UDC 004.02:519.87

Mathematical Model of the Process of Raising Integers to an Arbitrary Power of a Natural Number in the System of Residual Classes

Victor Krasnobayev[1], Alina Yanko[2], and Dmytro Kovalchuk[1]

[1]*N. Karazin Kharkiv National University, Svobody sq., 4, Kharkiv, 61022, Ukraine*
[2]*National University «Yuri Kondratyuk Poltava Polytechnic», Poltava, 36011, Ukraine*

Abstract

It is known that the use of a non-positional number system in residual classes (SRC) in computer systems (CS) can significantly increase the speed of the implementation of integer arithmetic operations. The use of such properties of a non-positional number system in the SRC as independence, equality and low-bitness (low-digit capacity) of the residues that define the non-positional code data structure of the SRC provides high user performance for the implementation in the CS of computational algorithms consisting of a set of arithmetic (modular) operations. The greatest efficiency from the use of the SRC is achieved when the implemented algorithms consist of a set of arithmetic operations such as addition, multiplication and subtraction.

There is a large class of algorithms and tasks (tasks of implementing cryptoalgorithms, optimization tasks, computational tasks of large dimension, etc.), where, in addition to performing integer arithmetic operations of addition, subtraction, multiplication, raising integers modulo and others in a positive numerical range, there is a need to implement the listed above arithmetic and other operations, in the negative numerical range. The need to perform these operations in a negative numerical range significantly reduces the overall efficiency of using the SRC as a number system of the CS. In this aspect, the lack of a mathematical model for the process of raising integers in the SRC in the negative numerical region makes it difficult to develop methods and procedures for raising integers to an arbitrary power of a natural number in the SRC, both in positive and negative numerical ranges.

The purpose of the article is the synthesis of a mathematical model of the process of raising integers to an arbitrary power of a natural number in the SRC, both in positive and negative numerical ranges.

Keywords: Artificial form, computer system, mathematical induction, mathematical model, method for raising integers, positional number system, system of residual classes

Introduction

Information security is one of the most important issues in the modern world, which is the main reason for the constant development of methods and methods for processing, monitoring and controlling data. It should be noted that along with the currently widely used methods for increasing the speed and reliability of CSs operating in the conventional binary positional number system (PNS), great prospects open up through the development and implementation of new, non-traditional methods for representing and processing data in a non-positional number system. In particular, at present, data coding options are being considered based on mathematical models and methods arising from a special branch of mathematics – number theory [1-3]. As a result, the search for alternative ways to increase the speed of information processing and increase the reliability of the result of solving computational tasks leads to an increase in interest in the use of a non-positional system of residual classes in related fields of science and technology. First of all, the possibility of using SRC to increase the speed and fault-tolerance of the CS is investigated [4-6]. This interest is caused, first of all, by the following circumstances:

- the appearance, both in our country and abroad, of numerous scientific and theoretical publications devoted to the theory and practice of creating high-speed, reliable, survivable and fault-tolerant computer systems and components operating in the

SRC; in particular, the elements of the theory of ensuring fault tolerance and the classification of the CS functioning on the basis of the use of the SRC are being developed [7-9];

- mass distribution of mobile device processors, which require high data processing performance with low energy consumption; the use of the SRC when performing arithmetic operations of addition and multiplication of numbers ensures high performance due to the absence of interdigit transfers in the process of performing arithmetic operations; at the same time, during the operation of mobile devices, the use of the SRC can significantly reduce energy consumption [10];
- banking structures are of great interest, where there is a need to reliably and reliably process large amounts of data in real time, i.e. high-performance computing tools are required for highly reliable calculations with possible self-correction of errors, which is typical for corrective codes in the SRC [11];
- increasing the density of the placement of elements on a single chip doesn't in all cases allow for high-quality and complete testing of computer components; in this case, the importance of ensuring fault-tolerant functioning of the CS increases; preliminary research results have shown that with the help of the SRC it is possible to organize fault-tolerant operation of real-time CS [12];
- the need to use specialized CS to perform a huge number of operations on multidimensional numerical structures in real time, require a high speed of integer addition and multiplication operations (tasks of matrix multiplication, tasks of the scalar product of vectors, Fourier transform, etc.) [10, 13];
- at present, the widespread introduction of microelectronics in all spheres of human life has significantly increased the relevance and importance of previously rare, but now widespread, such mass scientific and practical problems as digital signal and image processing, pattern recognition, cryptographic transformations, processing and storage of multi-bit information etc.; this circumstance requires huge computing resources that exceed the existing capabilities of the CS operating in binary PNS [14];
- research notes that from the point of view of ensuring the necessary performance, reliability and fault tolerance of real-time processing of large data arrays, existing and prospective CSs and components operating in the PNS cannot provide this [15];
- it is obvious to specialists in the field of computer technology that the current level of development of microelectronics is approaching the limit of its capabilities; considered promising ways for the further development of microelectronics, replacing nanoelectronics, such as, for example, molecular and biological electronics, micromechanics, optical, optoelectronic and photonic CSs and other exotic areas for improving existing CSs, are still very far from real widespread industrial production and practical use [16-18].

1. Problem statement

It should be noted that the high efficiency (increase in speed and reliability) of the use of SRC in the implementation of the integer arithmetic operation of addition, subtraction and multiplication has been proven by the results of research by many inventors. At the same time, there is a numerous class of problems and algorithms, where, in addition to performing the above integer arithmetic operations, it is necessary to implement the operation of raising numbers to a power. At the moment, there is a problem of implementing the operation of raising integers represented in the SRC to an arbitrary power of a natural number in a negative numerical region. The absence of methods for raising integers represented in the SRC to an arbitrary power of a natural number in the whole numerical area, significantly narrows the area of effective use of the SRC as a number system of the CS [1].

It should be noted that the operation of raising to a power widely used in cryptography, which is one of the effective methods of protecting information through the use of coded algorithms, hashes and signatures. It is used in various cryptographic algorithms such as:

- in the RSA algorithm, operation of raising to a power used to encrypt and decrypt messages. When encryption, the recipient's public key is used the raising to a power of a number representing the plaintext of the message, resulting in the ciphertext. When decryption, the recipient's private key is used

the raising to a power of the ciphertext, resulting in the original plaintext.

- in the Diffie-Hellman algorithm, the operation of raising integers to a power is used to create a shared secret key between two participants. Participants choose a random number and the raising to a power of this number is performed using the public key of another participant, after which the resulting number is transmitted to another participant. Then other participant also raises the resulting number to the power of its private key to get the shared secret key.
- in the ElGamal algorithm, operation of raising to a power used to encrypt and decrypt messages. When encryption, the sender randomly chooses a number and raises the recipient's public key to the power of that number, and also raises the plaintext of the message to the power of the sender's private key. The results of the operations are multiplied to get the ciphertext. When decrypting, the recipient raises the first part of the ciphertext to the power of their private key, then uses that number to divide the second part of the ciphertext to get the original plaintext.

Thus, operation of raising to a power is an important tool in cryptography that is used for privacy, data protection, authentication and encryption.

Thus, researches devoted to the development of a method for raising the residues of integers modulo an arbitrary SRC to the power of a natural number are relevant and important. However, the existing methods for implementing the modular operation of raising integers to a power [19] are not always applicable for their implementation in a negative numerical range. This is mainly due to the fact that there is no simple mathematical model [20] for the process of raising integers to an arbitrary power of a natural number in the SRC, both in positive and negative numerical ranges. The researches carried out in this article are primarily devoted to the synthesis of a mathematical model of the process of raising integers to an arbitrary power of a natural number in the SRC, both in positive and negative numerical ranges.

The purpose of the article is the synthesis of a mathematical model of the process of raising integers to an arbitrary power of a natural number in the SRC, both in positive and negative numerical ranges.

2. Literature Source Review

Cryptographic encryption methods have their own characteristics and are applied depending on the requirements for security and ease of use. The more individual protection systems, the more difficult it is to carry out a cyber attack, says Mark Stamp, professor of computer science and engineering, specializing in cybersecurity and cryptography [21]. Such systems include unique methods and tools that are difficult to replicate or circumvent.

In addition, unique data protection and monitoring systems can be tailored to the specific needs and requirements of the organization, which increases the efficiency of their work. However, building and maintaining such systems requires more time, resources, and cybersecurity expertise.

The positional binary number system is the most common number system in computer systems. She was studied by many scientists researchers in mathematics, computer science and cryptography have been sent, such as Jian Liu, Junjie Yan, Jun Jiang, Yitong He, Xuren Wang, Zhengwei Jiang, and came to the conclusion that there are some shortcomings of this system, in particular, hacking methods, hacker attacks, viruses and information integrity violations are based on working with binary positional code.Due to shortcomings in cryptography, other number systems began to be used, including systems based on residual classes. One such system is the non-positional number system in residual classes, which is used to encrypt messages in cryptography.

The literature describes a number of algorithms and methods for processing integer data in a non-positional number system, the so-called SRC, which are used in cryptography due to their high performance and speed.

The application of the residual class system in cryptography used by Dr. Dimitrios Shinianakis and Thanos Sturaitis providing a detailed explanation of cryptographic algorithms based on the SRC, including RSA, ElGamal and cryptography on elliptic curves [22]. They discuss the problem and limitation of the use of the SRC in cryptography, such as the difficulty of handling negative numbers. Various methods for solving this problem and the reliability of cryptographic systems based on the SRC are investigated. Indeed, as a review of the literature has shown, today the scope of SRC use is limited by the certain class of tasks to be solved: the

performance of integer arithmetic operations in positive numerical range. However, there are numerous class of algorithms and tasks for the implementation of cryptoalgorithms, where in addition to performing integer arithmetic operations of addition, subtraction, multiplication, raising integer numbers modulo, in a positive numerical range, there is a need to implement the above arithmetic operations in a negative numerical range. The need to perform operations in a negative numerical range is significantly reduces the overall efficiency of using SRC as a number system of the CS. In this aspect, the lack of a mathematical model for the process of raising integers in the SRC in the negative numerical region makes it difficult to develop methods and procedures for raising integers to an arbitrary power of a natural number in the SRC, both in positive and negative numerical ranges.

3. Synthesis of a mathematical model

It is known that according to the type of the initial number presented in the SRC $C_{SRC} = (c_1 \| c_2 \| ... \| c_{e-1} \| c_e \| c_{e+1} \| ... \| c_g)$, where c_e – residue an arbitrary modulo μ_e of the number C represented in the SRC;|| – mathematical sign of the concatenation operation: gluing operation, joining operation; it is impossible to determine whether it belongs to the positive or negative numerical ranges [23]. Consider the option of representing numbers in the SRC, both in positive and negative numerical ranges.

For implement the process of performing the operation of raising the residue of integers by an arbitrary modulo SRC to the power of a natural number, both in positive and negative numerical ranges, it is supposed to represent the original number $C_{SRC} = (c_1 \| c_2 \| ... \| c_{e-1} \| c_e \| c_{e+1} \| ... \| c_g)$, artificial form (AF) [1]:

$$\begin{cases} C'_{SRC} = \dfrac{D}{2} + |C_{SRC}|, \; if \; C \geq 0, \\ C'_{SRC} = \dfrac{D}{2} - |C_{SRC}|, \; if \; C < 0, \end{cases} \quad (1)$$

where C'_{SRC} – initial number in the SRC $C_{SRC} = (c_1 \| c_2 \| ... \| c_{e-1} \| c_e \| c_{e+1} \| ... \| c_g)$ in AF; $D = \prod_{e=1}^{g} \mu_e$ – the size of the range of represented numbers in the SRC used; μ_e – SRC module; C – initial (natural) number; i.e. for positive numbers: $C'_{SRC} = \dfrac{D}{2} + |C_{SRC}|$ and for negative: $C'_{SRC} = \dfrac{D}{2} - |C_{SRC}|$.

Expression (1) is also valid for natural numbers in the PNS [24].

In addition, the processed numbers in the power of C^n_{SRC} and $(C'_{SRC})^n$ in the SRC are in the corresponding numerical intervals:

$$\begin{cases} -\dfrac{D}{2} \leq C^n_{SRC} \leq \dfrac{(D-1)}{2} \\ 0 \leq (C'_{SRC})^n \leq D-1 \end{cases} \quad (2)$$

where n – an arbitrary power of a natural number C represented in the SRC.

Note that the following equalities hold in the SRC:

$$D = \prod_{e=1}^{g} \mu_e = (0 \| 0 \| ... \| 0 \| 0 \| 0 \| ... \| 0) \quad (3)$$

and

$$\frac{D}{2} = \prod_{e=2}^{g} \mu_e = (1 \| 0 \| ... \| 0 \| 0 \| 0 \| ... \| 0) \quad (4)$$

where g – number of bases (modules) SRC.

At present, there is no effective method for raising the residues of integers represented in the SRC, by an arbitrary modulus to the power of a natural number, simultaneously, both in positive and negative numerical ranges, based on their representation in the AF. This circumstance significantly narrows the area of effective application of the SRC. Thus, research is relevant in the field of creating methods and algorithms for raising the residues of integers represented in the SRC, by an arbitrary modulus to the power of a natural number, both in positive and negative numerical ranges, based on their representation in the AF.

To develop a method for the process of raising integers to an arbitrary power of a natural number in the SRC, it is necessary to synthesize a mathematical model for the process of raising the residues of integers C'_{SRC}, represented in the SRC, by an arbitrary modulo μ_e to the power n of a natural number of the form:

$$(C^n_{SRC})' = f(C'_{SRC}) \quad (5)$$

In this case, it is necessary to obtain an analytical expression (5), which determines the dependence of the result C^n_{SRC} of the operation of raising the number C_{SRC} in the SRC to the power

n, presented in the AF, on the value of the number C'_{SRC}, directly represented in the AF.

4. Proof of the mathematical model

Let's show that as a mathematical model of the process of raising integers C_{SRC} to an arbitrary power n of a natural number in the SRC, it is advisable to consider the mathematical expression:

$$(C^n_{SRC})' = (C'_{SRC})^n \tag{6}$$

Let's prove expression (6) by mathematical induction on n.

First step. Let's check the correctness of expression (6) for the minimum value $n = 2 = \min$, i.e. when squaring numbers.

In accordance with the definition of AF numbers in the SRC, get it that:

$$\begin{cases} C'_{SRC} = \dfrac{D}{2} + C_{SRC} \\ (C^n_{SRC})' = \dfrac{D}{2} + C^n_{SRC} \end{cases} \tag{7}$$

Taking into account the numerical ranges of changes in the values of C_{SRC} and C'_{SRC}, expression (7) can be represented as:

$$(C^n_{SRC})' = \left(\frac{D}{2} + C^n_{SRC} \right) \bmod D \tag{8}$$

Let's carry out the following numerical transformations:

$$(C'_{SRC})^2 = C'_{SRC} \cdot C'_{SRC} = (\frac{D}{2} + C_{SRC}) \cdot (\frac{D}{2} + C_{SRC}) = \\ = C^2_{SRC} + C_{SRC} \cdot D + \frac{D}{2} \cdot \frac{D}{2} \tag{9}$$

Taking into account expressions (3) and (4), obtain that:

$$C_{SRC} \cdot D = (c_1 \| c_2 \| ... \| c_{e-1} \| c_e \| c_{e+1} \| ... \| c_g) \times \\ \times (0 \| 0 \| ... \| 0 \| 0 \| 0 \| ... \| 0) = 0 \tag{10}$$

and

$$\frac{D}{2} \cdot \frac{D}{2} = (1 \| 0 \| ... \| 0 \| 0 \| 0 \| ... \| 0) \times \\ \times (1 \| 0 \| ... \| 0 \| 0 \| 0 \| ... \| 0) = \\ = (1 \| 0 \| ... \| 0 \| 0 \| 0 \| ... \| 0) = \frac{D}{2} \tag{11}$$

In this case, expression (9) will be presented in the form:

$$(C'_{SRC})^2 = C^2_{SRC} + \frac{D}{2} \tag{12}$$

In this case, based on expression (7), have that:

$$C^2_{SRC} = (C^2_{SRC})' - \frac{D}{2} \tag{13}$$

Substituting the value of C^2_{SRC} (13) into expression (12), obtain that:

$$(C'_{SRC})^2 = (C^2_{SRC})' - \frac{D}{2} + \frac{D}{2}$$

or

$$(C'_{SRC})^2 = (C^2_{SRC})' \tag{14}$$

Analytical expression (14) is the mathematical model of the process of raising the residues of integers to an arbitrary power of a natural number in the SRC in different numerical ranges.

Second step. Let's assume that the mathematical model is valid for an arbitrary admissible value of n, i.e. $(C^n_{SRC})' = (C'_{SRC})^n$.

Third step. Let's show that expression (6) is also valid for an arbitrary admissible value $n+1$, i.e. the condition:

$$(C^{n+1}_{SRC})' = (C'_{SRC})^{n+1} \tag{15}$$

From expression (15) have that $(C'_{SRC})^{n+1} = (\frac{D}{2} + C_{SRC})^{n+1}$. Let's expand the expression $(\frac{D}{2} + C_{SRC})^{n+1}$ in the form of Newton's binomial, obtain the following analytical expression:

$$\left(\frac{D}{2} + C_{SRC} \right)^{n+1} = \left(\frac{D}{2} \right)^{n+1} + B^1_{n+1} \cdot \left(\frac{D}{2} \right)^n \cdot C_{SRC} \cdot \\ + B^2_{n+1} \cdot \left(\frac{D}{2} \right)^{n-1} \cdot C^2_{SRC} + ... + C^{n+1}_{SRC} \tag{16}$$

where B^k_{n+1} – a binomial coefficient [25].

Taking into account expressions (3) and (4), the analysis of expression (16) showed that when reducing similar terms, two terms remain $\frac{D}{2}$ and C^{n+1}_{SRC}. The remaining terms of expression (16) will be zero. In this case, $\frac{D}{2} + C^{n+1}_{SRC} = (C^{n+1}_{SRC})'$. Thus, condition (15) is satisfied, i.e., received by mathematical model $(C^n_{SRC})' = (C'_{SRC})^n$ the process of raising integers C_{SRC} to an arbitrary power n of a natural number in theSRC.

Consider examples of the implementation of the process of raising integers to an arbitrary power of a natural number for a specific SRC given by the bases (modules) $\mu_1 = 3$, $\mu_2 = 4$ and $\mu_3 = 5$, wherein $D = 3 \cdot 4 \cdot 5 = 60$. The total

volume of positive code words C_{SRC} in the SRC is presented in Table 1.

Table 1
The code words in the SRC

C_{PNS}	C_{SRC} $\mu_1 = 3$	$\mu_2 = 4$	$\mu_3 = 5$
0	0	0	0
1	1	1	1
2	2	2	2
3	0	3	3
4	1	0	4
5	2	1	0
6	0	2	1
7	1	3	2
8	2	0	3
9	0	1	4
10	1	2	0
11	2	3	1
12	0	0	2
13	1	1	3
14	2	2	4
15	0	3	0
16	1	0	1
17	2	1	2
18	0	2	3
19	1	3	4
20	2	0	0
21	0	1	1
22	1	2	2
23	2	3	3
24	0	0	4
25	1	1	0
26	2	2	1
27	0	3	2
28	1	0	3
29	2	1	4
30	0	2	0
31	1	3	1
32	2	0	2
33	0	1	3
34	1	2	4
35	2	3	0
36	0	0	1
37	1	1	2
38	2	2	3
39	0	3	4
40	1	0	0
41	2	1	1
42	0	2	2
43	1	3	3
44	2	0	4
45	0	1	0
46	1	2	1
47	2	3	2
48	0	0	3
49	1	1	4
50	2	2	0
51	0	3	1
52	1	0	2
53	2	1	3
54	0	2	4
55	1	3	0
56	2	0	1
57	0	1	2
58	1	2	3
59	2	3	4

Table 2 shows the correspondence between the initial numerical data C_{PNS} and their AF C'_{PNS} in the PNS.

Table 2
Correspondence of the initial numerical data with their artificial forms in the PNS

C_{PNS}	C'_{PSN}	C_{PNS}	C'_{PSN}	C_{PNS}	C'_{PSN}
-30	0	-10	20	10	40
-29	1	-9	21	11	41
-28	2	-8	22	12	42
-27	3	-7	23	13	43
-26	4	-6	24	14	44
-25	5	-5	25	15	45
-24	6	-4	26	16	46
-23	7	-3	27	17	47
-22	8	-2	28	18	48
-21	9	-1	29	19	49
-20	10	0	30	20	50
-19	11	1	31	21	51
-18	12	2	32	22	52
-17	13	3	33	23	53
-16	14	4	34	24	54
-15	15	5	35	25	55
-14	16	6	36	26	56
-13	17	7	37	27	57
-12	18	8	38	28	58
-11	19	9	39	29	59

5. Examples of the process of raising integers to an arbitrary power of a natural number in the SRC

Let's give some examples of determining the value C_{SRC}^{n} for a specific SRC given by the bases

(modules) $\mu_1 = 3,\ \mu_2 = 4$ and $\mu_3 = 5,$ wherein $D = 60.$

Example 1.Let it be given that: $C_{PNS} = -3,$ $n = 3$. It is necessary to determine the value of C_{PNS}^3 in the SRC. Since the number $C_{PNS} = -3 < 0,$ then in the AF the number $C_{PNS} = -3$ in the PNS is represented as follows: $C'_{PNS} = \frac{D}{2} - C_{PNS} = \frac{60}{2} - 3 = 30 - 3 = 27$. In the SRC (based on the data in Table 1) the number C'_{PNS} is represented as: $C'_{SRC_{27}} = (0 \| 3 \| 2).$

After the first iteration of the multiplication, that is, multiplying the value C'_{SRC} by itself $C'_{SRC} \times C'_{SRC} = (0 \| 3 \| 2) \times (0 \| 3 \| 2),$ that is $0 \cdot 0 = 0 (\mathrm{mod}\, 3),\ 3 \cdot 3 = 1 (\mathrm{mod}\, 4)$ and $2 \cdot 2 = 4 (\mathrm{mod}\, 5)$ as a result, gets that $(C'_{SRC})^2 = (0 \| 1 \| 4).$ Since $n = 3$, then carry out the second iteration of the multiplication operation $(C'_{SRC})^3 = (C'_{SRC})^2 \times C'_{SRC} = (0 \| 1 \| 4) \times (0 \| 3 \| 2),$ that is $0 \cdot 0 = 0 (\mathrm{mod}\, 3),\ 1 \cdot 3 = 3 (\mathrm{mod}\, 4)$ and $4 \cdot 2 = 3 (\mathrm{mod}\, 5)$ as a result, gets that $(C'_{SRC})^3 = (0 \| 3 \| 3).$ In accordance with the data of Table 1, it has that in the SRC $(0 \| 3 \| 3)$ corresponds to the value 3in the AF in the PNS, i.e. $(0 \| 3 \| 3) = 3$.

Check of the result: $(C'_{SRC})^3 = 27^3 = 27 \times 27 \times 27 = 19683 = 3 (\mathrm{mod}\, 60) =$ $= (0 \| 3 \| 2) \times (0 \| 3 \| 2) \times (0 \| 3 \| 2) = (0 \| 3 \| 3) = 3.$ According to Table 2, the value3 in the AF corresponds to the value of -27.

$$(C_{PNS}^3)' = \frac{D}{2} + C_{PNS}^3,\ C_{PNS}^3 = (C_{PNS}^3)' - \frac{D}{2},$$

$$(-3)^3 = 3 - \frac{60}{2} = 3 - 30 = -27.$$

Thus, gets that $(-3)^3 = -27$. The result of the operation is valid.

Example 2.Let it be given that: $C_{PNS} = 3,\ n = 3$. It is necessary to determine the value of C_{PNS}^3 in the SRC. Since the number $C_{PNS} = 3 > 0,$ then in the AF the number $C_{PNS} = 3$ in the PNS is represented as follows: $C'_{PNS} = \frac{D}{2} + C_{PNS} = \frac{60}{2} + 3 = 30 + 3 = 33$. In the SRC (based on the data in Table 1) the number C'_{PNS} is represented as: $C'_{SRC_{33}} = (0 \| 1 \| 3).$

The result of the operation of raising the number C_{PNS} to the SRC in the AF is determined as follows (since $n = 3$): $(C'_{SRC})^3 = C'_{SRC} \times C'_{SRC} \times C'_{SRC} = (0 \| 1 \| 3) \times (0 \| 1 \| 3) \times$ $\times (0 \| 1 \| 3)$ that is $0 \cdot 0 \cdot 0 = 0 (\mathrm{mod}\, 3),$ $1 \cdot 1 \cdot 1 = 1 (\mathrm{mod}\, 4)$ and $3 \cdot 3 \cdot 3 = 2 (\mathrm{mod}\, 5)$ as a result, gets that $(C'_{SRC})^3 = (0 \| 1 \| 2).$ In accordance with the data of Table 1, it has that in the SRC $(0 \| 1 \| 2)$ corresponds to the value 57in the AF in the PNS, i.e. $(0 \| 1 \| 2) = 57$.

Check of the result: $(C'_{SRC})^3 = 33^3 = 33 \times 33 \times 33 = 35937 = 57 (\mathrm{mod}\, 60) =$ $= (0 \| 1 \| 3) \times (0 \| 1 \| 3) \times (0 \| 1 \| 3) = (0 \| 1 \| 2) = 57.$ According to Table 2, the value 57 in the AF corresponds to the value of 27 in the PNS.

$$(C_{PNS}^3)' = \frac{D}{2} + C_{PNS}^3,\ C_{PNS}^3 = (C_{PNS}^3)' - \frac{D}{2},$$

$$3^3 = 57 - \frac{60}{2} = 57 - 30 = 27.$$

Thus, gets that $(3)^3 = 27$. The result of the operation is valid.

Example 3. Let it be given that: $C_{PNS} = -2,$ $n = 2$. It is necessary to determine the value of C_{PNS}^2 in the SRC. Since the number $C_{PNS} = -2 < 0,$ then in the AF the number $C_{PNS} = -2$ in the PNS is represented as follows: $C'_{PNS} = \frac{D}{2} - C_{PNS} = \frac{60}{2} - 2 = 30 - 2 = 28$. In the SRC (based on the data in Table 1) the number C'_{PNS} is represented as: $C'_{SRC_{28}} = (1 \| 0 \| 3).$

The result of the operation of raising the number C_{PNS} to the SRC in the AF is determined as follows (since $n = 2$): $(C'_{SRC})^2 = C'_{SRC} \times C'_{SRC} = (1 \| 0 \| 3) \times (1 \| 0 \| 3),$ that is $1 \cdot 1 = 1 (\mathrm{mod}\, 3),\ 0 \cdot 0 = 0 (\mathrm{mod}\, 4)$ and $3 \cdot 3 = 4 (\mathrm{mod}\, 5)$ as a result, gets that $(C'_{SRC})^2 = (1 \| 0 \| 4).$ In accordance with the data of Table 1, it has that in the SRC $(1 \| 0 \| 4)$ corresponds to the value 4 in the AF in the PNS, i.e. $(1 \| 0 \| 4) = 4$.

Check of the result: $(C'_{SRC})^2 = 28^2 = 28 \times 28 = 784 = 4 (\mathrm{mod}\, 60) =$ $= (1 \| 0 \| 3) \times (1 \| 0 \| 3) = (1 \| 0 \| 4) = 4.$ The result of the operation: $(C_{PNS}^2)' = \frac{D}{2} + C_{PNS}^2,$

$C_{PNS}^2 = (C_{PNS}^2)' - \frac{D}{2} = 4 - 30 = -26$. According to Table 2, the value -26 corresponds to the value 4.

Thus, gets that $(-2)^2 = 4$. The result of the operation is valid.

Example 4.Let it be given that: $C_{PNS} = -2$, $n = 3$. It is necessary to determine the value of C_{PNS}^3 in the SRC. Since the number $C_{PNS} = -2 < 0$, then in the AF the number $C_{PNS} = -2$ in the PNS is represented as follows: $C'_{PNS} = \frac{D}{2} - C_{PNS} = \frac{60}{2} - 2 = 30 - 2 = 28$. In the SRC (based on the data in Table 1) the number C'_{PNS} is represented as: $C'_{SRC_{28}} = (1\|0\|3)$.

The result of the operation of raising the number C_{PNS} to the SRC in the AF is determined as follows (since $n = 3$): $(C'_{SRC})^3 = C'_{SRC} \times C'_{SRC} \times C'_{SRC} = (1\|0\|3) \times (1\|0\|3) \times \times (1\|0\|3)$ that is $1 \cdot 1 \cdot 1 = 1 (\mathrm{mod}\, 3)$, $0 \cdot 0 \cdot 0 = 0 (\mathrm{mod}\, 4)$ and $3 \cdot 3 \cdot 3 = 2 (\mathrm{mod}\, 5)$ as a result, gets that $(C'_{SRC})^3 = (1\|0\|2)$. In accordance with the data of Table 1, it has that in the SRC $(1\|0\|2)$ corresponds to the value 52 in the AF in the PNS.

Check of the result: $(C'_{SRC})^3 = 28^3 = 28 \times 28 \times 28 = 21952 = 52 (\mathrm{mod}\, 60) = = (1\|0\|3) \times (1\|0\|3) \times (1\|0\|3) = (1\|0\|2) = 52.$

The result of the operation: $(C_{PNS}^3)' = \frac{D}{2} + C_{PNS}^3$,

$C_{PNS}^3 = (C_{PNS}^3)' - \frac{D}{2}$, $C_{PNS}^3 = 52 - 30 = 22.$

According to Table 2, the value 22 in the AF corresponds to the value -8 in the PNS.

Thus, gets that $(-2)^3 = -8$. The result of the operation is valid.

Conclusions

In order to raise integers to an arbitrary power of a natural number in the non-positional number systems, this article synthesizes a mathematical model for the process of raising integers to an arbitrary power of a natural number in the SRC, both in positive and negative numerical ranges. To confirm the reliability of the obtained mathematical model, the proof of the obtained mathematical relation was carried out by the method of mathematical induction on n. The resulting mathematical model can be used as the basis for the data processing procedure in the SRC, both in positive and negative numerical ranges. Analytical ratio, which is a mathematical model of the process of raising integers in the SRC, is implemented by applying a special coding of numbers in the AF. The possibility of implementing the operation of raising integers to an arbitrary power n of a natural number, in a negative numerical range, significantly expands the area of effective application of the SRC. The reference material presented in the article (Table 1 and Table 2) can be used when using a synthesized mathematical model. Examples of the specific execution of the operation of raising integers, represented in the SRC, to various powers n of a natural number are given. Analysis of the results of solving examples showed the reliability and practical value of the developed mathematical model of the process of raising integers to an arbitrary power of a natural number in the SRC.

It is necessary to note the following that the non-positional number system in the residual classes has three basic properties: independence, equality and low-bitness of the residues that form the non-positional code structure in the SRC. These properties are due to the principles of code formation in the SRC. Let us briefly consider how the properties of the SRC qualitatively affect the process of raising integers to an arbitrary power of a natural number in the SRC, both in positive and negative numerical ranges. The property of the independence of the residues allows you to implement the operation of raising integers to an arbitrary power of a natural number for each of the residues, regardless of the rest of the residues. In this case, an error that occurred in one of the residues doesn't propagate into the remaining residues of the non-positional code structure in the SRC [26-27].

The low-bitness of the residues involves the processing of large data arrays, by means of small natural numbers. This property can significantly increase the reliability and performance of devices for constructing integers. This is achieved both due to the low-bitness (low-digit) construction of devices for raising integers, and due to the possibility of using (unlike PNS) tabular arithmetic [28], where the arithmetic operations of addition, subtraction and multiplication are performed almost in one

machine cycle. In particular, the low-bitness of the residues in the representation of numbers in the SRC makes it possible to choose a wide range of options for system engineering solutions when implementing modular arithmetic operations based on the following principles [29]: the summation principle (based on the use of low-bit binary modulo adders) [30]; tabular principle (based on the use of permanent storage devices of small sizes) [31]; the principle of ring shift(based on the use of ring shift registers) [32].This circumstance makes it possible to implement a device for raising integers to an arbitrary power modulo μ_e SRC of low-bitness (low-digit capacity). This increases the efficiency of using SRC to create devices for raising integers to an arbitrary power of a natural number in the SRC, both in positive and negative numerical ranges.

References

[1] I.Ya. Akushskii, D.I. Yuditskii, Machine Arithmetic in Residual Classes, Sov. Radio, Moscow, 1968.

[2] M. Weiser, The computer for the 21st Century, IEEE Pervasive Computing 1 (2002) 19–25. doi:10.1109/MPRV.2002.993141.

[3] V. A. Torgashov, System of residual classes and reliability of digital computers. Sov. radio, Moscow, 1973.

[4] P. Lyakhov, M. Bergerman, N. Semyonova, D. Kaplun, A. Voznesensky, Design Reverse Converter for Balanced RNS with Three Low-cost Modules, in: 2021 10th Mediterranean Conference on Embedded Computing (MECO), Budva, Montenegro, 2021, pp. 1–7. doi:10.1109/MECO52532.2021.9460200.

[5] I. Foster, C. Kesselman, The Grid: Blueprint for a New Computing Infrastructure, 2nd ed., Morgan Kaufmann, San Francisco, 2004.

[6] Michael D. Fried, Moshe Jarden, Fried, Field Arithmetic, Springer-Verlag, Berlin Heidelberg, 2008.

[7] N.I. Chervyakov, A.V. Veligosha, K.T. Tyncherov, S. A. Velikikh, Use of modular coding for high-speed digital filter design, Cybernetics and Systems Analysis 34 (1998) 254–260. doi:10.1007/BF02742075.

[8] B. Gérard, J.-G. Kammerer, N. Merkiche, Contributions to the Design of Residue Number System Architectures, in: Proceedings 22nd IEEE International Symposium on Computer Arithmetic, Lyon, 2015, pp. 105–112. doi:10.1109/ARITH.2015.25.

[9] C. Huang, D. Peterson, H. Rauch, J. Teague, D. Fraser, Implementation of a fast digital processor using the residue number system, IEEE Transactions on Circuits and Systems 28 (1981) 32–38. doi:10.1109/TCS.1981.1084905.

[10] E. B. Olsen, RNS Hardware Matrix Multiplier for High Precision Neural Network Acceleration: "RNS TPU", in: 2018 IEEE International Symposium on Circuits and Systems (ISCAS), Florence, Italy, 2018, pp. 1–5. doi:10.1109/ISCAS.2018.8351352.

[11] S. Onyshchenko, A. Yanko, A. Hlushko, S. Sivitska, Increasing Information Protection in the Information Security Management System of the Enterprise, volume 181 of Lecture Notes in Civil Engineering, Springer-Verlag, Cham, 2022. doi:10.1007/978-3-030-85043-2_67.

[12] M. H. El-Mahdy, S. A. Maged, M. I. Awad, End-to-End Fault Tolerant Control of Discrete Event System Using Recurrent Neural Networks, in: 2022 2nd International Mobile, Intelligent, and Ubiquitous Computing Conference (MIUCC), Cairo, 2022, pp. 266–271. doi:10.1109/MIUCC55081.2022.9781748.

[13] C. Böhm, C. Plant, Mining Massive Vector Data on Single Instruction Multiple Data Microarchitectures, in: 2015 IEEE International Conference on Data Mining Workshop (ICDMW), Atlantic City, NJ, 2015, pp. 597–606. doi:10.1109/ICDMW.2015.85.

[14] David A. Patterson, Series in Computer Architecture and Design, 1 ed., The Morgan Kaufmann, 2016.

[15] H. M. Waidyasooriya, D. Ono, M. Hariyama, M. Kameyama, Efficient data transfer scheme using word-pair-encoding-based compression for large-scale text-data processing, in: 2014 IEEE Asia Pacific Conference on Circuits and Systems (APCCAS), Ishigaki, 2014, pp. 639–642. doi:10.1109/APCCAS.2014.7032862.

[16] A. Fechan, I. Kremer, Y. Bashtyk and O. Boyko, Computer simulation of optical and

dynamic properties of the polymer – Liquid crystal system for optoelectronics devices, in: 2017 2nd International Conference on Advanced Information and Communication Technologies (AICT), Lviv, 2017, pp. 278–281. doi:10.1109/AIACT.2017.8020119.

[17] S. Gavrylenko, I. Sheverdin, M. Kazarinov, M., The ensemble method development of classification of the computer system state based on decisions trees, Advanced Information Systems 4 (2020) 5–10. doi:10.20998/2522-9052.2020.3.01.

[18] T. A. Kholomina, S. I. Malchenko, V. V. Gudzev, N. B. Rybin, Computer simulation of experimental methods to investigate materials and structures of micro- and nanoelectronics, in: 2017 6th Mediterranean Conference on Embedded Computing (MECO), Bar, 2017, pp. 1–5. doi: 10.1109/MECO.2017.7977225.

[19] V.Krasnobayev, A.Kuznetsov, I.Lokotkova, A.Kiian, T.Kuznetsova Techniques for Raising the Remainder to a Power in the System of Residual Classes, in: 2020 IEEE 11th International Conference on Dependable Systems, Services and Technologies (DESSERT), Kyiv, 2020, pp.145–150. doi: 10.1109/DESSERT50317.2020.9125049.

[20] V. A. Pavsky, K. V. Pavsky, A. A. Paznikov, M. S. Kupriyanov, Mathematical models and the effectiveness of functioning of scalable distributed computer systems with group and full restorations, in: 2017 XX IEEE International Conference on Soft Computing and Measurements (SCM), Saint Petersburg, 2017, pp. 496–499. doi:10.1109/SCM.2017.7970628.

[21] M. Stamp, Information Security: Principles and Practice, 3nd. ed., Wiley, 2021.

[22] D. Schinianakis, T. Stouraitis, Number Systems in Cryptography: Design, Challenges, Robustness, 2016. doi:10.1007/978-3-319-14971-4_4

[23] A. Yanko, S. Koshman, V. Krasnobayev, Algorithms of data processing in the residual classes system, in: 2017 4th International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T), Kharkov, 2017, pp.117–121. doi:10.1109/INFOCOMMST.2017.8246363.

[24] Z. Ulman, M. Czyzak, J. Zurada, Effective RNS scaling algorithm with the Chinese remainder theorem decomposition, in: Proceedings of IEEE Pacific Rim Conference on Communications Computers and Signal Processing, Rim, 1993, pp. 528–531. doi:10.1109/PACRIM.1993.407305.

[25] K. Youngmee, R. Sangwook, The Origin of Newton's Generalized Binomial Theorem, Journal for History of Mathematics 27 (2014) 127–138. doi:10.14477/jhm.2014.27.2.127.

[26] P. V. A. Mohan, Residue Number Systems: Theory and Applications, Birkhäuser Basel, Switzerland, 2016.

[27] R. Liu, L. Li, Y. Yang, Performance Residual Based Fault Detection for Feedback Control Systems, IEEE Transactions on Circuits and Systems II: Express Briefs 68 (2021) 3291–3295. doi:10.1109/TCSII.2021.3062718.

[28] B. Parhami, Modular reduction by multi-level table lookup, in: Proceedings of 40th Midwest Symposium on Circuits and Systems. Dedicated to the Memory of Professor Mac Van Valkenburg, Sacramento, CA, USA, 1997, pp. 381–384. doi:10.1109/MWSCAS.1997.666114.

[29] Tao Chen, Bin Yu, Jin-Hai Su, Zi-bin Dai, Jian-Guo Liu, A reconfigurable modular arithmetic unit for public-key Cryptography, in: 2007 7th International Conference on ASIC, Guilin, 2007, pp. 850–853. doi:10.1109/ICASIC.2007.4415764.

[30] Y. Wang, X. Song, M. Aboulhamid, H. Shen, Adder based residue to binary number converters for (2/sup n/-1, 2/sup n/, 2/sup n/+1), IEEE Transactions on Signal Processing 50 (2002) 1772–1779. doi:10.1109/TSP.2002.1011216

[31] M. G. Arnold, The Residue Logarithmic Number System: Theory and Implementation, in: 17th IEEE International Symposium on Computer Arithmetic, 2005, pp. 196–205. doi:10.1109/ARITH.2005.44.

[32] Z. Guo, Z. Gao, H. Mei, M. Zhao, J. Yang, Design and Optimization for Storage Mechanism of the Public Blockchain Based on Redundant Residual Number System, IEEE Access 7 (2019) 98546–98554. doi:10.1109/ACCESS.2019.2930125.