Jan Długosz University in Częstochowa
Scientific Issues, Mathematics XIV, Częstochowa 2009

CONSTRUCTION OF MODULAR NUMBER SYSTEMS WITH ARBITRARY FINITE RANGES

Mikhail Selyaninov

Institute of Technical and Informatics Education
Jan Długosz University in Częstochowa
al. Armii Krajowej 13/15, 42-200 Częstochowa, Poland
e-mail: m.selianinov@ajd.czest.pl

Abstract
In the present paper, we deal with the methodology of constructing modular number systems (MNS), named also residue number systems, on arbitrary mathematical structures such as finite groups, rings and Galois fields.

1. Introduction

The technique of modular information processing is oriented towards implementations of parallel computations within the framework of extensive class of procedures which can be practically defined on arbitrary mathematical structures. Thus, it is natural that the common methodology of constructing modular number systems (MNS), first of all minimum redundant MNS, on the set of ranges, which have received the wide distribution in modern computer applications, should be developed. First of all, it concerns the sets of real and complex numbers, quaternions, polynomials, etc.

The theoretical foundations of the offered technique for constructing the MNS are based on an abstract algebra, the number theory, coding theory and theory of algebraic systems (AS) [1–5].

2. Some theoretical foundations

The method of decomposition of sets into equivalence classes plays a leading part in definition of MNS of all types. This method is realized by means of special relations, and groups, rings or fields are usually used as initial mathematical structures [6, 7].

Definition 1. Let $\mathbf{F}$ be some subset of Cartesian product $\mathbf{X} \times \mathbf{Y}$ of any two sets $\mathbf{X}$ and $\mathbf{Y}$ ($\mathbf{F} \subseteq \mathbf{X} \times \mathbf{Y}$). It is said that elements $x \in \mathbf{X}$ and $y \in \mathbf{Y}$ are in relation $\mathbf{F}$ if $(x, y) \in \mathbf{F}$, and conditional notations $\mathbf{F}(x, y)$ or $x\mathbf{F}y$ is used.

Definition 2. If for every $x \in \mathbf{X}$ there is a unique pair $(x, y) \in \mathbf{F}$, then $\mathbf{F}$ is called a function or mapping from $\mathbf{X}$ into $\mathbf{Y}$.

Thus, a mapping is set by a triple $(\mathbf{X}, \mathbf{Y}, f)$, where f is a rule by which the correspondence between x and y is established. Often a mapping is denoted as $y = f(x)$ or $f : \mathbf{X} \to \mathbf{Y}$.

Definition 3. A mapping $f : \mathbf{X} \to \mathbf{Y}$ is called to be
1) injective if from $f(x_1) = f(x_2)$ $(x_1, x_2 \in \mathbf{X})$ it follows that $x_1 = x_2$;
2) surjective if $f(\mathbf{X}) = \mathbf{Y}$;
3) bijective when conditions 1) and 2) are fulfilled simultaneously.

Definition 4. A binary relation $\mathbf{F} \subseteq \mathbf{X} \times \mathbf{X}$ is called an equivalence relation if the following conditions are satisfied:
- $x\mathbf{F}x$ for all $x \in \mathbf{X}$ (reflexivity);
- $x_1\mathbf{F}x_2 = x_2\mathbf{F}x_1$ for any $x_1, x_2 \in \mathbf{X}$ (symmetry);
- from $x_1\mathbf{F}x_2$ and $x_2\mathbf{F}x_3$ $(x_1, x_2, x_3 \in \mathbf{X})$ it follows that $x_1\mathbf{F}x_3$ (transitivity);

An equivalence relation will be designated as $x \equiv x' \pmod{\mathbf{F}}$, where x, $x' \in \mathbf{X}$.

An equivalence relation $\mathbf{F} \subseteq \mathbf{X} \times \mathbf{X}$ separates the set $\mathbf{X}$ into disjoint classes (the equivalence classes or the adjacent classes) which union coincides with $\mathbf{X}$. All the adjacent classes in the aggregate constitute the so-called factor set of a set $\mathbf{X}$ under equivalence $\mathbf{F}$ which is denoted by $\mathbf{X}/\mathbf{F}$.

Let $[x]$ be an equivalence class containing the fixed set member x of a set $\mathbf{X}$:

$$[x] = \{x' \mid x' \equiv x \pmod{\mathbf{F}};\ x', x \in \mathbf{X}\}. \tag{1}$$

Let $|x|_{\mathbf{F}}$ be a residue of a class (1) and $|\cdot|_{\mathbf{F}}$ be an aggregate of residues of all classes of a factor set $\mathbf{X}/\mathbf{F}$.

Definition 5. A mapping $\Theta : \mathbf{X} \to |\cdot|_{\mathbf{F}}$, associating a residue $|x|_{\mathbf{F}} \in |\cdot|_{\mathbf{F}}$ of a class $[x]$ with every $x \in \mathbf{X}$, is called the residue modulo $\mathbf{F}$ operator.

3. Algebraic systems

The practical use of one or another AS as a basis for the information processing demands transformation of this system into suitable adequate computer analogue. It is natural that in the synthesis process of necessary variant of AS, the technique which ensures conservation of all most essential topological, algebraic and other properties of initial algebraic system should be applied [2].

Definition 6. The finite AS is a mathematical structure

$$S =< \mathbf{M},\ \Omega_{op},\ \Omega_{rel} >, \tag{2}$$

where $\mathbf{M}$ is some set;

$$\Omega_{op} = \{O_1, O_2, \dots, O_{N_{op}}\} \text{ and } \Omega_{rel} = \{R_1, R_2, \dots, R_{N_{rel}}\}$$

are sets of operations and relations on $\mathbf{M}$, correspondingly, (N_{op} and N_{rel} are numbers of operations and relations, accordingly; $N_{op} \geq 0$; $N_{rel} \geq 0$). Elements of a set $\mathbf{M}$ are named system components; a cardinal number of a set $\mathbf{M}$ is denoted by $|\mathbf{M}|$.

For synthesis of some computer model on the basis of AS S (2), it is necessary to realize a corresponding codification of the considered system.

Definition 7. Coding S of AS represents an injective mapping $\phi : \mathbf{M} \to \mathbf{A}$ which associates a word $(x_1, x_2, \dots, x_k) \in \mathbf{A}$ with each set element X of $\mathbf{M}$. A set $\mathbf{A}$ is the Cartesian product of some sets $\mathbf{A}_1, \mathbf{A}_2, \dots, \mathbf{A}_k$ which are named alphabets; $x_i \in \mathbf{A}_i$ $(i = 1, 2, \dots, k); k \geq 1$. The set $\mathbf{C} = \phi(\mathbf{M})$ $(f(\mathbf{M}) \subseteq \mathbf{A})$ is called a code or code space, its elements are named code words; a word $(x_1, x_2, \dots, x_k)$ is a code of a set element X, a symbol x_i is the ith digit of X; k is the length of a code.

If cardinal numbers of a code $\mathbf{C}$ and a set $\mathbf{A}$ satisfy an inequality $|\mathbf{C}| < |\mathbf{A}|$, then the code is redundant. The value

$$R(C) = 1 - \log|\mathbf{C}| / \log|\mathbf{A}|$$

or similar to it is usually used as a redundancy measure [5].

Definition 8. A mapping ϕ^{-1} inverse to coding ϕ is named decoding.

It is quite obvious that any coding $\phi : \mathbf{M} \to (\mathbf{C} \subseteq \mathbf{A})$ of the system S induces some AS on a code space $\mathbf{C}$

$$S_\phi =< \mathbf{C},\ O_1^\phi,\ O_2^\phi, \dots,\ O_{N_{op}}^\phi;\ \mathbf{R}_1^\phi,\ \mathbf{R}_2^\phi, \dots,\ \mathbf{R}_{N_{rel}}^\phi > \tag{3}$$

which has the same type as the initial AS S.

Codification of AS S assumes that a coding should be an isomorphism of systems (2) and (3), that is a one-to-one homomorphic mapping conserving base operations and relations. This means that the following conditions are fulfilled

$$O_r(X_1,\ X_2,\dots,\ X_{m_r}) = O_r^{\phi}(\phi(X_1),\ \phi(X_2),\dots,\ \phi(X_{m_r})),$$

$$O_r(\phi^{-1}(W_1),\ \phi^{-1}(W_2),\dots,\ \phi^{-1}(W_{m_r})) = O_r^{\phi}(W_1,\ W_2,\dots,\ W_{m_r}),$$

$$\mathbf{R}_s(X_1,\ X_2,\dots,\ X_{n_s}) = \mathbf{R}_s^{\phi}(\phi(X_1),\ \phi(X_2),\dots,\ \phi(X_{n_s})),$$

$$\mathbf{R}_s(\phi^{-1}(W_1),\ \phi^{-1}(W_2),\dots,\ \phi^{-1}(W_{n_s})) = \mathbf{R}_s^{\phi}(W_1,\ W_2,\dots,\ W_{n_s})$$

for all

$$(X_1, X_2, \dots, X_{m_r}) \in \mathbf{R}^{m_r},\ (W_1, W_2, \dots, W_{m_r}) \in \mathbf{C}^{m_r},$$

$$(X_1, X_2, \dots, X_{n_s}) \in \mathbf{R}^{n_s},\ (W_1, W_2, \dots, W_{n_s}) \in \mathbf{C}^{n_s},$$

$$r = 1, 2, \dots, N_{op};\ s = 1, 2, \dots, N_{rel}.$$

Definition 9. A codifying AS along with execution rules for its base operations and relations in a code language will be named a number system (NS). At the same time, the encoded set, i.e. pre-image $\mathbf{M}$ of a code $\mathbf{C}$, will be named a definitional domain or a range of NS, including it in the conditional designation of a system:

$$S_{\phi} =< \mathbf{M},\ \mathbf{C},\ O_1^{\phi},\ O_2^{\phi},\dots,\ O_{N_{op}}^{\phi};\ \mathbf{R}_1^{\phi},\ \mathbf{R}_2^{\phi},\dots,\ \mathbf{R}_{N_{rel}}^{\phi} > .$$

Groups, rings and fields are usually used as discrete AS which are immediate objects of codification.

Definition 10. Any additive subgroup $\mathbf{P}$ of commutative ring $\mathbf{R}$ with a property $(x \in \mathbf{P})\ \&\ (a \in \mathbf{R}) \Rightarrow xa \in P$ is called an ideal.

Let $\mathbf{R}$ be a commutative ring and $\mathbf{P}$ be an ideal in it. We will separate elements of a set $\mathbf{R}$ into classes referring elements x and x' to the same class if and only if $x - x' \in \mathbf{P}$. Such a partition defines an equivalence relation on $\mathbf{R}$. The corresponding factor set is a group which is named a factor group of a ring $\mathbf{R}$ and is denoted as $\mathbf{R}/\mathbf{P}$. It is evident that multiplication in $\mathbf{R}$ induces the uniquely defined multiplication in a factor group $\mathbf{R}/\mathbf{P}$. This converts it into a factor ring or a ring of residue classes.

Definition 11. An ideal $(x) = \mathbf{R}x$ consisting of all multiple of some element x of a ring $\mathbf{R}$ is named a principal ideal.

Definition 12. An ideal $\mathbf{P}$ in a ring $\mathbf{R}$ is called a prime ideal if $\mathbf{P} \neq (\mathbf{1})$ and it follows from $xy \in \mathbf{P}$ that either $x \in \mathbf{P}$ or $y \in \mathbf{P}$.

Let us define operations on ideals which are necessary for a statement of the technique of constructing modular number systems. Let $\mathbf{P}_1, \mathbf{P}_2, \dots, \mathbf{P}_k$ ($k \geq 2$) be ideals in a commutative ring $\mathbf{R}$. The sum and the product of the given ideals are defined by the following rules

$$\sum_{i=1}^{k} \mathbf{P}_i = \left\{ \sum_{i=1}^{k} x_i \;\mid\; x_i \in \mathbf{P};\ i = 1, 2, \dots, k \right\},$$

$$\prod_{i=1}^{k} \mathbf{P}_i = \left\{ \sum_{i=1}^{L} \prod_{n=1}^{k} x_{l,n} \;\mid\; x_{l,n} \in \mathbf{P}_n;\ n = 1, 2, \dots, k; L \in \{1, 2, \dots\}, L < \infty \right\}.$$

We note that intersection of any family of ideals of a ring $\mathbf{R}$, including $\bigcap_{i=1}^{k} \mathbf{P}_i$, is also an ideal. Operations of addition, multiplication and intersection of ideals are associative and commutative. The distributive law for multiplication with respect to addition is also valid.

The implication of the introduced operations is clearly explained by the following example.

Example. Let in the ring $\mathbf{Z}$ of integers, the ideals $\mathbf{P}1 = (l)$ and $\mathbf{P}2 = (n)$, where l and n are natural numbers, be defined. Then $\mathbf{P}1 + \mathbf{P}2$ is an ideal generated by the greatest common divisor (l, n) of numbers l and n, that is $\mathbf{P}1 + \mathbf{P}2 = ((l, n))$. An ideal $\mathbf{P}1 \cap \mathbf{P}2$ is generated by the least common multiple $[l, n]$ of numbers l and n, that is $\mathbf{P}1 \cap \mathbf{P}2 = ([l, n])$, and $\mathbf{P}1\mathbf{P}2 = (l, n)$. At the same time, the equality $\mathbf{P}1\mathbf{P}2 = \mathbf{P}1 \cap \mathbf{P}2$ occures if and only if l and n are coprime, i.e. ((l, n) = 1).

Definition 13. Ideals $\mathbf{P}1$ and $\mathbf{P}2$ of a ring $\mathbf{R}$ for which the condition $\mathbf{P}1 + \mathbf{P}2 = (1)$ is satisfied are named coprime ideals.

It is obvious that relative primality of ideals $\mathbf{P}1$ and $\mathbf{P}2$ is equivalent to existence of elements $x \in \mathbf{P}1$ and $y \in \mathbf{P}2$ such that $x + y = 1$.

It should be noted that for cardinals of a finite ring $\mathbf{R}$, its ideal $\mathbf{P}$, and factor ring $\mathbf{R}/\mathbf{P}$ the following equality is valid

$$|\mathbf{R}| = |\mathbf{P}|\ |\mathbf{R}/\mathbf{P}|. \tag{4}$$

4. The main theorem of modular arithmetic

Let us assume that a set $\mathbf{M}$ is a commutative ring and $\mathbf{M}_1, \mathbf{M}_2, \dots, \mathbf{M}_k$ are ideals of this ring ($k \geq 2$). We denote by $|\cdot|_{\mathbf{M}_i}$ an aggregate of some distinguished elements of residue classes (one from each class) of factor rings

$\mathbf{M}/\mathbf{M}_i$ $(i = 1, 2, \dots, k)$. The residue modulo operator (see definition 5) associates with each $X \in \mathbf{M}$ a unique element of a set $|\cdot|_{\mathbf{M}_i}$ which is denoted by $|X|_{\mathbf{M}_i}$. It is quite obvious that the set $|X|_{\mathbf{M}_i}$ is a commutative ring as well as a factor ring $\mathbf{M}/\mathbf{M}_i$.

Let us define a mapping $\phi : \mathbf{M} \to |\cdot|_{\mathbf{M}_1} \times |\cdot|_{\mathbf{M}_2} \times \ldots \times |\cdot|_{\mathbf{M}_k}$ on the set $\mathbf{M}$ acting according to a rule

$$\phi(X) = (|X|_{\mathbf{M}_1},\ |X|_{\mathbf{M}_2},\ \dots, |X|_{\mathbf{M}_k}). \tag{5}$$

As it was stated, ϕ is a homomorphism induced on the $\mathbf{M}$ system

$$S_\phi\ = < \mathbf{M},\ |\cdot|_{\mathbf{M}_1} \times |\cdot|_{\mathbf{M}_2} \times \ldots \times |\cdot|_{\mathbf{M}_k};\ (+, +, \dots, +),\ (\cdot, \cdot, \dots, \cdot) > . \tag{6}$$

As evident from (5), base operations on any X and Y from $\mathbf{M}$ in the system (6) are executed independently component-wise:

$$\begin{aligned}\phi(X) + \phi(Y) &= (|X|_{\mathbf{M}_1}, |X|_{\mathbf{M}_2}, \dots, |X|_{\mathbf{M}_k}) + (|Y|_{\mathbf{M}_1}, |Y|_{\mathbf{M}_2}, \dots, |Y|_{\mathbf{M}_k}) \\ &= (|X + Y|_{\mathbf{M}_1}, |X + Y|_{\mathbf{M}_2}, \dots, |X + Y|_{\mathbf{M}_k}) = \phi(X + Y), \qquad (7) \\ \phi(X) \cdot \phi(Y) &= (|X|_{\mathbf{M}_1}, |X|_{\mathbf{M}_2}, \dots, |X|_{\mathbf{M}_k}) \cdot (|Y|_{\mathbf{M}_1}, |Y|_{\mathbf{M}_2}, \dots, |Y|_{\mathbf{M}_k}) \\ &= (|X \cdot Y|_{\mathbf{M}_1}, |X \cdot Y|_{\mathbf{M}_2}, \dots, |X \cdot Y|_{\mathbf{M}_k}) = \phi(X \cdot Y). \qquad (8)\end{aligned}$$

Expressions (7) and (8) show that the system S (6) is a commutative ring with unity (1, 1..., 1).

Theorem (The main theorem of modular arithmetic). Let M be a commutative ring and $\mathbf{M}_1, \mathbf{M}_2, \dots, \mathbf{M}_k$ be its ideals. Then:

1) if $\mathbf{M}_1,\ \mathbf{M}_2, \dots, \mathbf{M}_k$ are pairwise prime, i.e.

$$\mathbf{M}_l + \mathbf{M}_k = (1);\quad (l \neq k;, n \in 1, 2, \dots, k), \tag{9}$$

then $\prod\limits_{i=1}^{k} \mathbf{M}_i = \bigcap\limits_{i=1}^{k} \mathbf{M}_i$;

2) a homomorphism $\phi : \mathbf{M} \to |\cdot|_{\mathbf{M}_1} \times |\cdot|_{\mathbf{M}_2} \times \ldots \times |\cdot|_{\mathbf{M}_k}$ defined by (5) is surjective if and only if (9) is valid;

3) a homomorphism ϕ is injective if and only if

$$\bigcap_{i=1}^{k} \mathbf{M}_i = (0). \tag{10}$$

In the proposed technique of constructing the MNS on such mathematical structures as finite groups, rings and Galois fields, the formulated theorem plays a fundamental role [3].

5. Technique of constructing a modular number system

According to the main theorem, in the case when the equality (10) is fulfilled for a ring $\mathbf{M}$ and ideals $\mathbf{M}_1$, $\mathbf{M}_2$, ... ,$\mathbf{M}_k$, an AS (5) (taking into account an injective homomorphism generating it) represents an NS (see definition 8) with a range $\mathbf{M}$, the coding (8), the code $= |\cdot|_{\mathbf{M}_1} \times |\cdot|_{\mathbf{M}_2} \times \ldots \times |\cdot|_{\mathbf{M}_k}$ and alphabets $\mathbf{A}_i = |\cdot|_{\mathbf{M}_i}$ $(i = 1, 2, \ldots, k)$. This NS will be called an MNS. At the same time, ideals $\mathbf{M}_1, \mathbf{M}_2, \ldots, \mathbf{M}_k$ and, in a case when they are principal ideals, their generating elements $m_1, m_2, \ldots, m_k$ $(\mathbf{M}_i = (m_i), m_i \in \mathbf{M};\ i = 1, 2, \ldots, k)$ will be named the modules of an MNS.

In the case $\mathbf{M}_i = (m_i)$, the notation $|\cdot|_{m_i}$ will be used for a ring $|\cdot|_{\mathbf{M}_i}$ as well as the notation $|X|_{m_i}$ will be used for a residue $|X|_{\mathbf{M}_i} \in |\cdot|_{\mathbf{M}_i}$. As follows from (7) and (8), the ring operations on any two elements A and B from $\mathbf{M}$, defined by their modular codes $A = (\alpha_1, \alpha_2, \ldots, \alpha_k)$ and $B = (\beta_1, \beta_2, \ldots, \beta_k)$ $(\alpha_i = |A|_{\mathbf{M}_i},\ \beta_i = |B|_{\mathbf{M}_i}\ (i = 1, 2, \ldots, k))$, are executed independently on each of residues, i.e. according to a rule

$$A \circ B = (|\alpha_1 \circ \beta_1|_{\mathbf{M}_1},\ |\alpha_2 \circ \beta_2|_{\mathbf{M}_2},\ \ldots,\ |\alpha_k \circ \beta_k|_{\mathbf{M}_k}\ \ (\circ \in \{+,\ \cdot\}). \quad (11)$$

The internal parallelism of an MNS, consisting in the property (11), represents the main merit of such systems.

Let $\mathbf{M}$ be a finite ring with cardinal $N = |\mathbf{M}|$. According to (7), for each ideal $\mathbf{M}_i \subseteq \mathbf{M}$ and a residue ring $|\cdot|_{\mathbf{M}_i}$ corresponding to it, the following equality is satisfied

$$N = N_i\, n_i \quad (N_i = |\mathbf{M}_i|;\ \ n_i = ||\cdot|_{\mathbf{M}_i}|;\ \ i = 1, 2, \ldots, k). \quad (12)$$

Taking into account (12), the foregoing allows us to formulate the following technique for constructing an MNS on a given range $\mathbf{M}$ [6, 7].

1. The order N of a ring $\mathbf{M}$ is factorized into a product $N = \prod_{i=1}^{k} n_i$ of acceptable pairwise prime natural multipliers $n_1, n_2, \ldots, n_k$ $(k \geq 2)$.

2. For every $i \in \{1, 2, \ldots, k\}$, the principal ideal $\mathbf{M}_i = (m_i)$ with the order $N_i = N/n_i$ is chosen by means of specially selected generating element m_i in $\mathbf{M}$. The element m_i always exists. It generates a cyclic additive group $\{k_i\, m_i \mid k_i = 0, 1, \ldots, N_i - 1\}$ which exactly coincides with $\mathbf{M}_i$.

For $\mathbf{M}_1$, $\mathbf{M}_2$, ... ,$\mathbf{M}_k$ the fulfillment of conditions (9) and (10) is ensured.

3. For principal ideals $\mathbf{M}_i$, the corresponding residue rings $|\cdot|_{\mathbf{M}_i}$ are constructed so that computer codes of their elements have minimum lengths in their own adjacent classes.

According to (12), a number of residues in a ring $|\cdot|_{\mathbf{M}_i}$ is equal to n_i.

4. For an MNS with modules $\mathbf{M}_1, \mathbf{M}_2, \ldots, \mathbf{M}_k$, the computer procedures of necessary operations in a language of a code $C = \phi(\mathbf{M}) = |\cdot|_{\mathbf{M_1}} \times |\cdot|_{\mathbf{M_2}} \times \ldots \times |\cdot|_{\mathbf{M_k}}$ are synthesized.

Any technique of constructing an MNS along with procedure of creating a modular code $(\chi_1, \chi_2, \ldots, \chi_k)$ $(\chi_i = |X|_{\mathbf{M}_i},\ i = 1, 2, \ldots, k)$ for every $X \in \mathbf{M}$ should include some procedure of restoring X according to its modular code. The Chinese remainder theorem (CRT) is a classical basis for synthesis of such procedures. According to the CRT, a decoding mapping $\phi^{-1} : |\cdot|_{\mathbf{M}_1} \times |\cdot|_{\mathbf{M}_2} \times \ldots \times |\cdot|_{\mathbf{M}_k} \to \mathbf{M}$ in an MNS with modules $\mathbf{M}_1$, $\mathbf{M}_2$, $\ldots$, $\mathbf{M}_k$ can be realized in the following constructive form

$$|X|_{M_k} = \left| \sum_{i=1}^{k} M_{i,k}\ \chi_{i,k} \right|_{M_k}, \tag{13}$$

where $M_k = \prod_{i=1}^{k} m_i$ is a generating element of a principal ideal $\widehat{\mathbf{M}} = (M_k) = \prod_{i=1}^{k} \mathbf{M}_i$; by $|Y|_{M_k}$ we denote the element of a residue ring $|\cdot|_{M_k} = |\cdot|_{\mathbf{M}_k}$ which is equivalent to $Y \in \mathbf{M}$; $M_{i,k} = M_k \ / \ m_i$; $\chi_{i,k}$ is a residue of the ring $|\cdot|_{m_i}$ such that

$$M_{i,k}\ \chi_{i,k} \equiv \chi_i \pmod{\mathbf{M}_i}. \tag{14}$$

In the case when principal ideals $(M_{i,k})$ and (m_i) are pairwise prime, the residue $\chi_{i,k}$ satisfying (14) always exists and is unique. As can be seen from (13), the CRT establishes a correspondence between words $(\chi_1, \chi_2, \ldots, \chi_k)$ of a code $\mathbf{C} = |\cdot|_{\mathbf{M_1}} \times |\cdot|_{\mathbf{M_2}} \times \ldots \times |\cdot|_{\mathbf{M_k}}$ and elements $|X|_{\mathbf{M}}$ of a residue ring $|\cdot|_{\mathbf{M}}$. If ideals $\mathbf{M}_1$, $\mathbf{M}_2$, $\ldots$, $\mathbf{M}_k$ satisfy conditions (9) and (10), then $\mathbf{M}/\widehat{\mathbf{M}} = \mathbf{M}/(0) = \mathbf{M}$ (for every $X \in \mathbf{M}$ the equivalence class $[X] \in \mathbf{M}/(0)$ contains only X). At the same time, a mapping ϕ defining an MNS with modules $\mathbf{M}_1$, $\mathbf{M}_2$, $\ldots$, $\mathbf{M}_k$ is an isomorphism (a bijective homomorphism) of range $\mathbf{M}$ and code space $\mathbf{C}$ (see the theorem). In this case, (13) becomes

$$X = \left| \sum_{i=1}^{k} M_{i,k}\ \chi_{i,k} \right|_{\mathbf{M}}. \tag{15}$$

6. Redundant modular number systems

The general bases of the developed technique for constructing an MNS on arbitrary AS can be detailed for the specific classes of MNS which are defined particularly on real, complex and polynomial ranges [8–10].

In modern applications of an MNS as priority computer-arithmetic base, it is naturally used the real modular arithmetic (MA). Besides exclusively great own importance, the real MNS has extreme significance for constructing MA on mathematical structures which possess multidimensional (vectorial) features. Usually, in specified configurations of MA the real MNS plays a role of a lower level system. Thus, the developed technique, first of all, should be applied to codification of real ranges.

The presented technique of constructing an MNS on finite rings (see (1)–(4)) along with the basic requirement (10) for the base ideals $\mathbf{M}_1$, $\mathbf{M}_2$, $\dots$,$\mathbf{M}_k$ imposes on them two additional restrictions (for simplicity): the pairwise prime condition (9) and a factorization of cardinal N of ring $\mathbf{M}$ on pairwise prime natural multipliers n_i fulfilling a role of cardinals of factor rings $\mathbf{M}/\mathbf{M}_i$ $(i = 1, 2, \dots, k)$. The main theorem of MA ensures an isomorphism between the encoded S and resultant S_ϕ algebraic systems and therefore, in view of the fact that $\mathbf{C} = \phi(\mathbf{M}) = |\cdot|_{\mathbf{M_1}} \times |\cdot|_{\mathbf{M_2}} \times \dots \times |\cdot|_{\mathbf{M_k}}$, leads to an irredundant MNS.

In the context of the described technique, for deriving the redundant MNS with a range $\mathbf{M}$ and modules $\mathbf{M}_1$, $\mathbf{M}_2$, $\dots$,$\mathbf{M}_k$, i.e. systems for which

$$N = |\mathbf{C}| < |\cdot|_{\mathbf{M}_1} \times |\cdot|_{\mathbf{M}_2} \times \dots \times |\cdot|_{\mathbf{M}_k}| = \prod_{i=1}^{k} n_i \quad (n_i = ||\cdot|_{\mathbf{M}_i}|),$$

it is obviously enough to remove the restriction (9).

However, for optimization of the modular computing structures another variant of redundant coding is most appropriated. In this case, some subset $\mathbf{D}$ (not necessarily a subring) of initial set $\mathbf{M}$ is used as a range in (6). This leads to a code space $\mathbf{C} = \phi(\mathbf{D})$ with cardinality $|\mathbf{C}| < \phi(\mathbf{M})$. A resultant redundant MNS

$$S_\phi = < \mathbf{D},\ \phi(\mathbf{D}) \subset |\cdot|_{\mathbf{M_1}} \times |\cdot|_{\mathbf{M_2}} \times \dots \times |\cdot|_{\mathbf{M_k}};$$

$$(+, +, \dots, +),\ (\cdot, \cdot, \dots, \cdot) > \tag{16}$$

is naturally a restriction of initial system (6) and possess all its merits stipulated by parallel structure of a homomorphism ϕ (see (5)–(8)).

The main purpose of using the range $\mathbf{D}$ with less cardinal number instead of a set $\mathbf{M}$ consists in constructing an MNS (16) which has minimum of redundancy of a code $\mathbf{C} = \phi(\mathbf{D})$ and gives the base relation for implementation of decoding mapping $\phi_{-1} : \mathbf{C} \to \mathbf{D}$ which is more simple than (13) and (15). Let X be an element of the range $\mathbf{D}$ and X possess the MC $(\chi_1, \chi_2, \dots, \chi_k)$. Let in the ring $\mathbf{M}$ the modules $\mathbf{M}_1$, $\mathbf{M}_2$, ... ,$\mathbf{M}_k$ of an MNS (16) be represented by principal ideals generated by elements $m_1, m_2..., m_k$, correspondingly. Then, in accordance with the CRT by analogy with (13), it is possible to write

$$|X|_{M_{k-1}} = \left| \sum_{i=1}^{k-1} M_{i,k-1} |M_{i,k-1}^{-1} \chi_i|_{m_i} \right|_{M_{k-1}}, \tag{17}$$

where $M_{k-1} = \prod_{i=1}^{k-1} m_i$, $M_{i,k-1} = M_{k-1}/m_i$; $M_{i,k-1}^{-1}$ is a residue of ring $|\cdot|_{m_i}$ such that $M_{i,k-1}\ M_{i,k-1}^{-1} \equiv 1 \pmod{\mathbf{M}_i}$. It follows from (17) that $X = \sum_{i=1}^{k} M_{i,k-1} |M_{i,k-1}^{-1} \chi_i|_{m_i}$ is an element of the principal ideal $(M_{k-1}) = \prod_{i=1}^{k-1} (m_i)$. This means that in $\mathbf{M}$ there is some element $I(X)$ such that

$$X = \sum_{i=1}^{k-1} M_{i,k-1} \chi_{i,k-1} \ + \ I(X) M_{k-1}. \tag{18}$$

Definition 14. An integral characteristic of an MC $I(X)$ will be named an interval index (II) corresponding to a principal ideal (M_{k-1}) or simply an interval index, and expression (18) will be called an interval-modular form (IMF) of an element X.

In contrast to the CRT (13) and (15), the IMF (18) does not contain operations of a residue modulo $\mathbf{M}$. Therefore, the decoding procedures of the MC synthesized on its basis are more effective than the procedures realizing direct implementations of the CRT. At the same time, the maximum effect is reached in the context of redundant coding, as in this case the computation of an II $I(X)$ becomes a trivial operation [8, 10]. Similar to redundant restrictions of the classical MNS, as a range $\mathbf{D}$ we will use sets of the form $\mathbf{Z}_M = \{0, 1, \dots, M-1\}$ and $\mathbf{Z}_{2M}^{-1} = \{-M, -M+1, \dots, M-1\}$, where $M = \prod_{i=0}^{k-1} m_i$; m_0 is the auxiliary natural module selected according to the condition $|\mathbf{D}| < |\mathbf{M}|$, simplicity of the computation of II and execution of the operations of MA with minimum of coding redundancy.

References

[1] V.M. Amerbaev. *Theoretical Bases of Machine Arithmetics.* Nauka, Alma-Ata 1976. (In Russian).

[2] A.I. Maltsev. *Algebraic Systems.* Nauka, Moscow 1970. (In Russian).

[3] M. Atghia, I. McDonald. *Introduction to Commutative Algebra.* Mir, Moscow 1972. (In Russian).

[4] I.M. Vinogradov. *Elements of Number Theory.* Nauka, Moscow 1981. (In Russian).

[5] T. Kasami, N. Tokura, E. Ivodari, J. Inagati. *Coding Theory.* Mir, Moscow 1978. (In Russian).

[6] A.A. Kolyada, V.V. Revinsky, M.Y. Selyaninov *et al.* Elements of the theory and applications of modular technique of parallel information processing. *Modern Problems of Optics, Radiation Materials Science, Informatics, Radiophysics and Electronics. Proc. Sci. Research Inst. Appl. Phys. Probl.* Belgosuniversitet, Minsk, vol. 2, pp. 1–51, 1996. (In Russian).

[7] M.Y. Selyaninov. Theoretical bases of modular codification of algebraic systems. *Proc. Nat. Acad. Sci. Belarus,* No. 1, 114–119, 2002. (In Russian).

[8] A.F. Chernyavsky, V.V. Danilevich, A.A. Kolyada, M.Y. Selyaninov. *High-speed Methods and Systems of Digital Information Processing.* Belgosuniversitet, Minsk 1996. (In Russian).

[9] M.Y. Selyaninov. Application of numerically-analytical modular computing techniques for performance of additive and multiplicative operations over signals in spaces of orthogonal projections. *Rep. Nat. Acad. Sci. Belarus,* **46**, No. 2, 62–66, 2002. (In Russian).

[10] M. Selyaninov M. Modular technique of parallel information processing. *Scientific Issues of Jan Długosz University of Czestochowa, Ser. Mathematics*, **XIII**, 43–52, 2008.