




Article

Rings of Multisets and Integer Multinumerals

Yuriy Chopiyuk , Taras Vasylyshyn  and Andriy Zagorodnyuk * 

Faculty of Mathematics and Computer Science, Vasyl Stefanyk Precarpathian National University,
57 Shevchenka Str., 76018 Ivano-Frankivsk, Ukraine; ur.chopiuk@gmail.com (Y.C.);
taras.v.vasylyshyn@gmail.com (T.V.)

* Correspondence: andriy.zagorodnyuk@pnu.edu.ua

Abstract: In the paper, we consider a ring structure on the Cartesian product of two sets of integer multisets. In this way, we introduce a ring of integer multinumerals as a quotient of the Cartesian product with respect to a natural equivalence. We examine the properties of this ring and construct some isomorphisms to subrings of polynomials and Dirichlet series with integer coefficients. In addition, we introduce finite rings of multinumerals “modulo (p, q) ” and propose an algorithm for construction of invertible elements in these rings that may be applicable in Public-key Cryptography. An analog of the Little Fermat Theorem for integer multinumerals is proved.

Keywords: set of multisets; multinumerals; supersymmetric polynomials; finite rings; applications in Cryptography

MSC: 11C08; 46G25; 94A60



Citation: Chopiyuk, Y.; Vasylyshyn, T.; Zagorodnyuk, A. Rings of Multisets and Integer Multinumerals. *Mathematics* **2022**, *10*, 778. <https://doi.org/10.3390/math10050778>

Academic Editors: Pavel Trojovský, Iwona Włoch and Štěpán Hubálovský

Received: 27 December 2021

Accepted: 25 February 2022

Published: 28 February 2022

Publisher’s Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.



Copyright: © 2022 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

Permutation-invariant objects naturally appear when we work with a large amount of information that does not depend on the order. Such a situation is typical, for example, in Quantum Statistical Physics, Data Science, Neural-Network Theory (see e.g., [1,2] and references cited therein). A *multiset*, defined as an unordered collection of elements that may be repeated, is a good tool for modeling such objects. Semiring algebraic structures on multisets and their applications for neural networks were considered in [3] (see also [4] for a more general context).

A set of finite multisets can be represented as the quotient set of the linear space Λ of all finite sequences with respect to the following equivalence: two vectors in Λ are equivalent if they are equal to each other up to a permutation of coordinates. Thus, we can consider a finite multiset of nonzero elements $x = \{x_1, \dots, x_n\}$ as a class of the equivalence containing the vector $(x_1, \dots, x_n, 0, \dots) \in \Lambda$. It is possible to introduce some algebraic operations on the set of multisets. We denote by $x \bullet z$ the union of two multisets x and z , and by $x \diamond z$ their product—that is, a multiset consisting of all products $x_i z_j$ of elements x and z . The set of finite multisets is a commutative semiring with respect to these operations [5,6]. The semiring structure is not rich enough. However, since we have a commutative semigroup with the cancellation law with respect to “ \bullet ”, we can apply the Grothendieck construction to embed it to a commutative group and extend the multiplication “ \diamond ” by the distributivity. Such a ring of multisets \mathcal{M}_0 was constructed in [6] using symmetric and supersymmetric polynomials on a Banach space (see also [7]). More details about algebras of symmetric polynomials on Banach spaces can be found in [8–14]. The combinatorial approach to symmetric polynomials can be found in [15]. Discrete dynamic systems based on \mathcal{M}_0 were considered in [16]. Systematic theory of multisets can be found in [17].

In this paper, we consider the subring \mathcal{Z} of \mathcal{M}_0 comprising multisets with positive integer elements. The subring \mathcal{Z} contains an isomorphic copy of the ring of integers and so can be considered as a generalization of integer numbers. We call \mathcal{Z} the *ring of multinumerals*.

We study properties of \mathcal{Z} and some finite rings of multinumbers “modulo (p, q) ”, and propose some applications of the finite rings to Cryptography.

In Section 2, we provide some definitions and preliminary results. In Section 3, we establish basic properties of the ring \mathcal{Z} , construct isomorphisms of \mathcal{Z} to a ring of polynomials of infinitely many variables with entire coefficients, and deduce from here some properties of \mathcal{Z} . Further, we show that \mathcal{Z} is isomorphic to a ring of Dirichlet series with entire coefficients. In Section 4, we introduce finite rings of multinumbers $\mathcal{Z}_{(p,q)}$, which are generalizations of \mathbb{Z}_p . The main result of this section is Theorem 4, where we found some conditions under which an element in $\mathcal{Z}_{(p,q)}$ is invertible. Moreover, an analogue of the Little Fermat Theorem for multinumbers is proved. In Section 5, we propose an algorithm of encryption and decryption involving integer multinumbers.

For more details about applications of Number Theory to Cryptography, we refer the reader to [18–20].

2. Definitions and Preliminaries

Let \mathbb{K} be the notation for one of the following sets: the set of complex numbers \mathbb{C} , the set of integers \mathbb{Z} , or the set of natural numbers \mathbb{N} . Further, we use \mathbb{Z}_+ for the set of nonnegative integers. We denote by $\Lambda_{\mathbb{K}}$ the set of infinite-dimensional vectors $(x_1, x_2, \dots, x_n, 0, 0, \dots)$ —that is, vectors with finitely many nonzero coordinates in \mathbb{K} , and by \mathbb{K}^∞ the set all vectors (infinity sequences) $(x_1, x_2, \dots, x_n, \dots)$, $x_j \in \mathbb{K}$, $j \in \mathbb{N}$. Let us consider the Cartesian product

$$\Lambda_{\mathbb{K}} \times \Lambda_{\mathbb{K}} = \{(y|x) = (\dots, 0, y_m, \dots, y_1|x_1, \dots, x_n, 0, \dots) : x, y \in \Lambda_{\mathbb{K}}\}.$$

For given permutations σ, τ on the set of natural numbers \mathbb{N} and

$$(\dots, 0, y_m, \dots, y_1|x_1, \dots, x_n, 0, \dots) \in \Lambda_{\mathbb{K}}$$

we denote

$$(\tau(\dots, 0, y_m, \dots, y_1)|\sigma(x_1, \dots, x_n, 0, \dots)) = (\dots, 0, y_{\tau(m)}, \dots, y_{\tau(1)}|x_{\sigma(1)}, \dots, x_{\sigma(n)}, 0, \dots).$$

We introduce the following relation of equivalence on $\Lambda_{\mathbb{K}} \times \Lambda_{\mathbb{K}}$. Let $(y|x) = (\dots, 0, y_m, \dots, y_1|x_1, \dots, x_n, 0, \dots)$ and $(y'|x') = (\dots, 0, y'_m, \dots, y'_1|x'_1, \dots, x'_n, 0, \dots)$ in $\Lambda_{\mathbb{K}}$. We say that $(y|x) \sim (y'|x')$ if and only if there are $a = (a_1, \dots, a_k, 0, \dots)$ and $b = (b_1, \dots, b_j, 0, \dots)$ in $\Lambda_{\mathbb{K}}$ and permutations σ and τ on \mathbb{N} such that

$$\begin{aligned} &(\tau(\dots, 0, y_m, \dots, y_1, a_1, \dots, a_k)|\sigma(a_1, \dots, a_k, x_1, \dots, x_n, 0, \dots)) \\ &= (\dots, 0, y'_m, \dots, y'_1, b_1, \dots, b_j|b_1, \dots, b_j, x'_1, \dots, x'_n, 0, \dots). \end{aligned}$$

The quotient set with respect to the equivalence, $\mathcal{M}_0 = (\Lambda_{\mathbb{C}} \times \Lambda_{\mathbb{C}})/\sim$, and its completion in the metric of the absolute convergence \mathcal{M} were considered in [6]. It is easy to see that the class $[(y|x)]$ containing $(y|x)$ is invariant with respect to the minimal semigroup of mappings from $\Lambda_{\mathbb{C}} \times \Lambda_{\mathbb{C}}$ to itself containing operators of permutation of the bases of $\Lambda_{\mathbb{C}}$ separately on each $\Lambda_{\mathbb{C}}$ and affine operators

$$(\dots, 0, y_m, \dots, y_1|x_1, \dots, x_n, 0, \dots) \mapsto (\dots, 0, y_m, \dots, y_1, a_0|a_0, x_1, \dots, x_n, 0, \dots)$$

for every $a_0 \in \mathbb{K}$. Let us denote by \mathcal{Z} the set $(\Lambda_{\mathbb{N}} \times \Lambda_{\mathbb{N}})/\sim$.

Consider the following mappings on $\Lambda_{\mathbb{C}} \times \Lambda_{\mathbb{C}}$ (so-called *supersymmetric polynomials*):

$$T_k(y|x) = \sum_{i=1}^{\infty} x_i^k - \sum_{j=1}^{\infty} y_j^k, \quad k \in \mathbb{Z}_+.$$

Here, for the case $k = 0$, we assume that $0^0 = 0$. In other words, $T_0(y|x) = |\text{supp } x| - |\text{supp } y|$, where $|A|$ is the cardinality of a given set A and $\text{supp } x = \{i \in \mathbb{N} : x_i \neq 0\}$.

It is easy to check that if $(y|x) \sim (y'|x')$, then $T_k(y|x) = T_k(y'|x')$ for every $k \in \mathbb{Z}_+$ because

$$T_k(\dots, 0, y_m, \dots, y_1, a_1, \dots, a_j | a_1, \dots, a_j, x_1, \dots, x_n, 0, \dots) \\ = \sum_{i=1}^n x_n^k + \sum_{i=1}^j a_i^k - \sum_{i=1}^j a_i^k - \sum_{i=1}^m y_i^k = T_k(\dots, 0, y_m, \dots, y_1 | x_1, \dots, x_n, 0, \dots).$$

Next, we will show that the inverse statement is also true.

Using ideas from [6,9,10] introduced algebraic operations of “addition” and “multiplication” on \mathcal{M}_0 . Let $z = (y|x)$, $z' = (y'|x') \in \Lambda_{\mathbb{C}} \times \Lambda_{\mathbb{C}}$, and $[z], [z'] \in \mathcal{M}_0$ be classes that contain z and z' , respectively. Then, we set

$$[z] + [z'] = [z \bullet z'] := [(\dots, y'_n, y_n, \dots, y'_1, y_1 | x_1, x'_1, \dots, x_n, x'_n, \dots)].$$

For every $[z] \in \mathcal{M}_0$ there is an inverse element $-[z]$, defined by $-[(y|x)] = [(x|y)]$. Thus, $(\mathcal{M}_0, +)$ is a commutative group with zero $0 = [(0|0)]$. Clearly, the operations “+” and taking of inverse do not depend on representatives.

In [6] (Theorem 1) it was observed that $[z] = 0$ if and only if $T_k(z) = 0$ for every $k \in \mathbb{Z}_+$. Since $T_k(z \bullet z') = T_k(z) + T_k(z')$, we have the following proposition.

Proposition 1. $z \sim z'$ if and only if $T_k(z) = T_k(z')$ for every $k \in \mathbb{Z}_+$.

For given x and x' in $\Lambda_{\mathbb{C}}$, $x \diamond x'$ denotes the resulting sequence of ordering the set $\{x_i y_j : i, j \in \mathbb{N}\}$ with one single index in some fixed order. So, we can define

$$[z][z'] = [((y \diamond x') \bullet (x \diamond y') | (y \diamond y') \bullet (x \diamond x'))].$$

To check that the multiplication does not depend on representatives, we observe that

$$T_k(z \diamond z') = T_k(z)T_k(z'), \quad k \in \mathbb{Z}_+$$

(see for the proof [6] (Proposition 5)). Thus, if $u \sim z$ and $u' \sim z'$, then $T_k(z \diamond z') = T_k(u \diamond u')$, and so, by Proposition 1, $z \diamond z' \sim u \diamond u'$.

Note that elements of the form $[(0|x)]$ may be considered as finite multisets—that is, unordered collections of numbers with possible repetitions. Let $\mathcal{M}_0^+ = \{[(0|x)] : x \in \Lambda_{\mathbb{C}}\}$. Then, $(\mathcal{M}_0^+, +, \cdot)$ is a commutative semiring. Since its additive semigroup $(\mathcal{M}_0^+, +)$ is cancellative—that is, $z + u = z + v$ implies $u = v$ for all $u, v, z \in (\mathcal{M}_0^+)$ —it follows that it can be isomorphically embedded into some commutative group (so-called *the Grothendieck group*) using a simple Grothendieck idea, which is the starting point of K -theory (see e.g., [21]). From this point of view, (\mathcal{M}_0) is the Grothendieck group, associated with (\mathcal{M}_0^+) .

Often, we will use notations $[(y_m, \dots, y_1 | x_1, \dots, x_n)]$ instead of

$$[(\dots, 0, y_m, \dots, y_1 | x_1, \dots, x_n, 0, \dots)].$$

Theorem 1. (See Theorem 4 and Example 1 in [6]). $(\mathcal{M}_0, +, \cdot)$ is a commutative ring with zero $0 = [(0|0)]$ and unity $\mathbb{1} = [(0|1)]$. Functions $\tau_k : \mathcal{M}_0 \rightarrow \mathbb{C}$,

$$\tau_k([z]) = T_k(z), \quad k \in \mathbb{Z}_+$$

are ring homomorphisms.

Example 1. Let $[z] = [(2| - 1)]$, $[u] = [(1, 2|3)]$, and $[v] = [(-1|1, 2)]$. Then,

$$[u] + [v] = [(1, 2|3)] + [(-1|1, 2)] = [(1, 2, -1|1, 2, 3)] = [(-1|3)];$$

$$\begin{aligned}
 [z]([u] + [v]) &= [(2|-1)][(-1|3)] = [(6,1|-2,-3)]; \\
 [z][u] + [z][v] &= [(2|-1)][(1,2|3)] + [(2|-1)][(-1|1,2)] \\
 &= [(6,-1,-2|2,-3,4)] + [(1,2,4|-2,-1,-2)] = [(6,1|-2,-3)] = [z]([u] + [v]).
 \end{aligned}$$

We call elements in \mathcal{M}_0 by *complex multinumbers*, in \mathcal{Z} by *integer multinumbers*, and in $\mathcal{N} := \{[0|x] : x \in \Lambda_{\mathbb{N}}\}$ by *natural multinumbers*. Note that $\mathcal{N} = \Lambda_{\mathbb{N}} / \sim$ and $(\mathcal{N}, +, \cdot)$ is a semiring of $(\mathcal{Z}, +, \cdot)$.

3. Basic Properties of Multinumbers

Proposition 2. \mathcal{Z} is a subring of \mathcal{M}_0 and functions $\tau_k, k \in \mathbb{Z}_+,$ restricted to \mathcal{Z} , are ring homomorphisms from \mathcal{Z} to \mathbb{Z} .

Proof. Clearly, if $[z]$ and $[z']$ are in \mathcal{Z} , then $[z] + [z'] \in \mathcal{Z}$ and $[z][z'] \in \mathcal{Z}$. So, \mathcal{Z} is a subring. Further, $\tau_k([z]) \in \mathbb{Z}$ if $[z] \in \mathcal{Z}$ and $k \in \mathbb{Z}_+.$ □

We will use notations $\mathbf{n} = (n_1, n_2, \dots)$ for a typical element in $\Lambda_{\mathbb{N}}$ and $\mathbf{v} = [(\mathbf{m}|\mathbf{n})]$ for a typical element in \mathcal{Z} . Let $j \in \mathbb{Z}$. We denote by $j\mathbf{v} = j[(\mathbf{m}|\mathbf{n})] = \underbrace{\mathbf{v} + \dots + \mathbf{v}}_j$ if $j > 0$ and $j\mathbf{v} = (-j)(-\mathbf{v})$ if $j < 0$, where $-\mathbf{v} = [(\mathbf{n}|\mathbf{m})]$. In particular, $j\mathbb{I} = [(0|\underbrace{1, \dots, 1}_j)]$, where $\mathbb{I} = (0|1)$ is the unity in \mathcal{Z} . Note that $j\mathbf{v} \neq [(0|j)]\mathbf{v} = [(\dots, jm_2, jm_1|jn_1, jn_2, \dots)]$.

Proposition 3. The map $j \mapsto j\mathbb{I}$ is an injective homomorphism from \mathbb{Z} into \mathcal{Z} .

Proof. It is easy to check that $(i + j)\mathbb{I} = i\mathbb{I} + j\mathbb{I}$ and $ij\mathbb{I} = i\mathbb{I}j\mathbb{I}$. Further, $i\mathbb{I} \neq j\mathbb{I}$ if $i \neq j.$ □

Thus, we have that \mathcal{Z} contains an isomorphic copy of \mathbb{Z} —that is, we can consider \mathcal{Z} as a generalization of \mathbb{Z} .

Let $\mathbb{Z}[\mathbb{C}^\infty]$ be the ring of formal polynomials over \mathbb{Z} on the set \mathbb{C}^∞ of all sequences of complex numbers—that is, every $Q \in \mathbb{Z}[\mathbb{C}^\infty]$ is of the form

$$Q(t) = Q(t_1, t_2, \dots) = \sum_{n_1, \dots, n_m} c_{n_1, \dots, n_m} t_{n_1}^{k_1} \cdots t_{n_m}^{k_m}$$

for some $m, k_i \in \mathbb{Z}_+, c_{n_1, \dots, n_m} \in \mathbb{Z}$ and the right side series contains a finite number of nonzero terms.

Note that \mathcal{M}_0 has divisors of zero; for example, $[(-1|1)][(0|1, -1)] = 0$. We will show that for \mathcal{Z} , it is not so.

Theorem 2. There is a ring isomorphism $\nu: \mathcal{Z} \rightarrow \mathbb{Z}[\mathbb{C}^\infty]$.

Proof. Let $\{p_n\}_{n=1}^\infty = \{2, 3, 5, \dots\}$ be the sequence of prime numbers. Let $a \in \mathbb{N}$ and $a = p_1^{k_1} \cdots p_n^{k_n}$. We set $\nu_0(a) = t_1^{k_1} \cdots t_n^{k_n} \in \mathbb{Z}[\mathbb{C}^\infty]$. Note that $\nu_0(1) = 1$. Let us define ν by

$$\nu([(\mathbf{m} | \mathbf{n})]) (t) := \sum_i \nu_0(n_i) - \sum_j \nu_0(m_j),$$

where $t = (t_1, t_2, \dots) \in \mathbb{C}^\infty$. If $(\mathbf{m}|\mathbf{n}) \sim (\mathbf{m}'|\mathbf{n}')$, then

$$(\mathbf{m} \bullet \mathbf{a} | \mathbf{n} \bullet \mathbf{a}) = (\mathbf{m}' \bullet \mathbf{b} | \mathbf{n}' \bullet \mathbf{b})$$

for some $\mathbf{a}, \mathbf{b} \in \Lambda_{\mathbb{N}}$; so, $\nu([(\mathbf{m} | \mathbf{n})]) (t) = \nu([(\mathbf{m}' | \mathbf{n}')]) (t)$. Thus, the definition of ν does not depend on the representative.

Clearly, if $[(\mathbf{m}|\mathbf{n})] \neq 0$, then $v([(\mathbf{m}|\mathbf{n})]) (t) \neq 0$ and so v is injective. It is easy to check that v is additive and multiplicative. The preimage of $rt_1^{k_1} \cdots t_n^{k_n}$ is equal to $r[(0|p_1^{k_1} \cdots p_n^{k_n})]$ and $v^{-1}(j) = j\mathbb{I}$ —that is, v is surjective. So, v is an isomorphism. \square

Since $\mathbb{Z}[\mathbb{C}^\infty]$ is an integral domain, we have the following corollary.

Corollary 1. *The ring \mathcal{Z} is an integral domain and every element in \mathcal{Z} has a unique representation by the product of irreducible elements.*

Example 2. *Let us factor the element $[(16|1)]$ into a product of irreducible elements in \mathcal{Z} . By Theorem 2,*

$$v([(16|1)]) (t) = 1 - t_1^4 = (1 - t_1)(1 + t_1)(1 + t_1^2).$$

Thus,

$$[(16|1)] = [(2|1)][(0|1, 2)][(0|1, 4)].$$

Since polynomials $1 - t_1$, $1 + t_1$, and $1 + t_1^2$ are irreducible in $\mathbb{Z}[\mathbb{C}^\infty]$, elements $[(2|1)]$, $[(0|1, 2)]$, and $[(0|1, 4)]$ are irreducible in \mathcal{Z} .

Corollary 2. *For every permutation σ on the set of prime numbers $\sigma: (p_1, p_2, \dots) \mapsto (p_{\sigma(1)}, p_{\sigma(2)}, \dots)$, there exists a ring isomorphism $\Phi_\sigma: \mathcal{Z} \rightarrow \mathcal{Z}$ such that*

$$\Phi_\sigma([(0|p_1^{k_1} \cdots p_n^{k_n}, 0, \dots)]) = [(0|p_{\sigma(1)}^{k_1} \cdots p_{\sigma(n)}^{k_n}, 0, \dots)].$$

Proof. For every permutation σ , the mapping $v \circ \Phi_\sigma \circ v^{-1}$ is a ring isomorphism of $\mathbb{Z}[\mathbb{C}^\infty]$ to itself, since

$$v \circ \Phi_\sigma \circ v^{-1}(Q)(t_1, t_2, \dots) = Q(t_{\sigma(1)}, t_{\sigma(2)}, \dots), \quad Q \in \mathbb{Z}[\mathbb{C}^\infty],$$

and $(t_1, t_2, \dots) \mapsto (t_{\sigma(1)}, t_{\sigma(2)}, \dots)$ is a linear isomorphism of the linear space \mathbb{C}^∞ . Indeed, if $P(t) = v(\mathbf{u})(t)$ and $Q(t) = v(\mathbf{v})(t)$, then

$$\Phi_\sigma(\mathbf{u}\mathbf{v}) = v \circ \Phi_\sigma \circ v^{-1}(P(t)Q(t)) = P(t_{\sigma(1)}, t_{\sigma(2)}, \dots)Q(t_{\sigma(1)}, t_{\sigma(2)}, \dots) = \Phi_\sigma(\mathbf{u})\Phi_\sigma(\mathbf{v}).$$

By the same reason, $\Phi_\sigma(\mathbf{u} + \mathbf{v}) = \Phi_\sigma(\mathbf{u}) + \Phi_\sigma(\mathbf{v})$. \square

Corollary 3. *For every fixed $t \in \mathbb{C}^\infty$ ($t \in \mathbb{Z}^\infty$), there is a ring homomorphism $\psi_t: \mathcal{Z} \rightarrow \mathbb{C}$ (resp. $\psi_t: \mathcal{Z} \rightarrow \mathbb{Z}$) defined by*

$$\psi_t(\mathbf{u}) = v(\mathbf{u})(t). \tag{1}$$

Conversely, any ring homomorphism from \mathcal{Z} to \mathbb{C} (from \mathcal{Z} to \mathbb{Z}) can be defined by (1) for some $t \in \mathbb{C}^\infty$ (resp. $t \in \mathbb{Z}^\infty$).

Proof. It is clear that ψ_t is a homomorphism and the range of ψ_t is in \mathbb{Z} if $t \in \mathbb{Z}^\infty$. Let $\psi: \mathcal{Z} \rightarrow \mathbb{C}$ be a homomorphism. Let us define t by

$$t = (\psi((0|p_1)), \psi((0|p_2)), \dots, \psi((0|p_n)), \dots) \in \mathbb{C}^\infty.$$

Then, $\psi(\mathbf{u}) = v(\mathbf{u})(t) = \psi_t(\mathbf{u})$ for every $\mathbf{u} \in \mathcal{Z}$. If ψ is a homomorphism from \mathcal{Z} to \mathbb{Z} , then $\psi((0|p_n)) \in \mathbb{Z}$ for every n ; so, $t \in \mathbb{Z}^\infty$. \square

Corollary 4. *Let us suppose that $\mathbf{u}_1, \dots, \mathbf{u}_n \in \mathcal{Z}$ and polynomials $v(\mathbf{u}_1)(t), \dots, v(\mathbf{u}_n)(t)$, $t \in \mathbb{C}^\infty$ have no common zeros in \mathbb{C}^∞ . Then, there are $\mathbf{v}_1, \dots, \mathbf{v}_n \in \mathcal{Z}$ and a positive integer j such that*

$$\sum_{k=1}^n \mathbf{u}_k \mathbf{v}_k = j\mathbb{I}.$$

Proof. Let N be a maximal natural number such that polynomials $v(\mathbf{u}_1)(t), \dots, v(\mathbf{u}_n)(t)$ depend on t_1, \dots, t_N . So, $v(\mathbf{u}_1)(t), \dots, v(\mathbf{u}_n)(t)$ have no common zeros in \mathbb{C}^N . By the Hilbert Nullstellensatz, there are polynomials $Q_1(t), \dots, Q_n(t)$ on \mathbb{C}^N such that

$$\sum_{k=1}^n v(\mathbf{u}_k)(t)Q_k(t) = 1 \quad \forall t \in \mathbb{C}^N.$$

Since all polynomials $v(\mathbf{u}_k) \in \mathbb{Z}[t_1, \dots, t_N] \subset \mathbb{Q}[t_1, \dots, t_N]$, polynomials Q_k are in $\mathbb{Q}[t_1, \dots, t_N]$ [22] (Ch. VII, Theorem 14)—that is, all coefficients of Q_k are rational numbers. Let j be the common denominator of all coefficients of all $Q_k, k = 1, \dots, n$. Then, we can write

$$\sum_{k=1}^n v(\mathbf{u}_k)(t)P_k(t) = j,$$

where $P_k = jQ_k \in \mathbb{Z}[t_1, \dots, t_N]$. Setting $\mathbf{v}_k = v^{-1}(P_k), k = 1, \dots, n$, we have the required identity. \square

Example 3. Let $\mathbf{u} = [(0|1, 1, 2)]$ and $\mathbf{v} = [(0|1, 2, 2)]$. Then, $v(\mathbf{u})(t) = 2 + t_1$ and $v(\mathbf{v})(t) = 1 + 2t_1$ have no common zeros. Clearly, $2v(\mathbf{u}) - v(\mathbf{v}) = 3$. Hence,

$$2\mathbf{u} - \mathbf{v} = 3\mathbb{I}, \quad \text{that is, } [(0|1, 1)][(0|1, 1, 2)] + [(1|0)][(0|1, 2, 2)] = [(0|1, 1, 1)].$$

Note that elements of the form $j\mathbb{I}, j > 1$, are not invertible even in the ring of multisets \mathcal{M} [6] (Proposition 10).

Let us denote

$$D(\mathbf{u}_1, \dots, \mathbf{u}_n) = \mathbf{a}_1\mathbf{u}_1^{k_1} + \dots + \mathbf{a}_n\mathbf{u}_n^{k_n},$$

for some fixed $\mathbf{a}_1, \dots, \mathbf{a}_n \in \mathcal{Z}$ and $k_1, \dots, k_n \in \mathbb{N}$. We say that the equation

$$D(\mathbf{u}_1, \dots, \mathbf{u}_n) = 0$$

is a Diophantine equation for undetermined multinumbers $\mathbf{u}_1, \dots, \mathbf{u}_n$.

Example 4. Let us solve the following equation

$$[(0|1, 3)]\mathbf{u} = [(1, 3|2, 6)].$$

By Theorem 2,

$$v([(0|1, 3)])(t)v(\mathbf{u})(t) = v([(1, 3|2, 6)])(t)$$

and so,

$$(t_2 + 1)v(\mathbf{u})(t) = t_1 + t_1t_2 - t_2 - 1,$$

$$v(\mathbf{u})(t) = \frac{t_1 + t_1t_2 - t_2 - 1}{t_2 + 1} = t_1 - 1.$$

Hence, $\mathbf{u} = v^{-1}(t_1 - 1) = [(1|2)]$.

The following proposition is obvious.

Proposition 4. If a Diophantine equation $D(\mathbf{u}_1, \dots, \mathbf{u}_n) = 0$ has a solution $(\mathbf{v}_1, \dots, \mathbf{v}_n)$, then $(\phi(\mathbf{v}_1), \dots, \phi(\mathbf{v}_n))$ is a solution of the following Diophantine equation in integers

$$\phi(\mathbf{a}_1)\phi(\mathbf{u}_1)^{k_1} + \dots + \phi(\mathbf{a}_n)\phi(\mathbf{u}_n)^{k_n} = 0$$

for every homomorphism $\phi: \mathcal{Z} \rightarrow \mathbb{Z}$.

From this proposition, in particular, it follows that if a Diophantine equation has no solution in \mathbb{Z} , then it has no solution in \mathcal{Z} .

Another representation of \mathcal{Z} can be given by a ring of finite Dirichlet series. Let us recall that a formal series of the form

$$d(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}, \quad a_n, s \in \mathbb{C},$$

is a Dirichlet series. We denote by $\mathcal{D}_0(\mathbb{Z})$ the subset of finite Dirichlet series with coefficients $a_n \in \mathbb{Z}$. Clearly, $\mathcal{D}_0(\mathbb{Z})$ is a ring with respect to usual addition and multiplication. The next proposition follows from direct calculations.

Proposition 5. *The following map is a ring isomorphism from \mathcal{Z} to $\mathcal{D}_0(\mathbb{Z})$*

$$\Psi: [(m|n)] \mapsto \sum_i \frac{1}{n_i^s} - \sum_j \frac{1}{m_j^s}.$$

Combining isomorphisms Ψ and ν , we can see that $\Psi \circ \nu^{-1}$ is a ring isomorphism from $\mathbb{Z}[C^\infty]$ to $\mathcal{D}_0(\mathbb{Z})$,

$$\Psi \circ \nu^{-1}: mt_1^{k_1} \dots t_r^{k_r} \mapsto \frac{m}{(p_1^{k_1} \dots p_r^{k_r})^s}.$$

Such an isomorphism is well-known in a more general context and is called the Borh transform. It can be extended to a map

$$\sum_n a_n z_1^{k_1} \dots z_r^{k_r} \mapsto \sum_n \frac{a_n}{n^s},$$

where $n = p_1^{k_1} \dots p_r^{k_r}$, $a_n \in \mathbb{C}$, $(z_1, z_2, \dots) \in c_0$, and is an isomorphism from the algebra $H_\infty(B_{c_0})$ of bounded holomorphic functions on the unit ball of the Banach space c_0 of convergent to zero sequences to the Banach algebra \mathcal{H}^∞ of Dirichlet series $d(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}$ such that

$$\|d\| = \sup_{\text{Re}(s) > 0} |d(s)| < \infty$$

(see for details [23] (p. 85)). Thus, from Corollary 4, we have the following result.

Corollary 5. *Let us suppose that $d_1, \dots, d_n \in \mathcal{D}_0$ are such that polynomials $\nu \circ \Psi^{-1}(d_1)(t), \dots, \nu \circ \Psi^{-1}(d_n)(t)$ have no common zeros in \mathbb{C}^∞ . Then, there are $b_1, \dots, b_n \in \mathcal{D}_0$ and a positive integer j such that*

$$\sum_{k=1}^n b_k(s) d_k(s) = j.$$

Example 5. *Let $\mathbf{u} = [(0|1, 1, 2)]$ and $\mathbf{v} = [(0|1, 2, 2)]$ as in Example 3. Then,*

$$2\Psi(\mathbf{u}) - \Psi(\mathbf{v}) = 2\left(2 + \frac{1}{2^s}\right) - \left(1 + \frac{2}{2^s}\right) = 3.$$

4. Finite Rings of Multinumerals

Let p, q be natural numbers. Let us consider the following relation of equivalence “modulo (p, q) ” on \mathcal{Z} defined by

$$[(\dots, m_2^{\bullet\{r\}}, m_1^{\bullet\{s\}} | n_1^{\bullet\{k\}}, n_2^{\bullet\{i\}}, \dots)] \approx [(0 | m_1^{\bullet\{s'\}}, m_2^{\bullet\{r'\}}, \dots, n_1^{\bullet\{k'\}}, n_2^{\bullet\{i'\}}, \dots)],$$

where $n^{\bullet\{k\}} = \underbrace{n, \dots, n}_k$, and $n'_j \equiv n_j \pmod q$, $m'_j \equiv m_j \pmod q$, $k' \equiv k \pmod p$, $i' \equiv i \pmod p$, $r' \equiv -r \pmod p$, $s' \equiv -s \pmod p$. In other words, entries n_j and m_j are in \mathbb{Z}_q and the number of repetitions of any number n_j or m_j is in \mathbb{Z}_p . For example, for every $0 < n < q$, we have

$$[(0|\underbrace{n, \dots, n}_k)] \approx [(0|\underbrace{n, \dots, n}_i)] \approx [(\underbrace{n, \dots, n}_s|0)],$$

if $k \equiv i \pmod p$ and $k \equiv -s \pmod p$.

Let us denote by $\mathcal{Z}_{(p,q)}$ the set of classes of the equivalence. In sequel, we always assume that $p > 1$ and $q > 1$. Since every element in $\mathcal{Z}_{(p,q)}$ has a representative of the form

$$[(0|\mathbf{n})] = [(0|n_1, n_2, \dots)],$$

we will use the notation (n_1, n_2, \dots) for the class containing $[(0|\mathbf{n})]$. Moreover, to simplify notation, we will write

$$(\underbrace{n_1, \dots, n_1}_k, \underbrace{n_2, \dots, n_2}_i, \dots) = (n_1^{\bullet\{k\}}, n_2^{\bullet\{i\}}, \dots) = k(n_1) + i(n_2) + \dots.$$

Proposition 6. $\mathcal{Z}_{(p,q)}$ has the following properties:

- (i) $\mathcal{Z}_{(p,q)}$ is a finite commutative ring with the unity $\mathbb{I} = (1)$. The cardinality of $\mathcal{Z}_{(p,q)}$ is $|\mathcal{Z}_{(p,q)}| = p^{q-1}$
- (ii) $\mathcal{Z}_{(p,2)}$ is isomorphic to \mathbb{Z}_p .
- (iii) The mapping

$$\begin{aligned} \mathcal{I}_{(p,q)}: \mathcal{Z} &\longrightarrow \mathcal{Z}_{(p,q)} \\ \mathcal{Z} \ni [(\mathbf{m}|\mathbf{n})] &\mapsto [(\mathbf{m}|\mathbf{n})] \in \mathcal{Z}_{(p,q)} \end{aligned}$$

is a ring homomorphism.

Proof. (i). From the definition of $\mathcal{Z}_{(p,q)}$, one can see that it is closed with respect to the algebraic operations. The properties of these operations (the associativity, the commutativity, the distributivity law) can be checked by the same way as in the case \mathcal{Z} . Every element in $\mathcal{Z}_{(p,q)}$ can be written as

$$(1^{\bullet\{k_1\}}, 2^{\bullet\{k_2\}}, \dots, (q-1)^{\bullet\{k_{q-1}\}}) = k_1(1) + k_2(2) + \dots + k_{q-1}(q-1), \quad 0 \leq k_j < p,$$

where $m^{\bullet\{0\}} = 0$. Thus, the number of such elements is equal to the number of all multi-subsets of the multiset

$$(1^{\bullet\{p-1\}}, 2^{\bullet\{p-1\}}, \dots, (q-1)^{\bullet\{p-1\}}).$$

It is well-known in Combinatorics that such a number is equal to p^{q-1} (e.g., see [24] for a more general case).

(ii). Every element in $\mathcal{Z}_{(p,2)}$ can be represented by

$$k\mathbb{I} = (1^{\bullet\{k\}}) = (\underbrace{1, \dots, 1}_k, 0, \dots),$$

$0 \leq k < p$, and the correspondence $k\mathbb{I} \mapsto k$ is the required isomorphism onto \mathbb{Z}_p .

(iii). It is well-known that the mapping $\mathcal{I}_p: n \mapsto (n \pmod p)$ is a ring homomorphism from \mathbb{Z} to \mathbb{Z}_p .

Let

$$\mathbf{u} = [(\dots, m_2^{\bullet\{r\}}, m_1^{\bullet\{s\}} | n_1^{\bullet\{k\}}, n_2^{\bullet\{i\}}, \dots)] \in \mathcal{Z}_{(p,q)},$$

then

$$\mathcal{I}_{(p,q)}(\mathbf{u}) = [(\dots, \mathcal{I}_p(m_2)^{\bullet\{\mathcal{I}_q(r)\}}, \mathcal{I}_p(m_1)^{\bullet\{\mathcal{I}_q(s)\}} | \mathcal{I}_p(n_1)^{\bullet\{\mathcal{I}_q(k)\}}, \mathcal{I}_p(n_2)^{\bullet\{\mathcal{I}_q(i)\}}, \dots)].$$

By the additivity and the multiplicativity of maps $\mathcal{I}_p(k)$ and $\mathcal{I}_q(k)$, using routine calculations, we have that $\mathcal{I}_{(p,q)}(\mathbf{uv}) = \mathcal{I}_{(p,q)}(\mathbf{u})\mathcal{I}_{(p,q)}(\mathbf{v})$ and $\mathcal{I}_{(p,q)}(\mathbf{u} + \mathbf{v}) = \mathcal{I}_{(p,q)}(\mathbf{u}) + \mathcal{I}_{(p,q)}(\mathbf{v})$ for all $u, v \in \mathcal{Z}_{(p,q)}$. \square

Next, we consider the following question: *Under which conditions is an element $\mathbf{n} \in \mathcal{Z}_{(p,q)}$ invertible in $\mathcal{Z}_{(p,q)}$?*

It is easy to find divisors of zero in $\mathcal{Z}_{(p,q)}$. For example,

$$(1, 2)(1, 2) = (1, 2, 2, 1) = 0 \text{ in } \mathcal{Z}_{(2,3)}.$$

Theorem 3. *The ring $\mathcal{Z}_{(p,q)}$ is a field if and only if $q = 2$ and p is a prime number. In this case, the field is isomorphic to \mathbb{Z}_p .*

Proof. The case $q = 2$ is considered in Proposition 6. If $q > 2$, then $(1, q - 1) \neq (1, 1)$ and $(1, q - 1) \neq 0$. We claim that, in this case, $(1, q - 1)$ is not invertible. Indeed,

$$(1, q - 1)(1, q - 1) = (1, 1, q - 1, q - 1) = (1, q - 1)(1, 1).$$

So, if $\mathbf{n}_0 = (1, q - 1)^{-1}$, then

$$\mathbf{n}_0(1, q - 1)(1, q - 1) = \mathbf{n}_0(1, q - 1)(1, 1), \quad \text{that is, } (1, q - 1) = (1, 1).$$

This is a contradiction. \square

Clearly, elements $(k) = [(0|k, 0, \dots, 0)]$, where k is coprime with q , are “trivial” examples of invertible elements in $\mathcal{Z}_{(p,q)}$. Indeed, if $kr \equiv 1 \pmod q$, then $(k)(r) = (1) = \mathbb{I}$. Other “trivial” examples of invertible elements in $\mathcal{Z}_{(p,q)}$ are $m\mathbb{I} = (1^{\bullet\{m\}})$ if m is coprime with p . Let us show that there are nontrivial invertible elements.

Example 6. *In $\mathcal{Z}_{(2,4)}$, we have*

$$(2, 3)(2, 3) = (4, 6, 6, 9) = (9) = (1).$$

That is, $(2, 3)$ is invertible.

Theorem 4. *Let p be a prime number. Suppose that \mathbf{m} is invertible in $\mathcal{Z}_{(p,q)}$ and \mathbf{k} is such that $\mathbf{k}^p = 0$ in $\mathcal{Z}_{(p,q)}$ for some $q \in \mathbb{N}$. Then, $\mathbf{m} + \mathbf{k}$ is invertible in $\mathcal{Z}_{(p,q)}$ and*

$$(\mathbf{m} + \mathbf{k})^{-1} = (\mathbf{m} + \mathbf{k})^{p-1}(\mathbf{m}^{-1})^p.$$

Proof.

$$(\mathbf{m} + \mathbf{k})^p = \sum_{j=0}^p \binom{p}{j} \mathbf{m}^j \mathbf{k}^{p-j}.$$

Since p is prime, coefficients $\binom{p}{j} = \frac{p!}{j!(p-j)!}$, $0 < j < p$ are divisible by p and so

$$\binom{p}{j} \mathbf{m}^j \mathbf{k}^{p-j} = 0 \text{ in } \mathcal{Z}_{(p,q)}, \quad 0 < j < p.$$

Hence,

$$(\mathbf{m} + \mathbf{k})^p = \mathbf{m}^p + \mathbf{k}^p = \mathbf{m}^p$$

since $\mathbf{k}^p = 0$ in $\mathcal{Z}_{(p,q)}$. However, \mathbf{m} is invertible. Thus,

$$(\mathbf{m} + \mathbf{k}) \left[(\mathbf{m} + \mathbf{k})^{p-1} (\mathbf{m}^{-1})^p \right] = \mathbb{I}.$$

□

Corollary 6. Let p be a prime number. Suppose that \mathbf{m} is invertible in $\mathcal{Z}_{(p,q)}$ and $k \in \mathbb{N}$ is such that $k^p \equiv 0 \pmod q$ for some $q \in \mathbb{N}$. Then, $\mathbf{m} + (k)$ is invertible in $\mathcal{Z}_{(p,q)}$ and

$$(\mathbf{m} + (k))^{-1} = (\mathbf{m} + (k))^{p-1} (\mathbf{m}^{-1})^p. \tag{2}$$

The corollary is a partial case of Theorem 4 for $\mathbf{k} = (k)$. For given p and k , we can find q satisfying the condition $k^p \equiv 0 \pmod q$. It is enough to set $q = h_1^{r_1} h_2^{r_2} \cdots h_i^{r_i}$, where $ch_1 h_2 \cdots h_i = k < q$ for some $c \in \mathbb{N}$ and $0 < r_j \leq p, j = 1, \dots, i$. In particular, we have the following corollary.

Corollary 7. Let $n \in \mathbb{N}, n > 1$, and p be a prime number. Suppose that \mathbf{m} is invertible in $\mathcal{Z}_{(p,n^p)}$ and $k \in \mathbb{N}$ is such that $k^p \equiv 0 \pmod n^p$. Then, $\mathbf{m} + (k)$ is invertible in $\mathcal{Z}_{(p,n^p)}$ and $(\mathbf{m} + (k))^{-1}$ can be computed by (2).

Corollary 8. Let $n \in \mathbb{N}, n > 1$, and p be a prime number. Then,

1. The multinumber $\mathbf{u} = (n, n^p - 1)$ is invertible in $\mathcal{Z}_{(p,n^p)}$ and $\mathbf{u}^p = (-1)^p$.
2. If $p \neq 2$, then $\mathbf{v} = (n, 1)$ is invertible in $\mathcal{Z}_{(p,n^p)}$ and $\mathbf{v}^p = (1)$.

Proof. Clearly, $(k) = (n)$ is such that $(k)^p = 0$ in $\mathcal{Z}_{(p,n^p)}$ and both $\mathbf{m} = (1)$ and $\mathbf{m} = (n^p - 1)$ are invertible. □

Since a product of invertible elements is invertible, we have the following corollary.

Corollary 9. Let $n \in \mathbb{N}$ and p be a prime number. Then, multinumbers $(n, n^p - 1)^m (n, 1)^k, m, k < p$ are invertible in $\mathcal{Z}_{(p,n^p)}$.

Let us recall that according to the Euler Theorem, if n is coprime with p , then

$$n^{\varphi(p)} \equiv 1 \pmod p,$$

where $\varphi(p)$ is the Euler totient function counting integers between 0 and p , which are coprime with $p \in \mathbb{N}$. If p is a prime number, then $\varphi(p) = p - 1$ and we have the Little Fermat Theorem $n^{p-1} \equiv 1 \pmod p$. The following theorem can be considered a generalization of the Little Fermat Theorem for multinumbers.

Theorem 5. Let p be a prime number and $0 \neq \mathbf{n} = (n_1, n_2, \dots, n_k) \in \mathcal{Z}_{(p,p)}$. Then,

1. $\mathbf{n}^p = \mathbf{n}$.
2. If \mathbf{n} is invertible, then $\mathbf{n}^{p-1} = (1)$ in $\mathcal{Z}_{(p,p)}$.

Proof. Since $\mathbf{n} = (n_1, n_2, \dots, n_k) = (n_1) + (n_2) + \cdots + (n_k)$, we can write

$$\begin{aligned} \mathbf{n}^p &= ((n_1) + (n_2) + \cdots + (n_k))^p = \sum_{r_1 + \cdots + r_k = p} \frac{p!}{r_1! \cdots r_k!} (n_1)^{r_1} \cdots (n_k)^{r_k} \\ &= (n_1^p) + (n_2^p) + \cdots + (n_k^p) + \sum_{r_1 + \cdots + r_k = p, r_j \neq p} \frac{p!}{r_1! \cdots r_k!} (n_1)^{r_1} \cdots (n_k)^{r_k}. \end{aligned}$$

Since p is prime, $\frac{p!}{r_1! \cdots r_k!} (n_1)^{r_1} \cdots (n_k)^{r_k}$ is divisible by p for $r_j < p, j = 1, \dots, k$ and so it is equal to zero in $\mathcal{Z}_{(p,p)}$. Moreover, by the Little Fermat Theorem, $n_j^p \equiv n_j \pmod p$. Thus,

$$\mathbf{n}^p = (n_1) + (n_2) + \cdots + (n_k) = \mathbf{n}.$$

If \mathbf{n} is invertible, then $\mathbf{n}^{p-1} = \mathbf{n}\mathbf{n}^{-1} = (1)$. \square

Note that (n_1, n_2, \dots, n_k) is not necessarily invertible. For example, $(1, 2)$ is not invertible in $\mathcal{Z}_{3,3}$ because $(1, 1, 2)(1, 2) = 0$ but $(1, 2)^3 = (1, 2)$. So, it is naturally to ask the following: *Under which conditions is (n_1, n_2, \dots, n_k) invertible in $\mathcal{Z}_{(p,p)}$?* From Theorem 5, we have a criterium of invertibility of (n_1, n_2, \dots, n_k) in $\mathcal{Z}_{(p,p)}$.

Corollary 10. *Let p be a prime number and $\mathbf{n} = (n_1, n_2, \dots, n_k) \in \mathcal{Z}_{(p,p)}$. Then, \mathbf{n} is invertible if and only if $\mathbf{n}^{p-1} = (1)$ in $\mathcal{Z}_{(p,p)}$.*

Proof. Indeed, if $\mathbf{n}^{p-1} = (1)$, then $\mathbf{n}^{p-2} = \mathbf{n}^{-1}$. \square

Example 7. *The multinumber $(1, 2)$ is not invertible in $\mathcal{Z}_{(5,5)}$ because*

$$(1, 2)^4 = (1^{\bullet\{2\}}, 2^{\bullet\{4\}}, 3^{\bullet\{4\}}, 4) \neq (1),$$

but $(1, 2, 3)$ is invertible in $\mathcal{Z}_{(5,5)}$ because $(1, 2, 3)^4 = (1)$, and so, $(1, 2, 3)^{-1} = (1, 2, 3)^3$.

The question about possible extension of the Euler Theorem looks more complicated.

Example 8. *Let $\mathbf{n} = (1, 5) \in \mathcal{Z}_{(6,6)}$. Then $\mathbf{n}^2 = (1^{\bullet\{2\}}, 5^{\bullet\{2\}})$ and $\mathbf{n}^3 = (1^{\bullet\{4\}}, 5^{\bullet\{4\}}) \neq (1, 5)$. Thus, $\mathbf{n}^{\varphi(6)+1} = \mathbf{n}^3 \neq \mathbf{n}$ in this case while both pairs 1, 6 and 5, 6 are coprime numbers. On the other hand, $(1^{\bullet\{3\}}, 5^{\bullet\{2\}})^3 = (1^{\bullet\{3\}}, 5^{\bullet\{2\}})$, $(1^{\bullet\{2\}}, 5^{\bullet\{2\}})^3 = (1^{\bullet\{2\}}, 5^{\bullet\{2\}})$, $(1^{\bullet\{3\}}, 5^{\bullet\{3\}})^3 = (1^{\bullet\{3\}}, 5^{\bullet\{3\}})$, $(1^{\bullet\{4\}}, 5^{\bullet\{5\}})^3 = (1^{\bullet\{4\}}, 5^{\bullet\{5\}})$.*

Conditions of Theorem 4 show that it is important to know nilpotent elements in $\mathcal{Z}_{(p,q)}$. Moreover, structures of nilpotent ideals in a given ring are important for studying of the ring (see e.g., [25,26]). Next, the corollary shows that there are no nilpotent elements in $\mathcal{Z}_{(p,p)}$ if p is prime.

Corollary 11. *Let p be a prime number. Then, $\mathcal{Z}_{(p,p)}$ has no nonzero nilpotent elements.*

Proof. Let $\mathbf{n}^k = 0$ for some k . Since by Theorem 5, $\mathbf{n}^p = \mathbf{n}$ without loss of generality, we can assume that $k \leq p$. Then,

$$\mathbf{n} = \mathbf{n}^p = \mathbf{n}^{k+p-k} = 0\mathbf{n}^{p-k} = 0.$$

Hence, $n = 0$. \square

Note that even if both p and q are primes, $\mathcal{Z}_{(p,q)}$ still may have nilpotent elements. For example, as we already observed, $(1, 2)^2 = 0$ in $\mathcal{Z}_{(2,3)}$.

5. Possible Applications to Cryptography

The idea of open encryption in Cryptography is based on the fact that some operations are difficult for computing. For example, for an integer a , it is difficult to compute a^{-1} modulo p if a and p are big enough. In the case where a and p are multinumbers, the algorithm for finding the inverse could be more complicated because integer numbers are partial cases of integer multinumbers. Thus, we can consider the following protocol of encryption and decryption involving integer multinumbers.

1. Let $\mathbf{n} = (n_1, n_2, \dots, n_l)$ be a natural multinumber, coding a secret message $a = (a_1, a_2, \dots, a_s)$ by an open code.
2. Randomly choose a prime number p and a number q such that $p > l$ and $q > \max_{j \leq l} n_j$.
3. We consider three possible cases:
 - a. both numbers p and q are secret;
 - b. both numbers p and q are public;
 - c. either p or q is secret.
4. Generate two random keys: a public key \mathbf{u} and private key $\mathbf{v} = \mathbf{u}^{-1}$ in $\mathcal{Z}_{(p,q)}$ using Theorem 4 and corollaries after the theorem.
5. To encrypt, find $\mathbf{w} := \mathbf{n}\mathbf{u}$ and reduce each component of \mathbf{w} modulo q if q is public, and the number of repetitions of each component of \mathbf{w} modulo p if p is public.
6. To decrypt, find $\mathbf{w}\mathbf{v}$ and reduce it modulo (p, q) —that is, $\mathbf{n} = \mathcal{I}_{(p,q)}(\mathbf{w}\mathbf{v})$.

Let us explain some steps. We suppose that the secret message a in (1) is a vector with nonnegative integer coordinates. Let us construct the multinumber $\mathbf{n} = (n_1, n_2, \dots, n_l)$ coding a by the following way:

$$\mathbb{Z}_+^s \ni (a_1, a_2, \dots, a_s) \mapsto (\underbrace{1, \dots, 1}_{a_1}, \underbrace{2, \dots, 2}_{a_2}, \dots, \underbrace{s, \dots, s}_{a_s}) \in \mathcal{N}.$$

For example, if $a = (1, 0, 0, 1, 1)$, then $\mathbf{n} = (1, 4, 5)$; if $a = (0, 1, 1, 2, 0, 1, 2)$, then $\mathbf{n} = (2, 3, 4, 4, 6, 7, 7)$.

Formally, \mathbf{n} belongs to $\mathcal{N} \subset \mathcal{Z}$ and we will use the operator $\mathcal{I}_{(p,q)}$ as in Proposition 6 to reduce it modulo (p, q) . Further, we need operations of partial reductions. Define

$$\mathcal{I}_{(p,\cdot)}(n_1^{\bullet\{i_1\}}, n_2^{\bullet\{i_2\}}, \dots, n_l^{\bullet\{i_l\}}) = (n_1^{\bullet\{\mathcal{I}_p(i_1)\}}, n_2^{\bullet\{\mathcal{I}_p(i_2)\}}, \dots, n_l^{\bullet\{\mathcal{I}_p(i_l)\}})$$

and

$$\mathcal{I}_{(\cdot,q)}(n_1^{\bullet\{i_1\}}, n_2^{\bullet\{i_2\}}, \dots, n_l^{\bullet\{i_l\}}) = (\mathcal{I}_q(n_1)^{\bullet\{i_1\}}, \mathcal{I}_q(n_2)^{\bullet\{i_2\}}, \dots, \mathcal{I}_q(n_l)^{\bullet\{i_l\}}).$$

Here, \mathcal{I}_p is the homomorphism from \mathbb{Z} to \mathbb{Z}_p , $\mathcal{I}_p(n) = n \pmod p$. Clearly,

$$\mathcal{I}_{(p,q)} = \mathcal{I}_{(p,\cdot)} \circ \mathcal{I}_{(\cdot,q)}.$$

Let us consider step (2). Firstly, we randomly choose a big enough prime number p taking into account that $p > l$. To choose q , let us randomly select finite sequences of natural numbers $h_1, h_2, \dots, h_i; r_1, r_2, \dots, r_i$; and c_1, c_2, \dots, c_s such that $r_j \leq p, q := h_1^{r_1} h_2^{r_2} \dots h_i^{r_i} > n_j$ for every $1 \leq j \leq l$, and $k_t := c_t h_1 h_2 \dots h_i < q, 1 \leq t \leq s$. Moreover, we randomly select a natural number $m < p$ and set $\mathbf{m} := m\mathbb{1} = (1, \dots, 1)$. Since p is prime, \mathbf{m} is invertible and, according to the Little Fermat Theorem, $\mathbf{m}^{-1} = m^{p-2}\mathbb{1}$. As q divides $k_1^p, k_1^p \equiv 0 \pmod q$, and by Theorem 4, $\mathbf{m} + (k_1)$ is invertible. By the same reason, $k_2^p \equiv 0 \pmod q$, and so, $\mathbf{m} + (k_1) + (k_2)$ is invertible. Thus, applying Theorem 4 s times, we will obtain that

$$\mathbf{u} = \mathbf{m} + (k_1) + (k_2) + \dots + (k_s)$$

is invertible. In each step, we have the inverses $(\mathbf{m} + (k_1) + (k_2) + \dots + (k_t))^{-1}$, and at step $t = s$, we will obtain $\mathbf{v} = \mathbf{u}^{-1}$.

Note that we can repeat this process for the same p and q but with different constants m, r_i , and c_j to obtain another invertible element in $\mathcal{Z}_{(p,q)}$. The product of two invertible elements is invertible; so, the final key may be obtained as a product of several invertible multinumbers obtained by the algorithm above.

If both p and q are secret, then the encrypted code is of the form $\mathbf{w} = \mathbf{nu} \in \mathcal{N}$. Using Theorem 2, we can represent it as a product of polynomials of many variables

$$v(\mathbf{w})(t) = v(\mathbf{n})(t)v(\mathbf{u})(t).$$

Since $v(\mathbf{u})(t)$ is known, one can recover the secret information by dividing

$$v(\mathbf{n})(t) = \frac{v(\mathbf{w})(t)}{v(\mathbf{u})(t)}$$

using known division algorithms for multivariable polynomials. Thus, case 3a is not secure.

Suppose that both p and q are public. Then, the encrypted code is $\mathcal{I}_{(p,q)}(\mathbf{w}) = \mathcal{I}_{(p,q)}(\mathbf{n})\mathcal{I}_{(p,q)}(\mathbf{u}) \in \mathcal{Z}_{(p,q)}$. The operator $\mathcal{I}_{(p,q)}$ is not invertible, so the previous method of attack is not effective. However, one can consider the sequence $\mathcal{I}_{(p,q)}(\mathbf{n}) [\mathcal{I}_{(p,q)}(\mathbf{u})]^j$ for j big enough. It is well-known in Ring Theory that there is $j = N$ such that

$$\mathcal{I}_{(p,q)}(\mathbf{n}) [\mathcal{I}_{(p,q)}(\mathbf{u})]^N = \mathcal{I}_{(p,q)}(\mathbf{n})\mathcal{I}_{(p,q)}(\mathbf{u}).$$

Then, for the step $j = N - 1$, we have the secret information $\mathbf{n} = \mathcal{I}_{(p,q)}(\mathbf{n})$. So, case 3b is also not secure.

Before we turn to case 3c, let us consider what happens in the classical situation in \mathbb{Z}_p . If p is prime, then

$$a \mapsto a \pmod p = \mathcal{I}_p(a)$$

is a one-way function that is injective for $a < p$. Thus, the encryption $a \mapsto au \pmod p$ cannot be broken if p is secret. However, in this case, we have no public key and so the public-key cryptography system cannot be realized. If p is public, then the system may be attacked, as in case 3b.

In the well-known RSA algorithm [20] (p. 185), the encryption function is defined by

$$a \mapsto a^b \pmod p,$$

where b and $\varphi(p)$ are coprime and p is not a prime number. To obtain the inverse function, it is necessary to compute the Euler function $\varphi(p)$, which is equivalent to factoring p into prime numbers. The proposed algorithm is not a precise analog of the RSA algorithm because we do not have a good multinumber version of the Euler Theorem. However, case 3c allows us to use one-way functions

$$\mathbf{n} \mapsto \mathcal{I}_{(p,\cdot)}(\mathbf{nu}) \quad \text{or} \quad \mathbf{n} \mapsto \mathcal{I}_{(\cdot,q)}(\mathbf{nu})$$

having either p or q as a public key. As we can see in the following example, one must take care that \mathbf{nu} is big enough in some sense.

Example 9. Let a secret information be coded by the vector $a = (0, 1, 1, 2, 0, 1, 2)$. Then, the corresponding multinumber \mathbf{n} is $(2, 3, 4, 4, 6, 7, 7) \in \mathcal{N}$. We can take $p = 3$ and $q = 9$. It is easy to check that $\mathbf{u} = (1, 3)$ is invertible in $\mathcal{Z}_{(3,9)}$ and so we can choose it as a public key. The inverse element $\mathbf{v} = \mathbf{u}^{-1} = (1, 3, 3)$ is the private key.

Case 1. Let us consider the case when p is secret and q is public. Then, actually, the private key is the pair \mathbf{v}, p . For encoding, we have to make the multiplication $\mathbf{w} = \mathbf{nu} \in \mathcal{N}$ and reduce each component of the multinumber \mathbf{w} modulo $q = 9$. That is,

$$\mathbf{w} = \mathbf{nu} = (2, 3, 4, 4, 6, 6, 7, 7, 9, 12, 12, 18, 21, 21);$$

$$\mathcal{I}_{(\cdot,9)}(\mathbf{w}) = (2, 3, 3, 3, 3, 3, 4, 4, 6, 6, 7).$$

Thus, $\mathcal{I}_{(\cdot,9)}(\mathbf{w})$ is the encoded message. To decode it, one must reduce the number of repetitions of each component modulo $p = 3$ and to multiply the result by $\mathbf{v} = (1, 3, 3)$ in $\mathcal{Z}_{(3,9)}$. So,

$$\mathcal{I}_{(3,\cdot)}((2, 3, 3, 3, 3, 3, 4, 4, 6, 6, 7)) = (2, 3, 3, 4, 4, 6, 6, 7);$$

$$(2, 3, 3, 4, 4, 6, 6, 7)(1, 3, 3) = (2, 3, 4, 4, 6, 7, 7) = \mathbf{n}.$$

Case 2. Now, let q be secret and p be public. Then, having \mathbf{w} as above, we reduce the repetition of each component of \mathbf{w} modulo p . We have

$$\mathcal{I}_{(3,\cdot)}(\mathbf{w}) = (2, 3, 4, 4, 6, 6, 7, 7, 9, 12, 12, 18, 21, 21).$$

To decode, we have multiply \mathbf{w} by \mathbf{v} in $\mathcal{Z}_{(3,9)}$.

Note that in Case 1, \mathbf{w} cannot be recovered from $\mathcal{I}_{(\cdot,9)}(\mathbf{w})$ without information about p because \mathbf{w} has components that are greater than or equal to q . However, in Case 2 of this example, $\mathbf{w} = \mathcal{I}_{(3,\cdot)}(\mathbf{w})$; so, it is possible to find \mathbf{n} dividing \mathbf{w} by \mathbf{u} . It happens because the number of repetitions of each component of \mathbf{w} is less than 3.

In the general case, to guarantee that \mathbf{w} cannot be recovered from $\mathcal{I}_{(\cdot,q)}(\mathbf{w})$, we have to make sure that \mathbf{w} contains elements that are greater than or equal to q ; to guarantee that \mathbf{w} cannot be recovered from $\mathcal{I}_{(p,\cdot)}(\mathbf{w})$, we have to make sure that \mathbf{w} contains elements that repeat p or more times. This can be achieved if we add to the secret code a piece of random code with empty information containing components greater than q and repeated more than p times.

6. Conclusions

In the paper, we introduce and study the ring of integer multinumbers \mathcal{Z} and finite rings of multinumbers $\mathcal{Z}_{(p,q)}$. We can see that \mathcal{Z} is isomorphic as a ring to known objects such as the ring of polynomials $\mathbb{Z}[\mathbb{C}^\infty]$ or the ring of Dirichlet series $\mathcal{D}_0(\mathbb{Z})$. However, the representation in the form of multinumbers gives us a different point of view and suggests some new questions and directions of investigation. In particular, we can ask about solutions of Diophantine equations over multinumbers. In addition, using the concept of multinumbers, we introduced the multinumbers modulo (p, q) . Such kinds of objects may be applicable in Cryptography for the creation of new algorithms with open keys, and we proposed one of them. We did not examine in detail the complexities of encoding, decoding, and the resistance of the algorithm against other basic attacks—this may be a subject of further investigations. However, the comparison with RSA and Example 9 gives arguments that the proposed algorithm is applicable. This paper is an invitation to study multinumbers of different natures and their applications to Cryptography.

Finally, we note that the idea of multinumbers appeared from investigations of symmetric and supersymmetric analytic functions on Banach spaces. This is a good argument for the conceptual unity of different branches of Mathematics.

Author Contributions: Conceptualization and supervision the study A.Z.; investigation and original draft preparation of the manuscript Y.C. and T.V. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the National Research Foundation of Ukraine, 2020.02/0025, 0121U111037.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Acknowledgments: The authors thank the anonymous referees for their valuable constructive comments and suggestions, which improved the quality of this work in the present form.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Han, J.; Li, Y.; Lin, L.; Lu, J.; Zhang, J.; Zhang, L. Universal approximation of symmetric and anti-symmetric functions. *arXiv* **2019**, arXiv:1912.01765.
2. Zaheer, M.; Kottur, S.; Ravanbakhsh, S.; Póczos, B.; Salakhutdinov, R.R.; Smola, A.J. Deep sets. In *Advances in Neural Information Processing Systems*; Guyon, I., Luxburg, U.V., Bengio, S., Wallach, H., Fergus, R., Vishwanathan, S., Garnett, R., Eds.; 2017; pp. 3391–3401. Available online: <https://papers.nips.cc/paper/2017> (accessed on 26 December 2021).
3. Dos Martires, P.Z. Neural Semirings. *CEUR Workshop Proc.* **2021**, *2986*, 94–103. Available online: <http://ceur-ws.org/Vol-2986/paper7.pdf> (accessed on 27 February 2022).
4. Yarotsky, D. Universal Approximations of Invariant Maps by Neural Networks. *Constr. Approx.* **2021**, *55*, 407–474. [[CrossRef](#)]
5. Chernega, I.V. A semiring in the spectrum of the algebra of symmetric analytic functions in the space ℓ_1 . *J. Math. Sci.* **2016**, *212*, 38–45. [[CrossRef](#)]
6. Jawad, F.; Zagorodnyuk, A. Supersymmetric polynomials on the space of absolutely convergent series. *Symmetry* **2019**, *11*, 1111. [[CrossRef](#)]
7. Chernega, I.; Fushtei, V.; Zagorodnyuk, A. Power Operations and Differentiations Associated With Supersymmetric Polynomials on a Banach Space. *Carpathian Math. Publ.* **2020**, *12*, 360–367. [[CrossRef](#)]
8. Aron, R.; Galindo, P.; Pinasco, D.; Zalduendo, I. Group-symmetric holomorphic functions on a Banach space. *Bull. Lond. Math. Soc.* **2016**, *48*, 779–796. [[CrossRef](#)]
9. Chernega, I.; Galindo, P.; Zagorodnyuk, A. A multiplicative convolution on the spectra of algebras of symmetric analytic functions. *Rev. Mat. Complut.* **2014**, *27*, 575–585. [[CrossRef](#)]
10. Chernega, I.; Galindo, P.; Zagorodnyuk, A. Some algebras of symmetric analytic functions and their spectra. *Proc. Edinb. Math. Soc.* **2012**, *55*, 125–142. [[CrossRef](#)]
11. González, M.; Gonzalo, R.; Jaramillo, J.A. Symmetric polynomials on rearrangement-invariant function spaces. *J. Lond. Math. Soc.* **1999**, *59*, 681–697. [[CrossRef](#)]
12. Jawad, F. Note on separately symmetric polynomials on the Cartesian product of ℓ_p . *Mat. Stud.* **2018**, *50*, 204–210. [[CrossRef](#)]
13. Kravtsiv, V.V. Analogues of the Newton formulas for the block-symmetric polynomials. *Carpathian Math. Publ.* **2020**, *12*, 17–22. [[CrossRef](#)]
14. Kravtsiv, V.; Vasylyshyn, T.; Zagorodnyuk, A. On algebraic basis of the algebra of symmetric polynomials on $\ell_p(\mathbb{C}^n)$. *J. Funct. Spaces* **2017**. [[CrossRef](#)]
15. Macdonald, I.G. *Symmetric Functions and Orthogonal Polynomials*; University Lecture Serie 12; AMS: Providence, RI, USA, 1997.
16. Halushchak, I.; Novosad, Z.; Tsizhma, Y.; Zagorodnyuk, A. Logistic Map on the Ring of Multisets and Its Application in Economic Models. *Math. Stat.* **2020**, *8*, 424–429. [[CrossRef](#)]
17. Singh, D.; Ibrahim, A.M.; Yohanna, T.; Singh, J.N. An overview of the applications of multisets. *Novi Sad J. Math.* **2007**, *37*, 73–92.
18. Kaur, J.; Ramachandran, R. The Recent Trends in CyberSecurity: A Review. *J. King Saud-Univ.-Comput. Inf. Sci.* **2021**. [[CrossRef](#)]
19. Kraft, J.; Washington, L. *An Introduction to Number Theory with Cryptography*; Chapman and Hall/CRC: London, UK, 2018.
20. Stinson, D.R.; Paterson, M.B. *Cryptography. Theory and Practice*, 4th ed.; Taylor & Francis Group: Boca Raton, FL, USA; London, UK; New York, NY, USA, 2008.
21. Karoubi, M. K-theory, an elementary introduction. In *Cohomology of Groups and Algebraic K-Theory*; Advanced Lectures in Mathematics (ALM); International Press: Somerville, MA, USA, 2010; Volume 12, pp. 197–215.
22. Zariski, O.; Samuel, P. *Commutative Algebra. Volume II. With the Cooperation of I. S. Cohen*; The University Series in Higher Mathematics; D. Van Nostrand Company: Princeton, NJ, USA, 1960.
23. Defant, A.; Garcia, D.; Maestre, M.; Sevilla Peris, P. *Dirichlet Series and Holomorphic Functions in High Dimensions*; New Mathematical Monographs 34; Cambridge University Press: Cambridge, UK, 2019.
24. Makhnei, O.; Pylypiv, V.; Zatorskii, R. m -submultisets and m -permutations of multisets elements. *Carpathian Math. Publ.* **2021**, *13*, 240–258. [[CrossRef](#)]
25. Camillo, V.; Hong, C.Y.; Kim, N.K.; Lee, Y.; Nielsen, P.P. Nilpotent ideals in polynomial and power series rings. *Proc. Am. Math. Soc.* **2010**, *138*, 1607–1619. [[CrossRef](#)]
26. Steinberg, S.A. Rings of quotients of rings without nilpotent elements. *Pac. J. Math.* **1973**, *49*, 493–506. [[CrossRef](#)]