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

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

such that

\[ f(x) \equiv p(x) \mod n \quad \forall x = (x_1, \ldots, x_d) \in \mathbb{Z}_n^d. \]

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])
\[
s : \mathbb{N} \rightarrow \mathbb{N} \\
  n \mapsto s(n) := \min\{k \in \mathbb{N} : n \mid k!\},
\]
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 \( x^k \) 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 \( f : \mathbb{Z}_n^d \rightarrow \mathbb{Z}_n \) 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 \( (m, n) \) 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 \( \mathbf{k} = \langle k_1, k_2, \ldots, k_d \rangle \in \mathbb{N}_0^d \) and \( \mathbf{x} := \langle x_1, x_2, \ldots, x_d \rangle \), let

\[
\mathbf{x}^\mathbf{k} := \prod_{i=1}^{d} x_i^{k_i}
\]

and

\[
\mathbf{k}! := \prod_{i=1}^{d} k_i!.
\]

Furthermore, we write

\[
|\mathbf{k}| := \sum_{i=1}^{d} k_i
\]

and

\[
\left(\begin{array}{c} \mathbf{x} \\ \mathbf{k} \end{array}\right) := \prod_{i=1}^{d} \left(\begin{array}{c} x_i \\ k_i \end{array}\right).
\]

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

\[
\Delta_i g(x) := g(x + e_i) - g(x)
\]

\[
\Delta_0^0 := \text{identity}
\]

\[
\Delta_0^k := \Delta_i \circ \Delta_i^{k-1}.
\]

For a multi-index \( \mathbf{k} \), let

\[
\Delta^\mathbf{k} := \Delta_1^{k_1} \circ \ldots \circ \Delta_d^{k_d}.
\]

Notice that the \( \Delta \) operators commute and that \( \Delta_1^{k_1} \circ \Delta_1^{k_2} = \Delta_1^{k_1+k_2} \). We recall that

\[
\Delta^r g(x) = \sum_{\mathbf{k} \leq \mathbf{r}} g(x + r - \mathbf{k})(-1)^{|\mathbf{k}|} \binom{\mathbf{r}}{\mathbf{k}},
\]

where \( \mathbf{k} \leq \mathbf{r} \) means \( 0 \leq k_i \leq r_i \) (see e.g. [16]). A polynomial \( p \) equals its “Taylor expansion”

\[
p(x) = \sum_{|\mathbf{k}| \leq \deg(p)} \Delta^\mathbf{k} p(0) \left(\begin{array}{c} \mathbf{x} \\ \mathbf{k} \end{array}\right)
\]

(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

\[
\Delta^r x^l = \begin{cases} 
0 & \text{if } r > l, \\
 r! & \text{if } r = l.
\end{cases}
\]
Hence, the summation in (3) can be restricted to the shadow of \( p \), i.e., the multi-indices \( k \) with the property that \( 0 \leq k \leq r \) for a monomial \( x^r \) in \( p \). Indeed, if \( k \) does not belong to the shadow of \( p \), then \( \Delta^k p(0) = 0 \) by (4).

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

\[
\text{if } k \text{ belongs to the shadow of } p, \text{ then } \Delta^k p(0) = 0 \text{ by (4).}
\]

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

3. Characterization of Polyfunctions

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

\[
f(x) \equiv p(x) \mod n \text{ for all } x \in \mathbb{Z}^d_n.
\]

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 \( x \in \mathbb{Z}^d_n \):

\[
f(x) \overset{\text{by (6)}}{=} p(x) \overset{\text{by (3)}}{=} \sum_{k_i < n} \Delta^k p(0) \binom{x}{k} \overset{\text{by (6)}}{=} \sum_{k_i < n} \Delta^k f(0) \binom{x}{k} \overset{=: h(x)}{=}
\]

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

\[
\Delta^k p(0) = \Delta^k f(0)
\]

holds for all \( k \), we obtain:

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

$$k! \mid \beta_k,$$

and

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

From (7) it follows, that

$$(n, k!) \mid \Delta^k f(0)$$

for all $k$ 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 $\mathbb{Z}_n$,

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

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

$$f(x) = \sum_{k_i < n} \beta_k \binom{x}{k} \mod \left( \sum_{k=0}^{n-1} \beta_k \binom{x}{k}, n \right),$$

for all $x \in \mathbb{Z}_n^d$. 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 $(n, k!) \mid \Delta^k f(0)$ for all multi-indices $k$ 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 $x \in \mathbb{Z}_n^d$, there holds $f(x)g(x) = 1$) if and only if $\text{Image}(f) \subset U(\mathbb{Z}_n)$. 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

$$\text{Image}(f) \subset U(\mathbb{Z}_n).$$
Proof. The necessity of the condition is trivial. In order to prove that it is also sufficient, let \( k := \text{lcm}\{\text{ord}(x) \mid x \in U(\mathbb{Z}_n)\}^2 \). Then, if \( p \) denotes a polynomial representing \( f \), we have
\[
p^k(x) = 1 \quad \text{in} \quad \mathbb{Z}_n
\]
for all \( x \in \mathbb{Z}_n^d \). Hence, the polynomial \( p^{k-1} \) represents the inverse of \( f \).

\[ \square \]

5. The Number of Polyfunctions

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

The following lemma characterizes the tuples \( k \) for which \( ax^k \) is (weakly) reducible.

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

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

Proof. (i) We assume, that \( p(x) \) reduces \( ax^k \) weakly. Hence, \( q(x) := ax^k - p(x) \) 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
\[
q(x) = \sum_{\substack{l \in \mathbb{N}_0^d \\mid \|l\| \leq |k|}} q_l x^l \tag{9}
\]
for suitable coefficients \( q_l \in \mathbb{Z}_n \), with \( q_k = a \). Using the linearity of the \( \Delta \) operator, we obtain that, modulo \( n \),
\[
0 = \Delta^k q(x) \stackrel{(9)}{=} \sum_{\substack{l \in \mathbb{N}_0^d \\mid \|l\| \leq |k|}} q_l \Delta^k x^l \stackrel{(4)}{=} ak!.
\]

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

\[ \text{lcm}(M) \text{ is the least common multiple of all integer numbers in a finite set } M. \text{ ord}(x) \text{ denotes the order of an element } x \text{ in a finite multiplicative group } G, \text{ i.e., ord}(x) \text{ is the smallest number } k \in \mathbb{N} \text{ such that } x^k = 1. \]
(ii) We assume, that \( n \mid a^k! \). Then, the polynomial

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

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

\[ \square \]

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

\[
S_d(n) := \{ k \in \mathbb{N}_0^d : n \nmid k! \}
\]

(10)

denote the set of multi-indices \( k \) such that \( ax^k \) is not reducible modulo \( n \). Its cardinality is the natural generalization of the Smarandache function to the case of several variables:

\[
s_d(n) := |S_d(n)|.
\]

(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 \( n \).

<table>
<thead>
<tr>
<th>( n )</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
<th>11</th>
<th>12</th>
<th>13</th>
</tr>
</thead>
<tbody>
<tr>
<td>( s_1 )</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>7</td>
<td>8</td>
<td>9</td>
<td>10</td>
<td>11</td>
<td>12</td>
</tr>
<tr>
<td>( s_2 )</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>7</td>
<td>8</td>
<td>9</td>
<td>10</td>
<td>11</td>
</tr>
<tr>
<td>( s_3 )</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>7</td>
<td>8</td>
<td>9</td>
<td>10</td>
</tr>
<tr>
<td>( s_4 )</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>7</td>
<td>8</td>
<td>9</td>
</tr>
</tbody>
</table>

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,

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

is a normed⁵ 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

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

where $\alpha_{k_i} \in \mathbb{Z}_p$.

**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

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

for the number of factors $p$ in $k!$. Notice that $\nu_p(k!) < i$ if and only if $k \in S_d(p^i)$. 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

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

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

$$\alpha_k = \sum_{\{i \in m : k \in S_d(p^i)\}} p^{m-i} \alpha_{k_i}$$

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

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

---

⁵i.e., its leading coefficient is $1$
Theorem 6 The number of polyfunctions in $G_d(\mathbb{Z}_{p^m})$, $p$ prime, is given by

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

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

$$S_2(2) = \{ (k_1, k_2) : 0 \leq k_1 \leq 1, 0 \leq k_2 \leq 1 \}$$
$$s_2(2) = 4$$

$$S_2(4) = \{ (k_1, k_2) : 0 \leq k_1 \leq 3, 0 \leq k_2 \leq 3, k_1k_2 < 4 \}$$
$$s_2(4) = 12$$

$$S_2(8) = \{ (k_1, k_2) : 0 \leq k_1 \leq 3, 0 \leq k_2 \leq 3 \}$$
$$s_2(8) = 16.$$

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

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

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

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

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

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

Corollary 8 \[ \sum_{i=1}^{m} s_d(p^i) = \sum_{k \in S_d(p^m)} (m - \nu_p(k!)) = m s_d(p^m) - \sum_{k \in S_d(p^m)} \nu_p(k!). \]

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

$$\Psi_d(n) = \Psi_d\left(\prod_{i=1}^{k} p_i^{\nu_p(n_i)}\right) = \prod_{i=1}^{k} \Psi_d(p_i^{\nu_p(n_i)}).$$

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

$$\ln \Psi_d(n) = \sum_{i=1}^{k} \ln \Psi_d(p_i^{\nu_p(n_i)})$$
$$= \sum_{i=1}^{k} \ln p_i \sum_{j=1}^{\nu_p(n_i)} s_d(p_i^j).$$
Observe that the Mangoldt function
\[ \Lambda : \mathbb{N} \to \mathbb{N}, \quad x \mapsto \begin{cases} \ln p & \text{if } x = p^k, \text{ } p \text{ } \text{prime}, \text{ } k \geq 1 \\ 0 & \text{else} \end{cases} \]
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
\[
(f \ast g)(n) = \sum_{d|n} f \left( \frac{n}{d} \right) g(d)
\]
with \( f \equiv 1 \) and \( g = s_d \Lambda \), we arrive at
\[ \ln \Psi_d(n) = (1 \ast (s_d \Lambda))(n). \]
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
\[ \Psi_d(n) = e^{1 \ast (s_d \Lambda)(n)}. \]

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
\[ a_k := s(2^k) - s(2^{k-1}), \quad k = 1, 2, 3, \ldots \]
The sequence starts with
\[
(a_k)_{k \in \mathbb{N}} = (2, 2, \overbrace{0, 2, 2}^{\varepsilon_1}, \overbrace{0, 2, 2}^{\varepsilon_2}, \overbrace{0, 2, 2}^{\varepsilon_3}, \overbrace{0, 2, 0, 0, 2, 2}^{\varepsilon_4}, \overbrace{0, 2}^{\varepsilon_5}, \overbrace{2, 2, \ldots}^{\varepsilon_6}).
\]
Two 2s alternate with groups of $\varepsilon_k$ 0s. The sequence

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

with the property that $2^{\varepsilon_k}$ 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


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


