INTEGERS: ELECTRONIC JOURNAL OF COMBINATORIAL NUMBER THEORY 6 (2006), #A23

A GENERALIZATION OF THE SMARANDACHE FUNCTION TO SEVERAL VARIABLES

Norbert Hungerbühler
Department of Mathematics, University of Fribourg, Pérolles, 1700 Fribourg, Switzerland
norbert.hungerbuehler@unifr.ch

Ernst Specker
Department of Mathematics, ETH Zürich, 8092 Zürich, Switzerland
specker@math.ethz.ch

Received: 1/16/06, Accepted: 6/30/06, Published: 10/06/06

Abstract

We investigate polyfunctions in several variables over $\mathbb{Z}_n$. We show in particular how the problem of determining the cardinality of the ring of these functions leads to a natural generalization of the classical Smarandache function.

1. Introduction

Let us consider the ring $\mathbb{Z}_n := \mathbb{Z}/n\mathbb{Z}$, $n > 1$, and a function

$$f : \mathbb{Z}_n^d \to \mathbb{Z}_n$$

of d variables in $\mathbb{Z}_n$ with values in $\mathbb{Z}_n$. Such a function is called a **polyfunction** if there exists a polynomial

$$p \in \mathbb{Z}_n[x_1, \dots, x_d]$$

such that

$$f(\boldsymbol{x}) \equiv p(\boldsymbol{x}) \mod n \qquad \forall \boldsymbol{x} = \langle x_1, \dots, x_d \rangle \in \mathbb{Z}_n^d.$$

The set of polyfunctions of d variables in $\mathbb{Z}_n$ with values in $\mathbb{Z}_n$, equipped with pointwise addition and multiplication, is a ring with unit element. We denote this ring by $G_d(\mathbb{Z}_n)$, or, for simplicity, by $G(\mathbb{Z}_n)$ in the case of only one variable.

In the present article, we investigate polyfunctions in several variables over $\mathbb{Z}_n$. We show in particular how the problem of determining the cardinality of the ring of these functions leads to a natural generalization of the classical Smarandache function (named after [17])

$$\begin{array}{rcl} s:\mathbb{N} & \to & \mathbb{N} \\ n & \mapsto & s(n) := \min\{k \in \mathbb{N} : n \mid k!\}, \end{array} \tag{1}$$

which was studied by Lucas in [10] for powers of primes, and by Kempner in [8] and Neuberg in [12] for general n. Indeed, $s(n)$ is the minimal degree of a normed polynomial which vanishes (as a function) identically in $\mathbb{Z}_n$ (see [5]). The key is then to reformulate the above definition by setting

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

This definition then generalizes in a natural way to $d > 1$ dimensions (see (10) and (11)), where the number can be interpreted as the number of irreducible monomials $\boldsymbol{x}^{\boldsymbol{k}}$ modulo n (see Section 5).

The number of polyfunctions in $G_d(\mathbb{Z}_n)$ is multiplicative in n (see Section 5). It therefore suffices to compute the values for $n = p^m$, p prime. By analysing the structure of the additive group of $G_d(\mathbb{Z}_{p^m})$, which is completely described in Proposition 7, we find

$$|G_d(\mathbb{Z}_{p^m})| = p^{\sum_{i=1}^{m} s_d(p^i)}$$

(see Theorem 6). However, the factors $p^{s_d(p^i)}$ do not correspond to additive subgroups of $G_d(\mathbb{Z}_{p^m})$.

In Section 3 we present a characterization which allows us to test whether a given function $f : \mathbb{Z}_n^d \to \mathbb{Z}_n$ is a polyfunction, and if so, to determine a polynomial representative of f. In Section 4 we characterize the units in the ring $G_d(\mathbb{Z}_n)$.

We conclude this introduction with a short overview on the history of polyfunctions. The study of polyfunctions in one variable goes back to Kempner who discussed polyfunctions over $\mathbb{Z}_n$ in connection with Kronecker modular systems [9]. He also gave a formula for the number of polyfunctions over $\mathbb{Z}_n$. Later, Carlitz investigated properties of polyfunctions over $\mathbb{Z}_{p^n}$ for p prime [2]. Keller and Olson gave a simplified proof of Kempner's formula [7] and also determined the number of polyfunctions which represent a permutation of $\mathbb{Z}_{p^n}$. Null-polynomials over $\mathbb{Z}_n$ (i.e., polynomials which represent the zero-function) have been investigated by Singmaster [15]. Certain aspects of polyfunctions in several variables over $\mathbb{Z}_n$ were addressed in [11]. Recently, polyfunctions from $\mathbb{Z}_n$ to $\mathbb{Z}_m$ have attracted increasing attention (see [3], [4] and [1]). The focus there is to find conditions on the pair $\langle m, n\rangle$ such that all functions (or certain subclasses) from $\mathbb{Z}_n$ to $\mathbb{Z}_m$ are polyfunctions. In [13] and [14] polyfunctions over a general ring were discussed: the question asked being "for which rings R one can find a ring S, such that all functions on R can be represented by polynomials over S?"

2. Notation, Definitions and Basic Facts

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

$$\boldsymbol{x}^{\boldsymbol{k}} := \prod_{i=1}^{d} x_i^{k_i}$$

and

$$\boldsymbol{k}! := \prod_{i=1}^{d} k_i!.$$

Furthermore, we write

$$|\boldsymbol{k}| := \sum_{i=1}^{d} k_i$$

and

$$\binom{\boldsymbol{x}}{\boldsymbol{k}} := \prod_{i=1}^{d} \binom{x_i}{k_i}.$$

Let $\boldsymbol{e}_i := \langle 0, \ldots, 0, 1, 0, \ldots, 0 \rangle \in \mathbb{Z}_n^d$, with the 1 at place i. Then, we define the (forward) partial difference operator Δ by

$$\begin{aligned} \Delta_i g(\boldsymbol{x}) &:= g(\boldsymbol{x} + \boldsymbol{e}_i) - g(\boldsymbol{x}) \\ \Delta_i^0 &:= \text{identity} \\ \Delta_i^k &:= \Delta_i \circ \Delta_i^{k-1}. \end{aligned}$$

For a multi-index $\boldsymbol{k}$, let

$$\Delta^{\boldsymbol{k}} := \Delta_1^{k_1} \circ \ldots \circ \Delta_d^{k_d}.$$

Notice that the Δ operators commute and that $\Delta^{\boldsymbol{k}_1} \circ \Delta^{\boldsymbol{k}_2} = \Delta^{\boldsymbol{k}_1 + \boldsymbol{k}_2}$. We recall that

$$\Delta^{\boldsymbol{r}} g(\boldsymbol{x}) = \sum_{\boldsymbol{k} \leqslant \boldsymbol{r}} g(\boldsymbol{x} + \boldsymbol{r} - \boldsymbol{k})(-1)^{|\boldsymbol{k}|} \binom{\boldsymbol{r}}{\boldsymbol{k}}, \tag{2}$$

where $\boldsymbol{k} \leqslant \boldsymbol{r}$ means $0 \leqslant k_i \leqslant r_i$ (see e.g. [16]). A polynomial p equals its "Taylor expansion"

$$p(\boldsymbol{x}) = \sum_{|\boldsymbol{k}| \leqslant \deg(p)} \Delta^{\boldsymbol{k}} p(\boldsymbol{0}) \binom{\boldsymbol{x}}{\boldsymbol{k}} \tag{3}$$

(see e.g. [6]). Observe, that the monomial x^l defines by $((x+n)^l)_{n \in \mathbb{Z}}$ for any fixed x an arithmetic sequence of order l. Therefor, one easily checks by induction, that

$$\Delta^r x^l = \begin{cases} 0 & \text{if } r > l, \\ r! & \text{if } r = l. \end{cases} \tag{4}$$

Hence, the summation in (3) can be restricted to the **shadow** of p, i.e., the multi-indices $\boldsymbol{k}$ with the property that $0 \leqslant \boldsymbol{k} \leqslant \boldsymbol{r}$ for a monomial $\boldsymbol{x}^{\boldsymbol{r}}$ in p. Indeed, if $\boldsymbol{k}$ does not belong to the shadow of p, then $\Delta^{\boldsymbol{k}} p(\mathbf{0}) = 0$ by (4).

It is well known (see e.g. [6]) that a polynomial p has integer coefficients if and only if the condition

$$\boldsymbol{k}! \mid \Delta^{\boldsymbol{k}} p(\mathbf{0}) \tag{5}$$

holds for all $\boldsymbol{k}$ in the shadow of p (for other values of $\boldsymbol{k}$, the condition (5) is trivially satisfied by the previous remark).

3. Characterization of Polyfunctions

Let $f : \mathbb{Z}_n^d \to \mathbb{Z}_n$ be a polyfunction, i.e., there exists a polynomial $p \in \mathbb{Z}_n[x_1, \ldots, x_d]$ such that

$$f(\boldsymbol{x}) \equiv p(\boldsymbol{x}) \mod n \quad \text{for all } \boldsymbol{x} \in \mathbb{Z}_n^d. \tag{6}$$

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

$$\prod_{i=0}^{n-1} (x - i) = 0 \text{ in } \mathbb{Z}_n,$$

we may assume, without loss of generality, that the degree of p is, in each variable separately, strictly less than n. Thus, in $\mathbb{Z}_n$ we have for arbitrary $\boldsymbol{x} \in \mathbb{Z}_n^d$,

$$\begin{aligned} f(\boldsymbol{x}) &\overset{\text{by (6)}}{=} p(\boldsymbol{x}) \\ &\overset{\text{by (3)}}{=} \sum_{k_i < n} \Delta^{\boldsymbol{k}} p(\mathbf{0}) \binom{\boldsymbol{x}}{\boldsymbol{k}} \\ &\overset{\text{by (6)}}{=} \underbrace{\sum_{k_i < n} \Delta^{\boldsymbol{k}} f(\mathbf{0}) \binom{\boldsymbol{x}}{\boldsymbol{k}}}_{=: h(\boldsymbol{x})}. \end{aligned}$$

Hence, the polynomial h represents f, but it does not necessarily have integer coefficients. However, observing (5) and exploiting the fact that in $\mathbb{Z}_n$,

$$\Delta^{\boldsymbol{k}} p(\mathbf{0}) = \Delta^{\boldsymbol{k}} f(\mathbf{0})$$

holds for all $\boldsymbol{k}$, we obtain:

Lemma 1 *If $f : \mathbb{Z}_n^d \to \mathbb{Z}_n$ is a polyfunction, then* *(i) for all multi-indices* $\boldsymbol{k}$ *with components* $k_i < n$*, there exist* $\alpha_{\boldsymbol{k}} \in \mathbb{Z}$ *such that for the numbers* $\beta_{\boldsymbol{k}} := \Delta^{\boldsymbol{k}} f(\boldsymbol{0}) + \alpha_{\boldsymbol{k}} n$*,*

$$\boldsymbol{k}! \mid \beta_{\boldsymbol{k}}, \tag{7}$$

and

(ii) the polynomial $\sum_{k_i<n} \beta_{\boldsymbol{k}} \binom{\boldsymbol{x}}{\boldsymbol{k}}$ *has integer coefficients and represents* f*.*

From (7) it follows, that

$$(n, \boldsymbol{k}!) \mid \Delta^{\boldsymbol{k}} f(\boldsymbol{0}) \quad [1] \tag{8}$$

for all $\boldsymbol{k}$ with $k_i < n$. We will show now that this condition characterizes polyfunctions. To this end, we consider an arbitrary function $f : \mathbb{Z}_n^d \to \mathbb{Z}_n$. Since there exists an interpolation polynomial for f, with degree in each variable strictly less than n, which agrees with f on the set $\{0, 1, \ldots, n-1\}^d$, we infer from (3) that, in $\mathbb{Z}_n$,

$$f(\boldsymbol{x}) = \sum_{k_i<n} \Delta^{\boldsymbol{k}} f(\boldsymbol{0}) \binom{\boldsymbol{x}}{\boldsymbol{k}}$$

for all $\boldsymbol{x} \in \mathbb{Z}_n^d$. If condition (8) is satisfied for f, we find coefficients $\beta_{\boldsymbol{k}} = \Delta^{\boldsymbol{k}} f(\boldsymbol{0}) + \alpha_{\boldsymbol{k}} n$, as above in Lemma 1(i), such that $\boldsymbol{k}! \mid \beta_{\boldsymbol{k}}$. Hence, in $\mathbb{Z}_n$

$$f(\boldsymbol{x}) = \sum_{k_i<n} \beta_{\boldsymbol{k}} \binom{\boldsymbol{x}}{\boldsymbol{k}} \bmod \Big(\sum_{k=0}^{n-1} \beta_k \binom{x}{k}, n\Big),$$

for all $\boldsymbol{x} \in \mathbb{Z}_n^d$. In other words, condition (8) implies that f is a polyfunction and we have the following characterization:

Theorem 2 *$f : \mathbb{Z}_n^d \to \mathbb{Z}_n$ is a polyfunction over $\mathbb{Z}_n$ if and only if $(n, \boldsymbol{k}!) \mid \Delta^{\boldsymbol{k}} f(\boldsymbol{0})$ for all multi-indices $\boldsymbol{k}$ with $k_i < n$.*

4. The Inverse of a Polyfunction

Let $f : \mathbb{Z}_n^d \to \mathbb{Z}_n$. Then f is invertible (i.e., there exists a function $g : \mathbb{Z}_n^d \to \mathbb{Z}_n$, such that for all $\boldsymbol{x} \in \mathbb{Z}_n^d$ there holds $f(\boldsymbol{x})g(\boldsymbol{x}) = 1$) if and only if $\mathrm{Image}(f) \subset U(\mathbb{Z}_n)$. Here, $U(\mathbb{Z}_n)$ denotes the multiplicative group of units in $\mathbb{Z}_n$. We want to show that the same characterization holds for invertible polyfunctions over $\mathbb{Z}_n$.

Proposition 3 *A polyfunction $f : \mathbb{Z}_n^d \to \mathbb{Z}_n$ is invertible in the ring of polyfunctions (and hence a unit in $G_d(\mathbb{Z}_n)$) if and only if*

$$\mathrm{Image}(f) \subset U(\mathbb{Z}_n).$$

Proof. The necessity of the condition is trivial. In order to prove that it is also sufficient, let $k := \operatorname{lcm}\{\operatorname{ord}(x) \mid x \in U(\mathbb{Z}_n)\}$[2]. Then, if p denotes a polynomial representing f, we have

$$p^k(\boldsymbol{x}) = 1 \quad \text{in } \mathbb{Z}_n$$

for all $\boldsymbol{x} \in \mathbb{Z}_n^d$. Hence, the polynomial p^{k-1} represents the inverse of f. □

5. The Number of Polyfunctions

Let a be an element of $\mathbb{Z}_n$. We say, the monomial $a\boldsymbol{x}^{\boldsymbol{k}} \in \mathbb{Z}_n[\boldsymbol{x}]$ 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** (modulo n) if $a\boldsymbol{x}^{\boldsymbol{k}} \equiv p(\boldsymbol{x}) \mod n$ for all $\boldsymbol{x} \in \mathbb{Z}_n^d$, for a polynomial $p \in \mathbb{Z}_n[\boldsymbol{x}]$ with $\deg(p) \leqslant |\boldsymbol{k}|$ (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.

The following lemma characterizes the tuples $\boldsymbol{k}$ for which $a\boldsymbol{x}^{\boldsymbol{k}}$ is (weakly) reducible.

Lemma 4 *(i) If $a\boldsymbol{x}^{\boldsymbol{k}} \in \mathbb{Z}_n[\boldsymbol{x}]$ is weakly reducible modulo n, then $n \mid a\boldsymbol{k}!$.*
(ii) If $n \mid a\boldsymbol{k}!$, then $a\boldsymbol{x}^{\boldsymbol{k}}$ is reducible modulo n.

In particular, a monomial is reducible if and only if it is weakly reducible.

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 (i.e., a polynomial which represents the zero-function) in d variables over $\mathbb{Z}_n$. Then, we write q in the form

$$q(\boldsymbol{x}) = \sum_{\substack{\boldsymbol{l} \in \mathbb{N}_0^d \\ |\boldsymbol{l}| \leqslant |\boldsymbol{k}|}} q_{\boldsymbol{l}} \boldsymbol{x}^{\boldsymbol{l}} \tag{9}$$

for suitable coefficients $q_{\boldsymbol{l}} \in \mathbb{Z}_n$, with $q_{\boldsymbol{k}} = a$. Using the linearity of the Δ operator, we obtain that, modulo n,

$$0 = \Delta^{\boldsymbol{k}} q(\boldsymbol{x}) \overset{(9)}{=} \sum_{\substack{\boldsymbol{l} \in \mathbb{N}_0^d \\ |\boldsymbol{l}| \leqslant |\boldsymbol{k}|}} q_{\boldsymbol{l}} \Delta^{\boldsymbol{k}} \boldsymbol{x}^{\boldsymbol{l}} \overset{(4)}{=} a\boldsymbol{k}!.$$

In fact, all terms in the above sum with $\boldsymbol{l} \neq \boldsymbol{k}$ vanish by (4), since $|\boldsymbol{l}| \leqslant |\boldsymbol{k}|$ and $\boldsymbol{l} \neq \boldsymbol{k}$ implies that $\boldsymbol{k}$ is not in the shadow of $\boldsymbol{x}^{\boldsymbol{l}}$. And the only remaining term, $\Delta^{\boldsymbol{k}} x^{\boldsymbol{k}}$, equals $\boldsymbol{k}!$, again by (4).

[2] $\operatorname{lcm}(M)$ is the least common multiple of all integer numbers in a finite set M. $\operatorname{ord}(x)$ denotes the order of an element x in a finite multiplicative group G, i.e., $\operatorname{ord}(x)$ is the smallest number $k \in \mathbb{N}$ such that $x^k = 1$.

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

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

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 to $a\boldsymbol{x}^{\boldsymbol{k}}$. □

Lemma 4 allows us to count the number of monomials $\boldsymbol{x}^{\boldsymbol{k}}$, $\boldsymbol{k} \in \mathbb{N}_0^d$, which are not reducible. Let

$$S_d(n) := \{\boldsymbol{k} \in \mathbb{N}_0^d : n \nmid \boldsymbol{k}!\} \tag{10}$$

denote the set of multi-indices $\boldsymbol{k}$ such that $\boldsymbol{x}^{\boldsymbol{k}}$ is not reducible modulo n. Its cardinality is the natural generalization of the Smarandache function to the case of several variables:

$$s_d(n) := |S_d(n)|. \tag{11}$$

Of course, for $d = 1$ the function s_1 agrees with the usual number theoretic Smarandache function (see introduction)—except for $n = 1$, since $s(1) = 1$, but $s_1(1) = 0$. Actually, by defining $s(n) := \min\{k \in \mathbb{N}_0 : n \mid k!\}$ (i.e., the minimum is taken over $k \in \mathbb{N}_0$ rather than over $k \in \mathbb{N}$), this discrepancy could be removed. Incidentally, Kempner originally defined $s(1) = 1$ in [8], but changed to $s(1) = 0$ in [9]. The following table displays $s_d(n)$ for the first few values of d and n.

n	1	2	3	4	5	6	7	8	9	10	11	12	13
s_1	0	2	3	4	5	3	7	4	6	5	11	4	13
s_2	0	4	9	12	25	9	49	16	27	25	121	13	169
s_3	0	8	27	32	125	27	343	56	108	125	1331	39	2197
s_4	0	16	81	80	625	81	2401	176	405	625	14641	113	28561

Table 1: Values of $s_d(n)$

Before we now start to compute the number of $\Psi_d(p^m)$ poyfunctions in $G_d(\mathbb{Z}_{p^m})$, it is useful to include a general remark. The notion of the ring of polyfunctions $G(\mathbb{Z}_n)$ generalizes in a natural way to the ring $G(R)$ of polyfunctions over an arbitrary ring R. 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 $(m, n) = 1$.

Analogously in several variables, we have the decomposition $G_d(\mathbb{Z}_{mn}) \cong G_d(\mathbb{Z}_m) \oplus G_d(\mathbb{Z}_n)$ if $(m, n) = 1$. This means, e.g., that the number $\Psi_d(n)$ of polyfunctions in $G_d(\mathbb{Z}_n)$ is multiplicative in n. Therefore, we may restrict ourselves to the case $n = p^m$ for p prime.

Now, the strategy to count the number of polyfunctions is to seek a unique standard representation of such functions by a polynomial. Such a representation is given in Proposition 5 below. Then, we will just have to count these representing polynomials. Let us first consider the case of one variable. Obviously,

$$\prod_{i=1}^{s_1(n)}(x-i)=\binom{x+s_1(n)}{s_1(n)}s_1(n)!$$

is a normed[3] null-polynomial in $G(\mathbb{Z}_n)$, and from Lemma 4 it follows in particular that there is no polynomial of smaller degree with this property. Therefore, every polyfunction in one variable over $\mathbb{Z}_n$ has a (not necessarily unique) representing polynomial of degree strictly less than $s_1(n)$ (and here $s_1(n)$ cannot be replaced by a smaller number). Basically by the same argument, Lemma 4 allows us to construct a unique representation of every polyfunction in d variables over $\mathbb{Z}_{p^m}$.

Proposition 5 *Every polyfunction $f \in G_d(\mathbb{Z}_{p^m})$ has a unique representation of the form*

$$f(\boldsymbol{x}) \equiv \sum_{i=1}^{m} p^{m-i} \sum_{\boldsymbol{k}\in S_d(p^i)} \alpha_{\boldsymbol{k}i}\boldsymbol{x}^{\boldsymbol{k}} \tag{12}$$

where $\alpha_{\boldsymbol{k}i} \in \mathbb{Z}_p$.

Proof. It is common to write $n=\prod p^{\nu_p(n)}$ for the prime decomposition of a positive integer n. We adopt this notation and write

$$\nu_p(\boldsymbol{k}!) = \max\{x \in \mathbb{N}_0 \,:\, p^x \mid \boldsymbol{k}!\}$$

for the number of factors p in $\boldsymbol{k}!$. Notice that $\nu_p(\boldsymbol{k}!) < i$ if and only if $\boldsymbol{k} \in S_d(p^i)$. Then, as an immediate consequence of Lemma 4, we obtain, that every polyfunction $f \in G_d(\mathbb{Z}_{p^m})$ has a unique representation of the form

$$f(\boldsymbol{x}) \equiv \sum_{\substack{\boldsymbol{k}\in\mathbb{N}_0^d\\ \nu_p(\boldsymbol{k}!)<m}} \alpha_{\boldsymbol{k}}\boldsymbol{x}^{\boldsymbol{k}}, \tag{13}$$

where $\alpha_{\boldsymbol{k}} \in \{0,1,\ldots,p^{m-\nu_p(\boldsymbol{k}!)}-1\}$. Since, on the other hand, every number $\alpha_{\boldsymbol{k}} \in \{0,1,\ldots,$ $p^{m-\nu_p(\boldsymbol{k}!)}-1\}$ has a unique representation of the form

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

for certain coefficients $\alpha_{\boldsymbol{k}i} \in \mathbb{Z}_p$, we can rewrite (13) such that we obtain (12). □

As an immediate consequence of Proposition 5, we now get the formula for the number of poyfunctions in the following theorem. Observe that we use the notation $\exp_p a := p^a$ for better readability.

[3]i.e., its leading coefficient is 1

Theorem 6 *The number of polyfunctions in $G_d(\mathbb{Z}_{p^m})$, p prime, is given by*

$$\Psi_d(p^m) = \exp_p\Big(\sum_{i=1}^{m} s_d(p^i)\Big).$$

Example. To compute the number of polyfunctions $\Psi_2(8)$ in two variables over $\mathbb{Z}_8$, we need:

$$\begin{aligned} S_2(2) &= \{\langle k_1, k_2\rangle : 0 \leqslant k_1 \leqslant 1, 0 \leqslant k_2 \leqslant 1\} \\ s_2(2) &= 4 \\ S_2(4) &= \{\langle k_1, k_2\rangle : 0 \leqslant k_1 \leqslant 3, 0 \leqslant k_2 \leqslant 3, k_1k_2 < 4\} \\ s_2(4) &= 12 \\ S_2(8) &= \{\langle k_1, k_2\rangle : 0 \leqslant k_1 \leqslant 3, 0 \leqslant k_2 \leqslant 3\} \\ s_2(8) &= 16. \end{aligned}$$

This gives $\Psi_2(8) = 2^{4+12+16} = 2^{32}$. ○

Notice that the formulas (13) and (12) reflect the structure of the additive group of $G_d(\mathbb{Z}_{p^m})$. In fact

$$A_{d\boldsymbol{k}}(\mathbb{Z}_{p^m}) := \{f \in G_d(\mathbb{Z}_{p^m}) \;:\; f(x) \equiv \alpha \boldsymbol{x}^{\boldsymbol{k}},\; \alpha \in \mathbb{Z}_{p^{m-\nu_p(\boldsymbol{k}!)}}\} \cong \mathbb{Z}_{p^{m-\nu_p(\boldsymbol{k}!)}}$$

are additive subgroups in $G_d(\mathbb{Z}_{p^m})$ and hence, by (13):

Proposition 7 $(G_d(\mathbb{Z}_{p^m}), +) \cong \bigoplus_{\substack{\boldsymbol{k}\in\mathbb{N}_0^d \\ \nu_p(\boldsymbol{k}!)<m}} \mathbb{Z}_{p^{m-\nu_p(\boldsymbol{k}!)}}.$

As an immediate consequence of Theorem 6 and Proposition 7, we note the following identity:

Corollary 8 $\displaystyle\sum_{i=1}^{m} s_d(p^i) = \sum_{\boldsymbol{k}\in S_d(p^m)} \big(m - \nu_p(\boldsymbol{k}!)\big) = m\, s_d(p^m) - \sum_{\boldsymbol{k}\in S_d(p^m)} \nu_p(\boldsymbol{k}!).$

For completeness, we add an explicit formula for $\Psi_d(n) = |G_d(\mathbb{Z}_n)|$ for general n. We start from the identity

$$\Psi_d(n) = \Psi_d(\prod_{i=1}^{k} p_i^{\nu_{p_i}(n)}) = \prod_{i=1}^{k} \Psi_d(p_i^{\nu_{p_i}(n)}).$$

By taking the logarithm on both sides and using Theorem 6 we obtain

$$\begin{aligned} \ln \Psi_d(n) &= \sum_{i=1}^{k} \ln \Psi_d(p_i^{\nu_{p_i}(n)}) \\ &= \sum_{i=1}^{k} \ln p_i \sum_{j=1}^{\nu_{p_i}(n)} s_d(p_i^j). \end{aligned} \tag{14}$$

Observe that the Mangoldt function

$$\Lambda : \mathbb{N} \to \mathbb{N}, \quad x \mapsto \begin{cases} \ln p & \text{if } x = p^k,\ p \text{ prime},\ k \geqslant 1 \\ 0 & \text{else} \end{cases}$$

allows us to simplify (14) further and to obtain

$$\ln \Psi_d(n) = \sum_{i=1}^{k} \sum_{j=1}^{\nu_{p_i}(n)} s_d(p_i^j)\Lambda(p_i^j).$$

Since the Mangoldt function is zero on all numbers which are not powers of primes, this last expression can be interpreted as a sum over *all* divisors of n. Moreover, since $\Lambda(1) = 0$, the value of $s_d(1)$ is irrelevant. Hence, using the Dirichlet convolution

$$(f * g)(n) = \sum_{d|n} f\Big(\frac{n}{d}\Big)g(d)$$

with $f \equiv 1$ and $g = s_d\,\Lambda$, we arrive at

$$\ln \Psi_d(n) = \big(1 * (s_d\,\Lambda)\big)(n).$$

Hence, we have the following Theorem:

Theorem 9 *The number $\Psi_d(n)$ of polyfunctions in $G_d(\mathbb{Z}_n)$, $n > 1$, is given by*

$$\Psi_d(n) = e^{1*(s_d\,\Lambda)(n)}.$$

6. The Towers of Hanoï

The Smarandache function can be used to solve the Towers of Hanoï problem. In Theorem 6, for $p = 2$ and one variable, we need the numbers

$$s(2^k).$$

Let us consider the first difference sequence

$$a_k := s(2^k) - s(2^{k-1}), \qquad k = 1, 2, 3, \ldots$$

The sequence starts with

$$(a_k)_{k\in\mathbb{N}} = (2, 2, \underbrace{0}_{\varepsilon_1}, 2, 2, \underbrace{0, 0}_{\varepsilon_2}, 2, 2, \underbrace{0}_{\varepsilon_3}, 2, 2, \underbrace{0, 0, 0}_{\varepsilon_4}, 2, 2, \underbrace{0}_{\varepsilon_5}, 2, 2, \ldots).$$

Two 2s alternate with groups of ε_k 0s. The sequence

$$(\varepsilon_k)_{k\in\mathbb{N}} = (1,2,1,3,1,2,1,4,1,2,1,3,1,2,1,5,\\ 1,2,1,3,1,2,1,4,1,2,1,3,1,2,1,6,1,\dots),$$

with the property that 2^{ε_k} divides exactly $2k$, is now indeed the solution of the Towers of Hanoï. It provides the number of the disk, which is to be relocated in the k-th move.

Alternatively, knowing the solution of the Towers of Hanoï one has an efficient way to compute $s(2^k)$.

References

[1] M. Bhargava: Congruence preservation and polynomial functions from Z_n to Z_m. Discrete Math. **173** (1997), no. 1–3, 15–21.

[2] L. Carlitz: Functions and polynomials (mod p^n). Acta Arith. **9** (1964), 67–78.

[3] Z. Chen: On polynomial functions from Z_n to Z_m. Discrete Math. **137** (1995), no. 1–3, 137–145.

[4] Z. Chen: On polynomial functions from $Z_{n_1} \times Z_{n_2} \times \cdots \times Z_{n_r}$ to Z_m. Discrete Math. **162** (1996), no. 1–3, 67–76.

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

[6] L. K. Hua: Introduction to Number Theory. Springer, 1982.

[7] G. Keller, F. R. Olson: Counting polynomial functions (mod p^n). Duke Math. J. **35** (1968), 835–838.

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

[9] A. J. Kempner: Polynomials and their residual systems. Amer. Math. Soc. Trans. **22** (1921), 240–288.

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

[11] G. Mullen, H. Stevens: Polynomial functions (mod m). Acta Math. Hungar. **44** (1984), no. 3–4, 237–241.

[12] J. Neuberg: Solutions de questions proposées, Question Nr. $^\times$**288**. Mathesis **7** (1887), 68–69.

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

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

[15] D. Singmaster: On polynomial functions (mod m). J. Number Theory **6** (1974), 345–352.

[16] N. J. A. Sloane, S. Plouffe: The Encyclopedia of Integer Sequences. San Diego, CA: Academic Press, 1995.

[17] F. Smarandache: A Function in the Number Theory. Analele Univ. Timisoara, Fascicle 1, Vol. **XVIII** (1980), 79–88.