : \mathbb{Z}_{p^{m+1}} \to \mathbb{Z}_{p^m}, \quad [x]_{p^{m+1}} \mapsto [x]_{p^m},$$

where $[x]_n$ denotes the coset of $x \in \mathbb{Z}$ modulo n. Similarly,

$$h^* : \mathbb{Z}^d_{p^m} \to \mathbb{Z}^d_{p^{m+1}}, \quad [\boldsymbol{x}]_{p^m} \mapsto [\boldsymbol{x}]_{p^{m+1}}$$

where $[\boldsymbol{x}]_{p^m} = [(x_1, \ldots x_d)]_{p^m} := ([x_1]_{p^m}, \ldots, [x_d]_{p^m})$ for $0 \leqslant x_i < p^m$. Then,

$$\Psi_d(p^{m+1}) = |G_d(\mathbb{Z}_{p^{m+1}})| = |G_d(\mathbb{Z}_{p^m})||\ker H|$$

and the equivalence of (14) and (15) is proved if we can show that

$$|\ker H| = p^{s_d(p^{m+1})}. \tag{17}$$

In view of (13), every polyfunction $f \in G_d(\mathbb{Z}_{p^{m+1}})$ has a unique representation

$$f(\boldsymbol{x}) = \sum_{\boldsymbol{k} \in S_d(p^{m+1})} \alpha_{\boldsymbol{k}} \boldsymbol{x}^{\boldsymbol{k}},$$

where $\alpha_{\boldsymbol{k}} \in \{0, 1, \ldots, p^{m+1-e_p(\boldsymbol{k})} - 1\}$. Since every number in this set can be written in a unique way as

$$\alpha_{\boldsymbol{k}} = \sum_{\{i \leqslant m+1 : \boldsymbol{k} \in S_d(p^i)\}} p^{m+1-i} \alpha_{\boldsymbol{k}i},$$

where $\alpha_{\boldsymbol{k}i} \in \mathbb{Z}_p$, all coefficients can be described as $ip^{m+1-e_p(\boldsymbol{k})}$, $\boldsymbol{k} \in S_d(p^{m+1})$ and $i = 0, 1, \ldots, p-1$ (see also [9, Proposition 5, p. 8]).

Observe, that $f \in \ker H$ if and only if $f(\boldsymbol{x}) \equiv 0 \mod p^m$, i.e. exactly if pf vanishes as a function $\mathbb{Z}^d_{p^{m+1}} \to \mathbb{Z}_{p^{m+1}}$.

Now, for each $\boldsymbol{k} \in S_d(p^{m+1})$ and every $a_i := ip^{m-e_p(\boldsymbol{k})}$, $i = 0, 1, \ldots, p-1$, the monomial $a_i p \boldsymbol{x}^{\boldsymbol{k}}$ is reducible modulo p^{m+1} by Lemma 24 since $p^{m+1} | a_i p \boldsymbol{k}!$. This implies that $p^m | a_i \boldsymbol{k}!$ and hence the monomial $a_i \boldsymbol{x}^{\boldsymbol{k}}$ is reducible modulo p^m, i.e. there exists a polynomial $q_{i,\boldsymbol{k}}(\boldsymbol{x})$ of degree strictly less than $|\boldsymbol{k}|$ which agrees modulo p^m with $a_i \boldsymbol{x}^{\boldsymbol{k}}$. Thus, $a_i \boldsymbol{x}^{\boldsymbol{k}} - q_{i,\boldsymbol{k}}(\boldsymbol{x})$ represent polyfunctions in $\ker H$. By the considerations above, every $f \in \ker H$ has therefore a unique representation of the form

$$f(\boldsymbol{x}) = \sum_{\boldsymbol{k} \in S_d(p^{m+1})} a_i \boldsymbol{x}^{\boldsymbol{k}} - q_{i,\boldsymbol{k}}(\boldsymbol{x}), \quad i \in \{0, 1, \ldots, p-1\}$$

and hence $|\ker H| = p^{|S_d(p^{m+1})|} = p^{s_d(p^{m+1})}$, as claimed. □

4.2. The number of units in $G_d(\mathbb{Z}_{p^m})$

We end this discussion by coming back to the question of units in the ring of polyfunctions (see Proposition 22). We denote by $U^d_{p^m}$ the multiplicative subgroup of units in $G_d(\mathbb{Z}_{p^m})$ and continue to use the notation $\Psi_d(p^m) = |G_d(\mathbb{Z}_{p^m})|$. We refer here to the formula $\Psi_d(p^m) = \exp_p(\sum_{k=1}^m s_d(p^k))$ from Proposition 26, where $s_d(p^k)$ is defined in (12). Then the following proposition holds

Proposition 27.

$$|U_{p^m}^d| = \left(\frac{p-1}{p}\right)^{dp} \Psi_d(p^m).$$

Proof. Using [9, Proposition 3, p. 5], we know that the elements in $U_{p^m}^d$ are precisely the unit-valued polyfunctions in $G_d(\mathbb{Z}_{p^m})$. Note that every function $\mathbb{Z}_p^d \to \mathbb{Z}$ is a polyfunction hence $|G_d(\mathbb{Z}_p)| = p^{dp}$ and since there are $p - 1$ units in $\mathbb{Z}_p$, we have

$$|U_p^d| = (p-1)^{dp}.$$

We use again the map

$$H : G_d(\mathbb{Z}_{p^{m+1}}) \to G_d(\mathbb{Z}_{p^m}), \quad f \mapsto H(f) = h \circ f \circ h^*$$

as defined after (16). Now

$$f \in U_{p^{m+1}}^d \iff H(f) \in U_{p^m}^d.$$

Indeed, $f \in U_{p^{m+1}}$ if and only if $f \circ h^*$ is unit valued with values in $\mathbb{Z}_{p^{m+1}}$ if and only if $((f \circ h^*)(\boldsymbol{x}), p^{m+1}) = 1$ if and only if $(H(f)(\boldsymbol{x}), p^{m+1}) = 1$ if and only if $(H(f)(\boldsymbol{x}), p^m) = 1$ (see also [2, Remark 12.1, Lemmas 7 and 8]). We conclude that

$$|U_{p^{m+1}}^d| = |\ker H||U_{p^m}^d|$$

and it follows from the proof of Proposition 26 that $|\ker H| = p^{s_d(p^{m+1})}$. So, inductively

$$|U_{p^m}^d| = \prod_{i=2}^m p^{s_d(p^i)} \left|U_p^d\right|$$

and since $|U_p^d| = (p-1)^{dp}$ we find using the formula for $\Psi_d(p^m)$ of Proposition 26

$$|U_{p^m}^d| = (p-1)^{dp} \exp_p\left(\sum_{i=2}^m s_d(p^i)\right) = \left(\frac{p-1}{p}\right)^{dp} \Psi_d(p^m).$$

□

Acknowledgments

We would like to thank the referee for his or her very careful reading and for all the valuable remarks and suggestions which greatly helped to improve the quality and readability of this article.

ORCID

Norbert Hungerbühler http://orcid.org/0000-0001-6191-0022

References

[1] Aigner, M. (1997). *Combinatorial Theory*. Berlin: Springer-Verlag.
[2] Al-Maktry, A. A. (2021). On the group of unit-valued polynomial functions. *Appl. Algebra Engrg. Comm. Comput*. DOI: 10.1007/s00200-021-00510-x.

[3] Bhargava, M. (1997). Congruence preservation and polynomial functions from Z_n to Z_m. *Discrete Math.* 173(1–3):15–21. DOI: 10.1016/S0012-365X(96)00093-3.

[4] Carlitz, L. (1964). Functions and polynomials $(\bmod\, p^n)$. *Acta Arith.* 9:67–78. DOI: 10.4064/aa-9-1-67-78.

[5] Chen, Z. (1995). On polynomial functions from Z_n to Z_m. *Discrete Math.* 137(1–3):137–145. DOI: 10.1016/0012-365X(93)E0162-W.

[6] Chen, Z. (1996). On polynomial functions from $Z_{n_1} \times Z_{n_2} \times \cdots \times Z_{n_r}$ to Z_m. *Discrete Math.* 162(1–3):67–76. DOI: 10.1016/0012-365X(95)00305-G.

[7] Dueball, F. (1949). Bestimmung von Polynomen aus ihren Werten $\bmod\ p^n$. *Math. Nachr.* 3:71–76. DOI: 10.1002/mana.19490030202.

[8] Halbeisen, L., Hungerbühler, N., Läuchli, H. (1999). Powers and polynomials in $\mathbb{Z}_m$. *Elem. Math.* 54(3):118–129. DOI: 10.1007/s000170050003.

[9] Hungerbühler, N., Specker, E. (2006). A generalization of the Smarandache function to several variables. *Integers.* 6:A23.

[10] Keller, G. E., Olson, F. R. (1968). Counting polynomial functions $(\bmod\, p^n)$. *Duke Math. J.* 35:835–838.

[11] Kempner, A. J. (1918). Concerning the smallest integer $m!$ divisible by a given integer n. *Amer. Math. Monthly.* 25(5):204–210. DOI: 10.2307/2972639.

[12] Kempner, A. J. (1921). Polynomials and their residual systems. *Trans. Amer. Math. Soc.* 22(2):240–266. DOI: 10.2307/1989020.

[13] Kempner, A. J. (1921). Polynomials and their residual systems (cont.). *Trans. Amer. Math. Soc.* 22(3):267–288. DOI: 10.2307/1988893.

[14] Li, X., Sha, M. (2019). Polynomial functions in the residue class rings of Dedekind domains. *Int. J. Number Theory.* 15(7):1473–1486. DOI: 10.1142/S1793042119500854.

[15] Lucas, E. (1883). Question Nr. $^{\times}$288. *Mathesis.* 3:232.

[16] Mullen, G., Stevens, H. (1984). Polynomial functions $(\bmod\, m)$. *Acta Math. Hungar.* 44(3–4):237–241. DOI: 10.1007/BF01950276.

[17] Rédei, L., Szele, T. (1947). Algebraisch-zahlentheoretische Betrachtungen über Ringe. I. *Acta Math.* 79:291–320. DOI: 10.1007/BF02404701.

[18] Rédei, L., Szele, T. (1950). Algebraisch-zahlentheoretische Betrachtungen über Ringe. II. *Acta Math.* 82:209–241. DOI: 10.1007/BF02398278.

[19] Singmaster, D. (1974). On polynomial functions $(\bmod\ m)$. *J. Number Theory.* 6:345–352. DOI: 10.1016/0022-314X(74)90031-6.

[20] Specker, E., Hungerbühler, N., Wasem, M. (2022). Polyfunctions over general rings (submitted).