Correction Codes in the System of Residual Classes

Victor Krasnobayev
Electronics and Control Systems Department
V. N. Karazin Kharkiv National University
Kharkiv, Ukraine
v.a.krasnobaev@gmail.com

Alexandr Kuznetsov
Department of Information Systems and Technologies Security
V. N. Karazin Kharkiv National University,
Kharkiv, Ukraine
kuznetsov@karazin.ua

Alina Yanko
Department of Computer Engineering
Poltava National Technical Yuri Kondratyuk
University, Poltava, Ukraine
al9_yanko@ukr.net

Kateryna Kuznetsova
Department of Information Systems and Technologies Security
V. N. Karazin Kharkiv National University,
Kharkiv, Ukraine
kate.kuznetsova.2000@gmail.com

***Abstract*—The report considers correction codes with mutually non-prime bases (CMNPB). To date, almost no one has been engaged in a deep study of the corrective properties of systems of residual classes (SRC), the bases of which are not mutually prime numbers. Such a system has certain corrective properties, which makes it necessary to assess the possibility and feasibility of using CMNPB to increase the reliability of computing in computer systems (CS). For the purpose of further research and development of CMNPB, we will consider a number of scientific statements, the use of the results of which will allow us to more fully study the corrective properties of codes with non-prime bases. Algorithms for monitoring and correcting errors in the SRC with mutually non-prime in pairs bases have been developed. Using these algorithms makes it relatively easy to implement a procedure for detecting and correcting one-time errors. Note that by the simplicity of the design of the decoder circuits, CMNPB have no analogues in the positional number systems. This is achieved by limiting the class of possible correctable errors, by introducing additional hardware redundancy in the representation of code words.**

Keywords—computer system, correction codes with mutually non-prime bases, correction codes with mutually prime bases, accuracy of computing of computer systems in the system of residual classes

I. Introduction

It is known that in the nonpositional number system in the residual classes (SRC), correction codes with mutually prime bases (CMPB) are widely used [1-12]. This is due to the simplicity of the formation of the structure of these codes, good corrective capabilities, as well as the relative simplicity of their construction for any given minimum code distance [13-15].

In this paper corrective codes with mutually non-prime bases (CMNPB) are considered. In the literature, CMNPB are described qualitatively rather than quantitatively [15]. The fact is that so far almost no one has been deeply involved in the study of the corrective properties of systems of residual classes, whose bases are not mutually prime numbers [16-21]. Such a system also has certain corrective properties, which makes it necessary to assess the possibility and feasibility of using CMNPB to increase the reliability of computing computer systems (CS) [22-24]. In some cases the use of the system of residue allows effectively to realize the different methods of information security [21-23, 25-30].

II. Scientific Statements on Error Correction

Lemma. For any integer $A=(a_1, a_2, ..., a_n)$ in the system of residual classes with bases m_i $(i=\overline{1, n})$ and for any pair of bases m_i and m_j the condition $(a_i-a_j)\equiv 0(\mathrm{mod}\, d_{ij})$ must be satisfied, where $d_{ij}(m_i, m_j)$ where the greatest common divisor (GCD) of the bases (modules) m_i and m_j, while $i, j=\overline{1, n}$; $i\neq j$. So, according to the results of the lemma, to determine the necessary and sufficient conditions for the detection of one-time errors with the help of CMNPB, we formulate and prove the following SS [14].

For the purpose of further research and development of CMNPB, we will consider a number of scientific statements (SS), the use of the results of which will allow us to more fully study the corrective properties of codes with non-prime grounds.

SS 1. To detect errors in the residual of an arbitrary base m_i $(i=\overline{1, n})$ of a number $A=(a_1, a_2, ..., a_n)$, specified in the system of residual classes with bases $m_1, m_2, ..., m_n$, it is necessary that the base m_i has at least one, different from one, common divisor with the other bases m_i $(i\neq j)$.

Proof. Let the GCD $d_{ij}(m_i, m_j)$ be defined for arbitrary SRC bases $(i\neq j)$, and the error occurred at the base m_i, i.e. $a_i=a_i+\Delta a_i$. We show that the expression $(a_i-a_j)\,\mathrm{mod}\, d_{ij}$ is equivalent to $\Delta a_i(\mathrm{mod}\, d_{ij})$. According to the lemma, the following equality holds $(a_i-a_j)=0(\mathrm{mod}\, d_{ij})$. We write the expression $a_i+\Delta a_i=a_i(\mathrm{mod}\, m_i)$ in the form $a_i+\Delta a_i=m\cdot m_i+a_i$, where m is an integer. From the last expression we define the distorted residual $a_i=a_i+\Delta a_i-m\cdot m_i$. Then we can write that $a_i-a_j=\left[(a_i-a_j)+(-mkd_{ij})+\Delta a_i\right]$. Since

$(a_i - a_j) \equiv 0(\mathrm{mod}\, d_{ij})$ and $-mkd_{ij} \equiv 0(\mathrm{mod}\, d_{ij})$, where $m_i = kd_{ij}$, and k is a positive integer, the following comparison is made $(a_i - a_j) \equiv \Delta a_i(\mathrm{mod}\, d_{ij})$. Obviously, in the absence of common dividers, i.e. if $d_{ij} = 1$, then we have that $\Delta a_i \equiv (\mathrm{mod}\, d_{ij})$. This proves the necessary condition of SS 1. The necessary condition of the theorem is sufficient if the error is not a multiple of the divisor d_{ij}. Indeed, $(md_{ij} + a_{ij}) \neq 0(\mathrm{mod}\, d_{ij})$, for $0 < a_{ij} < d_{ij}$.

In order to determine the necessary and sufficient conditions for correcting one-time errors with the help of CMNPB, we formulate and prove the following SS 2..

SS 2. To correct an error in the residual at an arbitrary base m_i of the number $A = (a_1, a_2, ..., a_n)$, specified in the system of residual classes with bases $m_1, m_2, ..., m_n$, it is necessary that the condition is met:

$$(d_{ik} - 1)(d_{ij} - 1) \geq m_i - 1 - (K_{d_{ik}} + K_{d_{ij}} - K_{[d_{ik}, d_{ij}]}), \quad (1)$$

where $d_{ik} = (m_i, m_k)$, $d_{ij} = (m_i, m_j)$; $K_{d_{ik}}$ – the number of divisors, multiples of d_{ik}; $K_{d_{ij}}$ – the number of divisors, multiples of d_{ij}; $K_{[d_{ik}, d_{ij}]}$ – the number of divisors, multiples of the least common multiple (LCM) $[d_{ik}, d_{ij}]$ of the divisors d_{ik} and d_{ij}, $(i \neq j)$.

Proof. Calculate the values a_{ij}, a_{ik}, a_{jk}. If the error occurred at the base m_i, then $a_{ik} = 0$, and $a_{ij} \neq 0$ and $a_{ik} \neq 0$. The number of different combinations a_{ij}, a_{ik}, is $(d_{ij} - 1) \cdot (d_{ik} - 1)$, where $(d_{ij} - 1)$ is the number of possible values of a_{ij} ($a_{ij} \neq 0$), $(d_{ik} - 1)$ – is the number of possible values of a_{ik} ($a_{ik} = 0$), and the number of possible values of errors for a base m_i is $m_i - 1$ $(\Delta a_i \neq 0)$ minus the number of undetected errors. The number of undetected errors consists of the number of errors, multiples of the divisor $d_{ik} - K_{d_{ik}}$ and multiples of the divisor $d_{ik} - K_{d_{ik}}$. Thus, the number of possible values of detectable errors is equal to the value $m_i - 1 - (K_{d_{ik}} + K_{d_{ij}} - K_{[d_{ik}, d_{ij}]})$. To ensure compliance with the possible values of the errors on the m_i it is necessary for equation (1) to be true. Q.E.D.

The method of correction of one-time errors, allowing to correct errors that are multiples of one of the divisors $d_{i-1\ i}$ or $d_{i\ i+1}$, consists in the following. Let a SRC be set with mutually not simple bases, i.e. GCD is defined as follows $(m_1, m_2, ..., m_n) \geq 2$. Let the number in the SRC be $A_{ucn} = (a_1, a_2, ..., a_n)$. We define all values $a_{k\ k+1}$, i.e. $a_{12}, a_{23}, a_{34}, ..., a_{n-1\ n}, a_{n\ 1}$. Without breaking the generality of reasoning, we assume that $a_{i\ i+1} \neq 0$, and all other values $a_{k\ k+1} \neq 0$. Since $a_{i\ i+1} = (a_i - a_{i+1}) \mathrm{mod}\, d_{i\ i+1} \neq 0$, the error can be present only in the residues on the bases m_i or m_{i+1}. Because of this, two hypotheses are possible: an error is present in the residual a_i and an error is present in the residual a_{i+1}. Before we consider the error correction process by the proposed method, we formulate and prove the following SS 3. We use the result of the proof of SS 3 when determining the convergence process of the totality of numbers of the form $A^{(k_i)} = (a_1, ..., a_{i-1}, a_{ik_i}, a_{i+1}, ..., a_n)$ to the correct number $A^{(\rho)} = (a_1, ..., a_{i-1}, a_{i\rho}, a_{i+1}, ..., a_n)$.

SS 3. Suppose that in the ordered ($m_{i-1} < m_i; i = \overline{1, n}$) system of residual classes with bases $m_1, m_2, ..., m_n$ the wrong number (distorted in one residue) is given $A = (a_1, a_2, ..., a_{i-1}, a_i, a_{i+1}, ..., a_n)$ and let $\Delta a_i = a_i - a_i = k_i d_{i-1\,i}$. Then, in the aggregate of values $a_{ik_i} = (a_i - k_i d_{i-1\,i}) \mathrm{mod}\, m_i$ there is a single value $a_{i\rho}$, at which the number $A^{(\rho)} = (a_1, a_2, a_{i\rho}, ..., a_n)$ is the correct number, where $d_{i-1\,i}(m_{i-1}, m_i)$, and k_i may take values $k_i = 1, 2, ..., m_i / d_{i-1\,i} - 1$.

III. Error Correction Algorithm

Imagine an error correction algorithm based on the result of a proven SS 3. Consider the first hypothesis. Since $a_{i-1\ i} = 0$, the error is a multiple of the divisor $d_{i-1\ i}$. Therefore, the error on the base can take values $\Delta a_i = kd_{i-1\,i}$, for $k_i = 1, 2, ..., m_i / d_{i-1\,i} - 1$. We calculate the set of values $a_{ik_1} = (a_i - k_i d_{i-1\,i}) \mathrm{mod}\, m_i$. If there is such a value a_{im} in this population for which $A^{(m)} = (a_1, a_2, ..., a_{im}, ..., a_n)$ is the correct number, then the first hypothesis is valid, i.e. the error is present in the remainder of the base m_i. In this case, the corrected number is the number $A_{ucn} = A^{(m)}$, where $a_{im} = (a_i - md_{i-1\,i}) \mathrm{mod}\, m_i$. If for all values of a_{ik_i} the number $A^{(k_i)}$ is incorrect, then the value a_i is correct, and the error occurred in the remainder of the base m_{i+1}. Since $a_{i+1\ i+2} = 0$, then the error on the basis m_{i+1} is of multiple divisor $d_{i+1\ i+2}$ i.e. $\Delta a_{i+1} = k_{i+1} d_{i+1\ i+2}$, where $k_{i+1} = 1, 2, ..., m_{i+1} / d_{i+1\,i+2} - 1$. Next, we define a set of the following values $a_{i+1\,k_{i+1}} = (a_{i+1} - k_{i+1} d_{i+1\ i+2}) \mathrm{mod}\, m_{i+1}$. On the basis of the obtained results of theorem 3, it follows that in this set there will necessarily be such a single number $a_{i+1\,N}$, for which the number $A^{(N)} = (a_1, a_2, ..., a_{i+1\,N}, ..., a_n)$ is the correct number. Note that the order of hypothesis testing is arbitrary and does not affect the probability of error correction. However, in order to increase the speed of determining the number of a distorted residue, it is first necessary to test the hypothesis for which the value $m_k / d_{k-1\ k}$ $(k = i, i+1)$ will be the least number.

IV. Example of Specific Implementation of the Error Correction Algorithm

An example of determining the correctness of a number. Let the SRC be given by the following bases $m_1 = 4$, $m_2 = 6$, $m_3 = 12$, $m_4 = 18$. Wherein $M = 36$,

$d_{12}=2,\ d_{23}=6,\ d_{34}=6,\ d_{41}=2$. It is necessary to determine the correctness of the number $A=(3, 5, 7, 7)$, and in case of its distortion, correct the wrong number.

1. Define the values $a_{12}=0,\ a_{23}=2,\ a_{34}=0,$ $a_{34}=0,\ a_{41}=0$. Since $a_{23}\neq 0$, the number A is incorrect, and the error occurred in the second or in the third residual.

2. Since $m_2/d_{12} > m_3/d_{34}$, then the first hypothesis is that the error is assumed in the residual of the base m_3.

3. Calculate the values $a_{3k_3}=a_3-k_3d_{23}$ for the value $k_3=1$.

We get $a_{3k_3}=a_3-k_3d_{23}=7-1\cdot 6=1$. The resulting number $A^{(1)}=(3, 5, 1, 7)$ is not a code word, i.e. the first hypothesis is not true. An error occurred in the residual of the base m_2.

4. We fix the number A. For this, by the values $k_3=1, 2$ we define the desired value $a_{2k_2}=a_2-k_2d_{21}$

$$k_2=1,\ a_{2k_2}=a_2-k_2d_{21}=5-1\cdot 2=3,$$

$$k_2=3,\ a_{2k_2}=a_2-k_2d_{21}=5-2\cdot 2=2.$$

Thus, we obtain two code words: $A^{(1)}=(3, 3, 7, 7)$ and $A^{(2)}=(3, 1, 7, 7)$. The only correct code word is the value $A^{(2)}$, i.e. $A_{ucn}=A^{(2)}=(3, 1, 7, 7)$.

The developed method of error correction in the SRC allows us to extend the class of corrected errors of the CS. This significantly expands the corrective capabilities of CMNPB [16-18, 31-34]. It is obvious that the process of detecting errors in the hardware-time aspect is implemented extremely simply. The time of error detection for the SRC, given by any base system, is always equal to three conditional time ticks and does not depend (as is observed for CMPB) on the number n of information bases.

We present some considerations that will simplify the above algorithm for error detection. First, we prove the equation $(a_1+\overline{a_i})=(\overline{a_1}+a_i)\bmod d_{1i}$, on the basis of which we compose an error correction algorithm. Let the remainder m_j in the operand $A=(a_1, a_2, ..., a_n)$ be distorted, i.e. $a_j=(a_j+\Delta a_j)\bmod m_j$.

We write the system of equations:

$$k_1=a_i-a_j=a_i+(m_j-a_j)=(a_i-a_j+m_j-\Delta a_j)\bmod m_j,$$

$$k_2=a_j-a_i=a_j+\Delta a_j-a_i=(a_j-a_i+a_j)=\bmod m_j.$$

We add these equations and get $k_1+k_2=m_j(\bmod m_j)$ or $k_1+k_2=0(\bmod d_{ij})$.

Thus, it is shown that equation

$$(a_1+\overline{a_i})=(\overline{a_1}+a_i)\bmod d_{1i}$$

holds, i.e. in the device for error detection instead of $n-1$ modulo m_i adders it is enough to have only one modulo m_1 adder. The developed algorithm for the implementation of the error detection process is determined by the following equations:

$$a_2+m_1-a_1=(a_2+\overline{a_1})\bmod d_{12},$$

$$a_3+m_1-a_1=(a_3+\overline{a_1})\bmod d_{13}.$$

The variants of devices for detecting errors in SRC considered above allow guaranteed detection of the fact of a number A distortion, however, this does not determine the number of the base on which the residual was distorted.

An example of a diagnostic process. The diagnosis of number A distortion is based on the following procedure. Consider this procedure for determining the number of the residue by which the number A. was distorted. Let the SRC be given by bases $m_1=4$, $m_2=6$, $m_3=12$, $m_4=18$. Wherein $L=M=[4, 6, 12, 18]=36$, $d_{12}=2,$ $d_{23}=6,$ $d_{34}=6,$ $d_{41}=2$, $A=(0, 2, 8, 2)$.

Let number A be distorted by base m_4, i.e. $a_4=(a_4-\Delta a_4)\bmod m_4$, and let $\Delta a_4=5$. In this case, at the output of the modulo m_2 adder we obtain the value $\overline{a_2}=m_2-a_2=4$; modulo m_3 we get $\overline{a_3}=m_3-a_3=4$, at the output of the modulo adder we get $m_4-\overline{a_4}=m_4-a_4=11$. At the output of the modulo d_{12} adder we get a number $(a_1+\overline{a_2})=0(\bmod d_{12})$, at the output of the modulo d_{23} adder we get the number $(a_1+\overline{a_3})=0(\bmod d_{23})$, at the output of the modulo d_{34} adder we get the number $(a_3+\overline{a_4})=0(\bmod d_{34})$, at the output of the modulo d_{41} we get the number $(a_4+\overline{a_1})=1(\bmod d_{41})$. At the inputs of the modulo d_{34} and d_{41} adders there is a non-zero result of the operation $(a_m+\overline{a_j})\bmod d_j$, therefore the fourth element I is open, i.e. a signal is present on the fourth output bus. It follows that the error occurred in the fourth residual a_4.

On the basis of the proven SS 3, a necessary condition for detecting an error in the modulo m_i residue is condition 1. This condition is also sufficient if the error $\Delta a_i=a_i-a_i$ is not a multiple of the divisors $d_{i-1\ i}$, d_{ii+1}, i.e. the following two dividers

$$d_{\Delta a_i}^{(i-1)}=(d_{i-1\ i}, \Delta a_i)=1,$$

$$d_{\Delta a_i}^{(i+1)}=(d_{ii+1}, \Delta a_i)=1.$$

In accordance with the results of SS 3, we construct an error correction algorithm for an arbitrary base m_i.

1. Define all possible values of type $(a_i-a_{i+1})=a_{i\ i+1}(\bmod d_{i\ i+1})$:

$$\begin{cases} a_1 - a_2 = a_{12}(\operatorname{mod} d_{12}), \\ a_2 - a_3 = a_{23}(\operatorname{mod} d_{23}), \\ \qquad \cdots \\ a_{n-1} - a_n = a_{n-1\ n}(\operatorname{mod} d_{n-1\ n}), \\ a_n - a_1 = a_{n1}(\operatorname{mod} d_{n1}), \end{cases} \qquad (2)$$

2. If all values of (2) are equal to zero, then either there is no error, or it is a multiple of each of the dividers d_{i-1}, $d_{i\,i+1}$, (a one-time error is assumed).

3. If $a_{i-1\ i} \neq 0$, $a_{i\ i+1} \neq 0$, and all other values $a_{ij} = 0$, the error occurred modulo m_i, i.e.

$$a_i = a_i + \Delta a_i \quad (1 \le \Delta a_i \le m_i - 1).$$

In accordance with the proven SS 3 a necessary condition for correcting the error in the residual is the condition (3), written in the general form:

$$(d_{ik} - 1)(d_{ij} - 1) \ge \delta(\Delta a_i), \qquad (3)$$

where

$$\delta(\Delta a_i) = m_i - 1 - (K_{d_{ik}} + K_{d_{ij}} - K_{[d_{ik}, d_{ij}]}).$$

In this case, we have the following notation: $K_{d_{ik}}$ – the number of possible error divisors Δa_i by the base m_i (i.e., the number of possible divisors of the number $m_i - 1$), that are multiples of the value d_{ik}; $K_{d_{ikj}}$ – the number of possible error Δa_i divisors by base m_i, multiples of the value d_{ij}; $K_{[d_{ik}, d_{ij}]}$ – the number of possible error Δa_i divisors by the base m_i, multiples of the SRC numbers d_{ik} and d_{ij}. Note that condition (3) is sufficient if different possible values $\delta(\Delta a_i)$ of error by base m_i $(i = \overline{1, n})$ correspond to different pairs of values a_{ik} and a_{ij}, where:

$$\delta(\Delta a_1) = m_1 - 1 - (K_{d_{12}} + K_{d_{31}} - K_{[d_{12}, d_{31}]}),$$
$$\delta(\Delta a_2) = m_2 - 1 - (K_{d_{12}} + K_{d_{23}} - K_{[d_{12}, d_{23}]}),$$
$$\delta(\Delta a_3) = m_3 - 1 - (K_{d_{23}} + K_{d_{31}} - K_{[d_{23}, d_{31}]}).$$

Let it be necessary to determine the correctness of the number $A = (11, 100, 0111)$ (Tables 1-3). The initial number A is entered in the first and second input registers. The first adder of the first group determines the value $\overline{a_1} = m_1 - a_1 = 01$, the second adder determines the value $\overline{a_2} = m_2 - a_2 = 010$, and the third adder determines the value $\overline{a_3} = m_3 - a_3 = 0101$. The first modulo d_{ij} adder determines the value $a_{12} = (a_1 + \overline{a_2})\operatorname{mod}_{12}$, the second adder $a_{23} = (a_2 + \overline{a_3})\operatorname{mod}_{23}$, the third adder $a_{31} = (a_3 + \overline{a_1})\operatorname{mod}_{13}$. Thus, from the outputs of the corresponding decoders, only the second switch receives the values $a_{12} = 1$, $a_{13} = 3$, according to which it determines the value of the error to be inverted modulo m_2, i.e. $\Delta\overline{a_2} = 3$, which through the second decoder in binary code is fed to the first input of the second adder, the second input of which receives the value

$$a_2 = a_2 + \Delta a_2 = 100.$$

The adder of the second group determines the result of the operation

$$(\Delta\overline{a_2} + a_2)\operatorname{mod} m_2 = (m_2 - \Delta a_2 + a_2 + \Delta a_2)\operatorname{mod} m_2 = 001.$$

The output of the device receives a corrected number $A = (11, 001, 0111)$.

TABLE I. TABLE OF SOLUTIONS

a_{31}	$a_{12} = 1$
1	$\Delta\overline{a_1} = 1$
2	–
3	$\Delta\overline{a_1} = 3$

TABLE II. TABLE OF SOLUTIONS

a_{23}	$a_{12} = 1$
1	$\Delta\overline{a_2} = 5$
2	–
3	$\Delta\overline{a_2} = 3$
4	–
5	$\Delta\overline{a_2} = 1$

TABLE III. TABLE OF SOLUTIONS

a_{31}	a_{23}				
	1	2	3	4	5
1	$\Delta\overline{a_3} = 7$	–	$\Delta\overline{a_3} = 3$	–	$\Delta\overline{a_3} = 11$
2	–	$\Delta\overline{a_3} = 2$	–	$\Delta\overline{a_3} = 10$	-
3	$\Delta\overline{a_3} = 1$	–	$\Delta\overline{a_3} = 9$	–	$\Delta\overline{a_3} = 5$

V. Conclusion

The report clarifies some aspects of the theory of CMNPB. Algorithms for monitoring and correcting errors of CS in SRC with mutual in pairs non-prime bases have been developed. Using these algorithms makes it relatively easy to implement a procedure for detecting and correcting one-time errors. The procedures proposed in this report for monitoring, detecting and correcting one-time errors make it possible to localize the erroneous basis and correct the error in one residual in just five conditional time steps for any number of bases of the SRC. The main advantages of CMNPB in SRC is the technical and temporal simplicity of the procedure for monitoring and detecting errors. Note that by the simplicity of the design of the circuits of the decoding devices of CS, CMNPB have no analogues in the positional number systems. This is achieved by limiting the class of possible corrected errors

References

[1] S. Shu, Y. Wang and Y. Wang, "A research of architecture-based reliability with fault propagation for software-intensive systems," *2016 Annual Reliability and Maintainability Symposium (RAMS)*, Tucson, AZ, 2016, pp. 1-6.

[2] S. S. Gokhale, M. R. Lyu and K. S. Trivedi, "Reliability simulation of component-based software systems," *Proceedings Ninth International Symposium on Software Reliability Engineering (Cat. No.98TB100257)*, Paderborn, Germany, 1998, pp. 192-201.

[3] Tiwari, Karen Tomko "Enhanced Reliability of Finite State Machines in FPGA Through Efficient Fault Detection and Correction", *IEEE Transaction on Reliability*, vol. 54, nr.3, pp. 459-467.

[4] Singh and A. Sprintson, "Reliability assurance of cyber-physical power systems," *IEEE PES General Meeting, Providence*, RI, 2010, pp. 1-6.

[5] V.A. Krasnobayev, S.A. Koshman, M.A. Mavrina. “A Method for Increasing the Reliability of Verification of Data Represented in a Residue Number System” *Cybernetics and Systems Analysis*, vol. 50, issue 6, pp. 969-976, November 2014. DOI: 10.1007/s10559-014-9688-3

[6] M. Reddy and N. Nalini, "FT2R2Cloud: Fault tolerance using time-out and retransmission of requests for cloud applications," *2014 International Conference on Advances in Electronics Computers and Communications*, Bangalore, 2014, pp. 1-4.

[7] Braun and H. Wunderlich, "Algorithm-based fault tolerance for many-core architectures," *2010 15th IEEE European Test Symposium*, Praha, 2010, pp. 253-253.

[8] M. Radu, "Reliability and fault tolerance analysis of FPGA platforms," *IEEE Long Island Systems, Applications and Technology (LISAT) Conference 2014*, Farmingdale, NY, 2014, pp. 1-4.

[9] Akushsky I., Yuditsky D. *Machine arithmetic in residual classes*. Moscow, Sov. Radio, 1968, 440 p. (in Russian)

[10] Torgashov V. *System of residual classes and reliability of digital computers*. Moscow, Sov. radio, 1973, 118 p. (in Russian)

[11] Krasnobayev V., Kuznetsov A., Koshman S., Moroz S. (2019) Improved Method of Determining the Alternative Set of Numbers in Residue Number System. *In: Chertov O., Mylovanov T., Kondratenko Y., Kacprzyk J., Kreinovich V., Stefanuk V. (eds) Recent Developments in Data Science and Intelligent Analysis of Information*. ICDSIAI 2018. Advances in Intelligent Systems and Computing, vol 836. Springer, Cham, pp. 319-328, 05 August 2018. DOI: 10.1007/978-3-319-97885-7_31

[12] V.A. Krasnobayev, A.S. Yanko, S.A. Koshman. “A Method for arithmetic comparison of data represented in a residue number system” *Cybernetics and Systems Analysis*, vol. 52, issue 1, pp. 145-150, January 2016. DOI: 10.1007/s10559-016-9809-2

[13] I.Ya. Akushskii and D.I. Yuditskii, *Arifmetika mashiny v klassah ostatkov* [*Machine Arithmetic in Residual Classes*], Sov. Radio, Moscow, 1968. (in Russian)

[14] V.A. Torgashov, *Sistema ostatochnykh klassov i nadezhnost' TsVM* [*System of residual classes and reliability of digital computers*], Sov. Radio, Moscow, 1973. (in Russian)

[15] V. Krasnobayev, S. Koshman and M. Mavrina, “Metod ispravleniya odnokratnykh oshibok dannykh, predstavlennykh kodom klassa vycheto [Method for correcting one-time data errors represented by a deduction class code],” *Elektronnoe modelirovanie*, vol. 75, issue 5, pp. 43-56, 2013. (in Russian)

[16] D. I. Popov and A. V. Gapochkin, "Development of Algorithm for Control and Correction of Errors of Digital Signals, Represented in System of Residual Classes," *2018 International Russian Automation Conference (RusAutoCon)*, Sochi, 2018, pp. 1-3.

[17] Y. N. Kocherov, D. V. Samoylenko and A. I. Koldaev, "Development of an Antinoise Method of Data Sharing Based on the Application of a Two-Step-Up System of Residual Classes," *2018 International Multi-Conference on Industrial Engineering and Modern Technologies (FarEastCon)*, Vladivostok, 2018, pp. 1-5.

[18] F. Barsi and P. Maestrini, "Error Correcting Properties of Redundant Residue Number Systems," *in IEEE Transactions on Computers*, vol. C-22, no. 3, pp. 307-315, March 1973.

[19] C. Fan and G. Ge, "A Unified Approach to Whiteman's and Ding-Helleseth's Generalized Cyclotomy Over Residue Class Rings," *in IEEE Transactions on Information Theory*, vol. 60, no. 2, pp. 1326-1336, Feb. 2014. doi: 10.1109/TIT.2013.2290694

[20] G. Harman and I. E. Shparlinski, "Products of Small Integers in Residue Classes and Additive Properties of Fermat Quotients," *in International Mathematics Research Notices*, vol. 2016, no. 5, pp. 1424-1446, Jan. 2016. doi: 10.1093/imrn/rnv182

[21] M. Kasianchuk, I. Yakymenko, I. Pazdriy, A. Melnyk and S. Ivasiev, "Rabin's modified method of encryption using various forms of system of residual classes," *2017 14th International Conference The Experience of Designing and Application of CAD Systems in Microelectronics (CADSM)*, Lviv, 2017, pp. 222-224. doi: 10.1109/CADSM.2017.7916120

[22] V.A. Krasnobayev, S.A. Koshman, M.A. Mavrina. “A Method for Increasing the Reliability of Verification of Data Represented in a Residue Number System” *Cybernetics and Systems Analysis*, , vol. 50, issue 6, pp. 969-976, November 2014. DOI: 10.1007/s10559-014-9688-3

[23] K. Tao, L. Peng, K. Liang and B. Zhuo, "Irregular repeat accumulate low-density parity-check codes based on residue class pair," *2017 IEEE 9th International Conference on Communication Software and Networks (ICCSN)*, Guangzhou, 2017, pp. 127-131. doi: 10.1109/ICCSN.2017.8230092

[24] V. Krasnobayev, A. Kuznetsov, A. Kononchenko, T. Kuznetsova. Method of data control in the residue classes. *In Proceedings of the Second International Workshop on Computer Modeling and Intelligent Systems (CMIS-2019)*, Zaporizhzhia, Ukraine, April 15-19, 2019., pp. 241–252. 2019.

[25] A. Kuznetsov, O. Smirnov, D. Kovalchuk, et al. Discrete signals with special correlation properties. *In Proceedings of the Second International Workshop on Computer Modeling and Intelligent Systems (CMIS-2019)*, Zaporizhzhia, Ukraine, April 15-19, 2019., pp. 618–629. 2019.

[26] V. Krasnobayev, A. Kuznetsov, M. Zub, K. Kuznetsova. Methods for comparing numbers in non-positional notation of residual classes. *In Proceedings of the Second International Workshop on Computer Modeling and Intelligent Systems (CMIS-2019)*, Zaporizhzhia, Ukraine, April 15-19, 2019., pp. 581–595. 2019.

[27] Yu.V. Stasev, A.A. Kuznetsov. “Asymmetric code-theoretical schemes constructed with the use of algebraic geometric codes”. *Kibernetika i Sistemnyi Analiz*, No. 3, pp. 47-57, May-June 2005.

[28] A. A. Kuznetsov, Yu. I. Gorbenko, D. I. Prokopovych-Tkachenko, M. S. Lutsenko, M. V. Pastukhov. “NIST PQC: Code-Based Cryptosystems.” *Telecommunications and Radio Engineering*, Volume 78, 2019, Issue 5, pp. 429-441. DOI: 10.1615/TelecomRadEng.v78.i5.50

[29] Gorbenko I.D., Zamula A.A., Semenko Ye.A. Ensemble and correlation properties of cryptographic signals for telecommunication system and network applications. *Telecommunications and Radio Engineering. - Volume 75, 2016 Issue 2,* p.p. 169-178. DOI: 10.1615/TelecomRadEng.v76.i17.40.

[30] M. Karpinski, S. Ivasiev, I. Yakymenko, M. Kasianchuk and T. Gancarczyk, "Advanced method of factorization of multi-bit numbers based on Fermat's theorem in the system of residual classes," *2016 16th International Conference on Control, Automation and Systems (ICCAS)*, Gyeongju, 2016, pp. 1484-1486.

[31] Runovski, K., & Schmeisser, H. -. (2004). On the convergence of fourier means and interpolation means. *Journal of Computational Analysis and Applications*, 6(3), 211-227.

[32] Gnatyuk, V. A. (2001). Mechanism of laser damage of transparent semiconductors. *Physica B: Condensed Matter*, 308-310, 935-938.

[33] Tkach, B. P., & Urmancheva, L. B. (2009). Numerical-analytic method for finding solutions of systems with distributed parameters and integral condition. *Nonlinear Oscillations*, 12(1), 113-122.

[34] Krasnobayev V. A. Method for realization of transformations in public-key cryptography. *Telecommunications and Radio Engineering. - Volume 66, 2007 Issue 17,* pp. 1559-1572. DOI: 10.1615/TelecomRadEng.v66.i17.60