UDC 681.142.01

THE CONCEPT OF PROCESSING INTEGER DATA REPRESENTED IN THE SYSTEM OF RESIDUE CLASSES

Viktor Krasnobayev[1], Sergey Koshman[2], Artem Moskalenko[3]

[1] V. N. Karazin Kharkiv National University, Svobody sq.,4, Kharkiv, 61022, Ukraine
krasnobaev@karazin.ua
[2] Kharkiv Petro Vasylenko National Technical University of Agriculture, Rizdviana st., 19, Kharkiv, 61052, Ukraine
s_koshman@ukr.net
[3] Poltava Institute of Business Academician Yuri Bugay International Science and Technical University, Sinna st., 7
Poltava, 36039, Ukraine
moskalenko_artem@ukr.net

Reviewer: Vyacheslav Kharchenko, Doctor of Sciences (Eng), Full Prof., Academicians of the Academy of Applied Radioelectronics Sciences, N.Ye. Zhukovskiy National Aerospace University – Kharkiv Aviation Institute (KhAI), 17 Chkalov St., Kharkiv, 61070, Ukraine.
v_s_kharchenko@ukr.net

Received on May 2017

Abstract: *The coding of residues number witch submitted the appropriate modules of residual classes system (RCS), made with data from complete system of the smallest non-negative residues (CSSNR) was show in the article. In this aspect, CSSNR is the basis for the construction of non-positional code structure in RCS. Possible field of science and engineering, where there is an urgent need for fast, reliable, and high-precision integer calculations were clarified and systematized in the paper. On the basis of studies of the properties of RCS were examined the advantages and disadvantages of using modular arithmetic (MA). Using the results of the analysis of problems of integer data and a set of positive attributes of MA, the classes of problems and algorithms, which using RCS, much more efficient binary positional numeral systems were defined in the article.*

Keywords: *residual classes system, modular arithmetic, positional numeral systems, complete system of the smallest non-negative residues, computer system and a data processing means witch represented in integer form, residual classes.*

1 Introduction

At present time there is a number of fields and directions of science and technology, where a need in fast, reliable and highly precise integer arithmetic calculations exists. We can say, that in almost all fields of science the integer arithmetic calculations are used. First of all, they are such fields of science as mathematics, physics, astronomy, technical science, geodesy and meteorology, seismology etc. Let's note the following directions in science and technology, where there exists the necessity in fast, reliable and highly precise integer arithmetic calculations: arithmetic operations with integer numbers and polynomials; integer linear programming; operations with numbers and sets, the solution of the multidimensional NP-complete problems; implementation of routing algorithms *(algorithms for finding the shortest path)*; problems of ways and matrix multiplication; problems of fast Fourier transform and it's applications; the creation of artificial intelligence systems *(neural network data processing system)*; tasks for military purposes; digital signal processing, digital image processing; cryptographic transformation; highly-precise integer arithmetic; the solution of problems related to the space research; highly-precise digital-to-analog and analog-to-digital conversions and so forth.

The results of the researches conducted during last few decades in the field of information technologies by different groups of scientists and engineers of methods of productivity improvement, reliability, survivability, and reliability of computer systems calculations and data processing means presented as integers (CSIDPM), showed that within the positional numeral systems (PNS), it is practically impossible to achieve it [1-3]. First of all, it's caused by the main disadvantage of modern CSIDPM that operate in PNS: the presence of inter-bits links between the processed operands.

These links significantly impact the architecture of the calculator and methods of implementation of arithmetic operations, implemented by CSIDPM; complicate the apparatus and limit the speed of the arithmetic operations of addition, subtraction and multiplication. In this regard, improving above mentioned characteristics of CSIDPM in PNS, is carried out, first of all, by increasing the clock frequency, development and application of methods and means of parallel data processing as well as by using different types of redundancy. This circumstance led to the need of finding the ways of increasing the effectiveness of CSIDPM functioning, for example, through the use of new architectural solutions by applying non-positional machine arithmetic, in particular, on the basis of non-positional numeral systems use in residual classes (NSRC). The well-known Chinese remainder theorem (*the task of restoring the original number A_k by the aggregating of its remains (deductions)* $\{a_i\}$ *by dividing it into a series of natural numbers m_1, m_2, ..., m_n (modules) of NSRC*), which was previously interpreted as a structural theorem of abstract algebra, guaranteed the specified parallelism in the calculations over integers, under the conditions that the result of ring operations belongs to the range of integers, defined by models product of NSRC. The results of conducted researches of the implementation of arithmetic operations methods in NSRC led to the creation of new machine arithmetic. Having its ideological roots of the classical works of Euler, Gauss and Chebyshev on the theory of comparisons, NSRC introduced new ideas in the development of creation methods of highly-productive and ultra reliable CSIDPM [1,4,5].

2 The main part

For the first time the results of theoretical studies devoted to the possibility of practical application of NSRC as a numeral system (NS) of CSIDPM, were published in 1955-1957 in the scientific works of Czech scientists M. Valaha and A. Svoboda. Non-positional number system in NSRC is a NS where integers are presented as a set of non-negative deductions (residues) in the group of mutually pairwise prime numbers which are called bases or modules of NSRC. In this case there are no inter-bits relations between processed numbers residues, that gives opportunity to perform arithmetic operations excluding bit relations between numbers residues. The use of NSRC-based machine arithmetic allowed to create actually operating CSIDPM. In the 60s of the past century the team of scientists and engineers headed by the doctor of technical sciences, professor D.I. Yuditskii, created A-340A the world's first experimental computer and T-340A serial computers, functioning in NSRC. These computers were intended for regular polygon version of Dunay-3UP radar, which was the part of the USSR A-35 missile defense system. In the 70s of the past century for radar stations there were created such CSIDPM in NSRC as "Diamond" and 5E53 supercomputers.

However in the 80s of the past century due to a number of objective and subjective reasons the interest to modular arithmetic (MA) is significantly reduced. It was primarily due to the death of the Director of the Microelectronics Center, developing the general theory and practical creation of a computer in NSRC located in Zelenograd, Moscow Region, the Director and the chief initiator of project Lukin Fedor Victorovich and therefore, the complete termination of practical works, connected with the use of MA. But then this direction was restrained by the imperfection of the existing at that time element base of computers, as well as the existing methodology of computer systems and components designing, principally focused at that time only on the binary system calculation.

Now the interest to the use of NSRC is increasing again. Ultimately it is caused by:

- the emergence of the numerous scientific and theoretical publications devoted to the theory and practice of the computer systems and components creating in NSRC;
- wide distribution of mobile processors that require high speed data processing at low energy consumption; the lack of inter-bits transfers during arithmetic operations of addition and multiplication of numbers in NSRC allows to reduce energy consumption;
- strong interest to NSRC is being shown by the banking structures, where it is necessary in real time to handle large amount of data safely and reliably, i.e. they are required highly-productive means for highly reliable computing with errors self-correction, that is typical to the NSRC codes;
- the elements density increasing on a single chip doesn't always allow to perform a complete

and qualitative testing; in this case there is an increasing importance of providing failover operation of CSIDPM;

– the need for the use of the specialized CSIDPM to perform a large number of operations on vectors, which require high-speed performance of integer addition and multiplication operations *(matrix multiplication problems, the problems of the scalar product of vectors, Fourier transformation, etc.)*;

– the widespread introduction of microelectronics into all spheres of human activity significantly increased relevance and importance of previously rare, and now so massive scientific and practical problems, as a digital signal and image processing, image recognition, cryptography, multi-bit data processing and storage, etc.; this circumstance requires enormous computing resources being in excess of the existing possibilities;

– the current level of microelectronics development is coming to its limits from the point of view of productive provision and reliability of existing and future computer systems and components of large data sets processing in real time;

– taking it over nanoelectronics, molecular electronics, micromechanics, bioelectronics, optical, optoelectronic and photonic computers and others are still rather far from the real industrial production and employment.

– the modern development of integrated circuit technology allows to have a fresh look at the principles of devices construction with modular arithmetic employment and provides wide opportunities to use new design techniques *(such as the methodology of systems design on a chip-SOC)* both in the development of individual computing units, and computer systems in general; integral technology enables more flexible design of computer systems and components and allows us to implement NSRC-based devices as effectively as on the basis of the binary system; furthermore at present in order to improve the effectiveness of computer devices development, automated design systems (ADS) are widely used; in this respect, the design of computer systems and components based on NSRC does not differ from the working with the help of ADS data of binary data-blocks in PNS;

– unfortunately, Ukraine today in contrast to the theoretical development, technologically is behind the foreign microelectronics of some leading countries; in this case, it is advisable to use the existing theoretical achievements and practical experience in the creation of effective computer systems and components in NSRC.

In [1] it is given a definition of NSRC. In this case NSRC is considered a generalized version of NS, in which any natural number *A*, including zero, is represented as a set of the smallest positive residues *(deductions)* of the division of the original A number on preset m_1, m_2, … m_n natural numbers, called bases or NSRC modules. In literature it is often not entirely fair the term NSRC is identified with "residue class". In some cases, this circumstance can interfere the analysis of the results of solving the data processing problems presented in MA. In this regard it is important to consider the correlation between the notion of NSRC and RC. We'll give a definition to the notion "residue class". Let's consider the set {*A*} of all natural numbers, including zero. From the set of natural numbers we choose an arbitrary number *(module)* m_i. While dividing any natural number on m_i module we can get the following set of residues: 0 *(A number is divided into the m module integrally)*, 1, 2 … $m_i - 2$ and $m_i - 1$. All the set of natural numbers including zero, can be divided into m_i (0, 1, 2, ... m_i -2 and m_i -1) of different groups of numbers *(residue classes)*, including in each RC the numbers which, while dividing into the module m_i, give the same remainder. It is considered, that these numbers are comparable with each other on module m_i.

The residue class modulo m_i of NSRC can be denoted by the symbol $RC_j^{(i)}$, where i – the number of the base of orderly ($m_i < m_{i+1}$) NSRC ($i = \overline{1, n}$); j – the RC number in the system of residues for a given module m_i ($j = \overline{0, m_i - 1}$). In the general case, the residue class of $RC_j^{(i)}$ modulo m_i we will call the set of all integers, including zero, which while dividing into the modules m_i give the same positive balance. Taking into account the well-known correlation

$(-A) \bmod m_i = (m_i \cdot k - A) \bmod m_i (k = 1, 2, 3, ...)$, all RC on arbitrary module m_i of NSRC can be represented in the form of

$$\begin{aligned}
RC_0^{(i)} &= \overline{0} \ \{ ..., -2 \cdot m_i, \quad -m_i, \quad 0, \ m_i, \quad 2 \cdot m_i, \quad 3 \cdot m_i, \quad ... \}, \\
RC_1^{(i)} &= \overline{1} \ \{ ..., -(2 \cdot m_i - 1), -(m_i - 1), \ 1, \ m_i + 1, \ 2 \cdot m_i + 1, \ 3 \cdot m_i + 1, \ ... \}, \\
RC_2^{(i)} &= \overline{2} \ \{ ..., -(2 \cdot m_i - 2), -(m_i - 2), \ 2, \ m_i + 2, \ 2 \cdot m_i + 2, \ 3 \cdot m_i + 2, ... \}, \\
RC_3^{(i)} &= \overline{3} \ \{ ..., -(2 \cdot m_i - 3), -(m_i - 3), \ 3, \ m_i + 3, \ 2 \cdot m_i + 3, \ 3 \cdot m_i + 3, ... \}, \\
&\vdots \qquad\qquad\qquad\qquad\qquad\qquad \vdots \\
RC_j^{(i)} &= \overline{j} \ \{ ..., -(2 \cdot m_i - j), -(m_i - j), \ j, \ m_i + j, \ 2 \cdot m_i + j, 3 \cdot m_i + j, ... \}, \\
&\vdots \qquad\qquad\qquad\qquad\qquad\qquad \vdots \\
RC_{m_i-2}^{(i)} &= \overline{m_i - 2} \{ ..., \ -(m_i + 2), \ -2, \ m_i - 2, \ 2 \cdot m_i - 2, \ 3 \cdot m_i - 2, \ 4 \cdot m_i - 2, \ ... \}, \\
RC_{m_i-1}^{(i)} &= \overline{m_i - 1} \{ ..., \ -(m_i + 1), \ -1, \ m_i - 1, \ 2 \cdot m_i - 1, \ 3 \cdot m_i - 1, \ 4 \cdot m_i - 1, \ ... \}.
\end{aligned} \tag{1}$$

If one arbitrary residue is taken from each RC, then such set of m_i integers will be called a complete residue system (CRS) modulo m_i. Having taken one specific residue from each RC, draw up some possible options for CRS modulo m_i: 0, 1, 2, 3, …, $m_i - 1$ – is a complete system of the smallest non-negative residues (CSSNR); m_i, 1, 2, 3, …, $m_i - 1$ – is a complete system of the smallest positive residues (CSSPR); 0, 1, 2, -2, …, -1 – is a complete system of the smallest in absolute value residues (CSSAVR). As within each module they operate only with natural numbers, including zero, for the formation of NSRC with the $m_1, m_2, ..., m_n$ bases it is necessary to use n CSSNR from each set of RS. In this case all possible RC ($C^{(1)}$) for the first m_1, for the second ($C^{(2)}$) m_2 and the last ($C^{(n)}$)m_n of NSRC modules, have been represented respectively by the expressions (2), (3) and (4). For the first NSRC m_1 module we have the following set of RC

$$\begin{aligned}
RC_0^{(1)} &= \overline{0} \ \{ \ 0, \quad m_1, \quad 2 \cdot m_1, \quad 3 \cdot m_1, \quad ... \}, \\
RC_1^{(1)} &= \overline{1} \ \{ \ 1, \quad m_i + 1, \quad 2 \cdot m_1 + 1, \ 3 \cdot m_1 + 1, \ ... \}, \\
RC_2^{(1)} &= \overline{2} \ \{ \ 2, \quad m_1 + 2, \quad 2 \cdot m_1 + 2, \ 3 \cdot m_1 + 2, \ ... \}, \\
&\vdots \\
RC_{m_1-2}^{(1)} &= \overline{m_1 - 2} \{ \ m_1 - 2, \ \ 2 \cdot m_1 - 2, \ 3 \cdot m_1 - 2, \ 4 \cdot m_1 - 2, ... \}, \\
RC_{m_i-1}^{(1)} &= \overline{m_1 - 1} \{ \ m_1 - 1, \ \ 2 \cdot m_1 - 1, \ 3 \cdot m_1 - 1, \ 4 \cdot m_1 - 1, ... \}.
\end{aligned} \tag{2}$$

Obviously, for the module m_1 of NSRC the CSSNR will consist of residues:

$$0, 1, 2, ..., m_1 - 1.$$

For the second m_2 module of NSRC we have the following set of RC

$$\begin{aligned}
RC_0^{(2)} &= \overline{0} \ \{ \ 0, \quad m_2, \quad 2 \cdot m_2, \quad 3 \cdot m_2, \quad ... \}, \\
RC_1^{(2)} &= \overline{1} \ \{ \ 1, \quad m_2 + 1, \quad 2 \cdot m_2 + 1, \ 3 \cdot m_2 + 1, \ ... \}, \\
RC_2^{(2)} &= \overline{2} \ \{ \ 2, \quad m_2 + 2, \quad 2 \cdot m_2 + 2, \ 3 \cdot m_2 + 2, \ ... \}, \\
&\vdots \\
RC_{m_2-2}^{(2)} &= \overline{m_2 - 2} \ \{ \ m_2 - 2, \ 2 \cdot m_2 - 2, \ 3 \cdot m_2 - 2, \ 4 \cdot m_2 - 2, \ ... \}, \\
RC_{m_2-1}^{(2)} &= \overline{m_2 - 1} \ \{ \ m_2 - 1, \ 2 \cdot m_2 - 1, \ 3 \cdot m_2 - 1, \ 4 \cdot m_2 - 1, \ ... \}.
\end{aligned} \tag{3}$$

For the module m_2 of NSRC the CSSNR will consist of residues: $0, 1, 2, ..., m_2 - 1$.

For the last NSRC m_n module we have

$$\begin{aligned}
RC_0^{(n)} &= \overline{0} \quad \{\ 0, \quad m_n, \quad 2\cdot m_n, \quad 3\cdot m_n, \quad ...\ \},\\
RC_1^{(n)} &= \overline{1} \quad \{\ 1, \quad m_n+1, \quad 2\cdot m_n+1, \quad 3\cdot m_n+1, \quad ...\ \},\\
RC_2^{(n)} &= \overline{2} \quad \{\ 2, \quad m_n+2, \quad 2\cdot m_n+2, \quad 3\cdot m_n+2, \quad ...\ \},\\
&\vdots\\
RC_{m_n-2}^{(n)} &= \overline{m_n-2} \quad \{m_n-2, \quad 2\cdot m_n-2, \quad 3\cdot m_n-2, \quad 4\cdot m_n-2, \quad ...\ \},\\
RC_{m_n-1}^{(n)} &= \overline{m_n-1} \quad \{m_n-1, \quad 2\cdot m_n-1, \quad 3\cdot m_n-1, \quad 4\cdot m_n-1, \quad ...\ \}.
\end{aligned} \tag{4}$$

For the module m_n the CSSNR will consist of residues: $0, 1, 2, ..., m_n - 1$.

Thus, the NSRC is characterized by using of n, the number of bases of CSSNR.

Here is an example of CRS definition for the module $m_i = 5$ of NSRC. Residue classes modulo five can be represented in general form

$$\begin{aligned}
&\overline{0} \ \{ \dots \text{-}10, \quad \text{-}5, \quad 0, \quad 5, \quad 10, \quad \dots \},\\
&\overline{1} \ \{ \dots \text{-}9, \quad \text{-}4, \quad 1, \quad 6, \quad 11, \quad \dots \},\\
&\overline{2} \ \{ \dots \text{-}8, \quad \text{-}3, \quad 2, \quad 7, \quad 12, \quad \dots \},\\
&\overline{3} \ \{ \dots \text{-}7, \quad \text{-}2, \quad 3, \quad 8, \quad 13, \quad \dots \},\\
&\overline{4} \ \{ \dots \text{-}6, \quad \text{-}1, \quad 4, \quad 9, \quad 14, \quad \dots \}.
\end{aligned}$$

Taking one residue from each RC, we compose all the variants of the complete residues systems modulo five: 0,1,2,3,4 – CSSNR; 5,1,2,3,4 – CSSPR and 0,1,2,-2,-1 – CSSAVD. According to the definition, CSSNR 0,1,2,3,4 is used in NSRC.

Actually, there is an opinion [3], that it is possible for NSRC not to be called a number system. Indeed, NSRC bases are connected to each other so, that they are selected in a certain way and secured by the permanent modules for the given NS. Each residue modulo is informationally independent on other residues, however, during the implementation of arithmetic operations within each residue unitary or binary NS is generally used. Thus NSRC may be determined not as the number system, but as a special design code numeric data structure, that is specially encoded block of numerical data.

It should be noted that in the proposed approach the NSRC is not opposed to binary PNS, and serves as its extension that allows to solve effectively a certain class of problems. Therefore, the most effective in this case, is an approach that unites the use of a combined MA and binary PNS notation in constructing the control systems. Upon that, for example, control of the entire system can be carried out by the conventional binary commands and blocks; and data processing is performed on the basis of a modular representation of numbers. Thus, the use of the advantages and benefits of NSRC, along with the traditional binary method of control systems constructing can lead to the productivity increase of CSIDPM in general.

To answer the question of whether to use NSRC it's necessary to investigate the influence of the MA basic properties on the structure and operation principles of CSIDPM. Possible logical algorithm research diagram of NSRC effective application can be represented as follows:

– to indentify the areas and directions of science and technology where integer calculations are necessary; to show in which tasks and algorithms *(specifically, to name and show the most important ones)* integer calculations are used; first of all the tasks and algorithms, which include such operations as arithmetic operations of addition, subtraction and multiplication in a positive and negative number ranges, as well as arithmetic operation and algebraic comparisons of numbers;

– to justify the relevance requirements and the need to increase the speed of integer calculations, i.e. to justify the need to increase CSIDPM productivity in order to (to increase the speed of integer calculations it's necessary to create CSIDPM of increased *(in comparison to the existing ones)*) productivity;

– to consider the existing and advanced methods for production increase of CDIDPM, operating in the PNS; possible conclusion: the existing and advanced methods of performance improving of CDIDPM in PNS do not always satisfy the increasing demands to the improved performance implementation of integer calculations *(denote the main reason)*;

– to consider one of the possible *(referred to in modern literature)* options for creation of highly productive CDIDPM on the basis of NSRC; on the basis of the analysis of the NSRC properties and the results of the previous and up-to-date researches of theoretical and practical developments in the application field of non-positional number system, to justify the possibility of its effective application in order to improve the CSIDPM performance.

If the proposed algorithm research scheme is adopted, then the theoretical researches, devoted to the CSIDPM production increase on the basis of NSRC implementation can be carried out. Methods, models and data processing algorithms in NSRC are being developed. Comparative analysis of the achieved results are being conducted.

Before defining a class of tasks and algorithms for which the mathematical apparatus of the numbers theory is effectively applied, it is necessary, on the basis of the results of the NSRC properties researches, to analyze the advantages and disadvantages of the MA use.

3 The properties of the residual classes system

Let's consider the influence of the NSRC basic properties on the CSIDPM structure and principles of functioning [6-9].

1. The independence of residuals. This property gives the opportunity to build CSIDPM in the form of a set of independent, parallel working separate computational paths of information processing, functioning independently from each other according to their specific module m_i. Thus, CSIDPM functioning in NSRC has a modular design, that allows to carry out technical service and elimination of failures and malfunctions of computational paths by their simple replacement without interrupting computational task solving. Arithmetic operations realization time in CSIDPM is determined by the time of operation realization in computing path over the NSRC greatest m_i basis.

Besides, the mistakes arising due to binary bits schemes refusals *(failures)* in any CSIDPM computing path, are not *"multiplied"* in the neighboring tracts they *(remain within one residue)*, that gives the chance to increase the calculations accuracy in NSRC. At that it doesn't matter whether there had been single or multiple errors or multitude of errors with the length of no more than $[\log_2(m_i-1)]+1$ binary bits. An error, occurred in the CSIDPM computing path on the base of m_i is stored in this path until the end of the calculations or is self-destructed in the process of the further calculations. This property of NSRC allows you to create a unique errors control and correction system in the dynamics of the CSIDPM computational process *(without stopping the process of calculation)* at the introduction of the minimum code redundancy that is essential for the data processing systems operating in real-time.

2. The residues equality. We can note that there is a close connection between the arithmetic codes in NSRC and arithmetic AN-codes in PNS. Arithmetic codes in RNS are a futher development of the known positional arithmetic noise-combating multiresidual AN-code. In general terms multiresidual AN-codes is represented in the form of

$$A'_k = (A_k, A_k(\mathrm{mod}\, m_1), A_k(\mathrm{mod}\, m_2), \ldots \\ \ldots, A_k(\mathrm{mod}\, m_i), \ldots, A_k(\mathrm{mod}\, m_{n-1}), A_k(\mathrm{mod}\, m_n)) \quad (5)$$

i.e.

$$A'_k = (A_k, a_1, a_2, \ldots, a_n), \quad (6)$$

where $a_i = A_k - [A_k / m_i]m_i$.

When performing a ratio $\prod_{i=1}^{n} m_i \geq A_k$ the set of residuals $\{a_i\}$ uniquely determines the number A_k. In this case, in the expression structure (5) the value A_k can be excluded. Then a multiresidual code (5) in PNS takes the form of the NSRC code $A'_k = (a_1, a_2, ..., a_n)$ (6), that allows to realize modular arithmetical operations on certain independent computing paths, operating only with residuals $\{a_i\}$.

Based on the procedure of numbers formation in NSRC, it's obviously, that any residual a_i of number $A = (a_1, a_2, ..., a_n)$ carries all the information about the original A number, that gives the opportunity by using the programming methods to replace the refused computing path m_i modulo on the operable path m_j modulo (under the condition that $m_i < m_j$) without interrupting the task solution. Thus, CSIDPM functioning in NSRC and having, for example, two control bases, ensure self operation in case of any two computing path failure. In case of failures in the third or fourth paths CSIDPM continues the computing program execution under some dilution of computing precision i.e. CIDPM in NSRC has the property of a gradual degradation. This property defines a specific difference of the CSIDPM functioning in NSRC: the computer system depending on the requirements imposed to it can have different reliability, computing accuracy and high-speed performance in the calculating process dynamics. Thus, during the tasks solution course, it is possible to vary CSIDPM reliability, computing validity, accuracy and speed. Really, let data be determined by the numerical code presented by the set of bases $\{m_i\}$ ($i = \overline{1, n+k}$) of NSRC. It is known that the time of arithmetic operations execution and decision accuracy depends on the amount of n information bases, and reliability of CSIDPM functioning and validity of calculations depends on the amount of k control bases of NSRC. Let in the process of calculations there was a necessity to enhance the reliability of CSIDPM functioning and (or) validity of calculations. In this case, in real time, without interrupting the calculations, there is a redistribution of NSRC bases $\{m_i\}$ as follows $i = \overline{1, n'+k'}$, and $n' < n$, $k' > k$. At that $n + k = n' + k' = const$. In this case accuracy of calculation is diminished and it is increased the speed of arithmetic operations, that are determined by the amount of information bases n'. If there is a necessity to increase accuracy of decision on the separate section of the computed program, then the redistribution of the program is carried out in the following way: $i = \overline{1, n''+k''}$ ($n + k = n'' + k'' = const$). In this case with the increasing of calculation accuracy ($n'' > n$), CSIDPM reliability (validity of calculations) and the speed of the given task execution is diminished.

Non-module operations *(operation of control, correction, comparison, etc)* in NSRC are carried out in the same way. The time necessary for the execution of non-module operations in NSRC is proportional to the number of n information bases, i.e. to the number of bases, determining the accuracy of calculations. Transition to the calculations with less accuracy allows to increase the speed of CSIDPM. If the ordered ($m_i < m_{i+1}$) NSRC is expanded by the addition of l bases, each of which is bigger than the previous base of the initial NSRC, then the minimum code distance $d_{\min}$ is increased automatically on the value of l. One can obtain the same by diminishing the information bases number of n, i.e. passing to the calculations with less accuracy. Therefore, there is some back proportional dependence between the correcting possibilities of codes in NSRC and the accuracy of calculations. Being applied to PNS the described property, having the possibility to change a correlation between the number of information and control bases in the process of problem solving is based on the well-known method of variable scaling, allowing to diminish the amount of bits in the presentation of numerical information in PNS. Due to it we can introduce the additional bits to organize hardware operative control while having limitations to the increase of weight, dimensions and cost of CSIDPM. Upon that one can vary the accuracy, speed and reliability of calculations. However the specific character of PNS creates the following limitations to the variable scaling method:

- before each timing period of the program implementation it is necessary to make the addi-

tional operations of data transfer, reducing the real speed of CSIDPM on 10 %;

– prior to the preparation of the variable scaling program it is expected to do more theoretical work on the definition of rational scaling coefficient;

– scaling should be applied only for a certain class of problems;

– the given method is generally inexpedient for CSIDPM operating in real time.

Sharing the first and the second properties of NSRC causes the existence of three types of redundancy simultaneously in CSIDPM: structural, information and functional. Based on the idea of the structural redundancy, the sharing of the first and second properties allows to synthesize a model of CSIDPM reliability in NSRC, corresponding to the model of the dynamic redundancy in the PNS. In this case, the information paths $m_1 \div m_n$ of CSIDPM play the role of the working elements and path $m_{(n+1)} \div m_{(n+k)}$ – the role of reserve elements, where k is the number of control *(backup)* NSRC bases.

3. The low-bit of residues. This characteristic allows significantly improve the reliability of CSIDPM and the speed of arithmetic operations both by the low-bit of CSIDPM computing paths and through the ability to use *(unlike PNS)* table arithmetic where arithmetic operations of addition, subtraction and multiplication are performed in one step virtually. In particular the low-bit of residues in representation of the numbers in modular arithmetic gives possibility of a wide choice of options for engineering solutions while implementing modular arithmetic operations based on the following principles:

– summation principle *(based on low-bit binary adders)*;

– table principle *(based on the use of ROM of small size)*;

– direct logical principle of arithmetic operations implementation, based on the modular operations description at the level of switch functions systems of Boolean algebra;

– ring shear principle based on the use of ring shear registers.

On the base of the analysis of the possible use of these three main characteristics *(independence, equal rightness and low-bit of residues, defining non-positional code structure in MA)* non-positional arithmetic in NSRC, compared with the PNS, has the following significant advantages:

– the possibility of calculations parallelization at the level of decomposition of operands, which greatly improves their high-speed performance;

– the possibility of spatial separation of data elements with the possibility of their following asynchronous independent processing;

– the possibility of table *(matrix)* execution of a basic set of arithmetic operations and polynomial functions with single-cycle sampling of modular operation results;

– the possibility of establishing a system of CSIDPM control and correction with the effective detection and correction of faults and failures;

– the possibility to control and correct the errors in the dynamics of the CSIDPM computing process;

– the possibility to use effectively passive and active failsoft on the base of the operational reconfiguration of the CSIDPM structure;

– -less computing and time complexity for the separate classes *(types)* of integer problems;

– demonstration of the special property of the CSIDPM structure in NSRC, ensuring the lack of error expansion effect when implementing arithmetic operations of addition, subtraction and multiplication;

– adaptation of the CSIDPM structure in NSRC for the rapid diagnostics of calculator blocks and points;

– the possibility to increase the CSIDPM reliability in NSRC as a result of the effective simultaneous use of both passive and active failsoft.

– Along with the mentioned benefits of modular arithmetic we can emphasize the number of advantages regarding to the integrated form devices implemented with the MA means [10,11]:

– independent operation of each computing channel of CSIDPM in NSRC according to the

corresponding modules provides significant flexibility in the topological design and layout of the crystal;

– trace interconnections are distributed only within a separate channel for each module of NSRC, which excludes the availability of long routes and, as a result, provides some reduction of power consumption and reduction of signals time delays over critical paths;

– tracing of clock frequency circuits within the data processing channels for each module of NSRC is being improved, that in turn reduces the peak emission in drive circuits;

– implementation of the computing devices on the base of PLD possessing less gating resources, can be easily planed and placed in a few crystals, the possibility of using the table methods of multi-bit numbers processing on a single chip, under the condition that the chip area is not critical;

– introduction of additional redundant channels to design fail-soft systems without full duplication of each computing path of CSIDPM in PSRC.

The represented peculiarities of the integrated devices based on the modular representation indicate that while analyzing and comparing them with conventional positional one, we can not be limited by only usual comparison of speed and occupied space. It is also necessary to take into account the given indicated factors, as they are very important in the development of highly-productive systems, among them the operating in real time ones. Let's note that when writing program in the PNS programmers have difficulties when they have to use large numbers in the program (2^{24}-2^{128} bits).

Let's consider the main drawbacks inherent to NSRC:

– by the type of number in NSRC its quantitative value can not be determined;

– one of the major practical problems is the complexity of the division operation execution; ratio of A/B may not be an integer number, and if it is integer one, in general case, it is impossible to find its exact modular presentation, computing a_i / b_i modulo m_i for each value of i;

– it's also difficult to perform comparison operations for a variety of modular representations $\{a_1, a_2, \ldots, a_p\}$ and $\{b_1, b_2, \ldots, b_p\}$; that leads to the problem of overflows control *(i.e., checking output results beyond the numerical range* $0 \div M-1$*)*;

– to ensure compatibility with the existing binary PNS *(binary representation of data)* CSIDPM in NSRC should have, respectively, the forward converter in modular representation and inverter in the binary number system; converters can also make a significant contribution in both hardware costs and speed of such devices;

– the basic modular operations are more complicated in the technical implementation and more expensive in terms of a chip occupied space and speed than similar binary ones.

Shortcomings listed above limit the scope of the MA, so computer components in the NSRC are rarely implemented in general-purpose machine blocks. But it is possible to allocate a number of specific applications, the implementation of which with the use of the MA is believed to be the most effective. Computer devices where the main calculation share is on multiplication operations combined with addition and subtraction, or computer systems of increased reliability belong to these applications.

Correction of the NSRC disadvantages expands the modular arithmetic applicable scope. In particular, the simplification of the comparison operation implementation and the development of the effective methods and numbers division algorithms will make it possible to apply NSRC in general-purpose computers for solving a wider range of tasks.

The results of the tasks analysis of the data integer processing and accounting for the whole positive properties of NSRC defines the following classes of problems and algorithms, in which the non-positional number system is essentially more effective than PNS:

– cryptographic and module transformations;

– signals digital processing *(image compression, algorithms implementation of Fourier rapid and discrete transformations, etc.)*;

– integer processing in real time and large bits storage (2^{32} - 2^{128} bit);

– vector and matrix processing of large data files;
– neurocomputing information processing;
– optoelectronic tabular data processing;
– monitoring, diagnostics and jam-resistant data coding in CSIDPM;
– using of CSIDPM in NSRC as a computer arithmetic expanders or a general-purpose computing system, performing modular operations of addition, subtraction and (or) multiplication.

4 Conclusions

In the present article it has been shown that the number residues coding, submitted by the respective NSRC bases, is performed by the data from CSSNR. Thus, CSSNR is the basis for the constructing of the non-positional data code structure in NSRC. This is on the one hand. On the other hand the residue classes for each module of NSRC are the basis for the CSSNR formation. Within this framework, strongly mathematically, the notions NSRC and RC cannot be identified. However, experts in the field of MA often use vernacular term RC, having in mind the NSRC.

In the paper there have been specified and systematized the possible fields of science and technology, where there is an urgent need for fast, reliable and high precision integer calculation. There have been shown, that to reach essential "breakthrough" in that direction in PNS is nearly impossible. In fact, the PNS employment in electronics has reached its potential, that is defined by the impossibility to eliminate the inter-bits links between the processed operands in CSIDPM. There is no such drawback in CSIDPM, functioning in NSRC. On the basis of the results of the NSRC properties research, there have been analized the advantages and disadvantages of the MA use. Having used the results of the analysis of the data integer processing tasks and a set of MA positive properties, in the paper there have been formulated tasks and algorithms classes, for which the NSRC use is essentially more efficient than PNS.

References

[1] Akushskii I. Ya. Mashinnaya arifmetika v ostatochnykh klassakh / I. Ya. Akushskii, D. I. Yuditskii. – Moskva: Sov. radio, 1968. – 440 s.
[2] Siora A. A. Otkazoustoichivye sistemy s versionno-informatsionnoi izbytochnost'yu v ASU TP: monografiya / A. A. Siora, V. A. Krasnobaev, V. S. Kharchenko. – Khar'kov: MON, NAU im. N. E. Zhukovskogo (KhAI), 2009. – 320 s.
[3] Morgado M. Modular arithmetic [Electronic Resource] / Matthew Morgado. – Way of access: http://math.uchicago.edu/~may/REU2014/REUPapers/Morgado.pdf. – Title from the screen.
[4] Stewart I. Concepts of Modern Mathematics / Ian Stewart. – Dover Publications: Amazon Digital Services, Inc, 2012. – 352 p.
[5] Lance S. A survey of primality tests [Electronic Resource] / Stefan Lance. – Way of access: http://math.uchicago.edu/~may/REU2014/REUPapers/Lance.pdf. – August 27, 2014. – Title from the screen.
[6] Krasnobaev V. A. Osnovnye svoistva nepozitsionnoi sistemy schisleniya / V. A. Krasnobaev, S. V. Somov, A. S. Yanko // Systemy upravlinnja, navigacii' ta zv'jazku. – 2013. – Vyp. 1 (25). – S. 110–113.
[7] Grandini D. Notes on Modular Arithmetic [Electronic Resource] / Daniele Grandini. – Way of access: http://math.unm.edu/~daniele/Notes%20on%20 Modular%20Arithmetic.pdf. – Spring 2013. – Title from the screen.
[8] Krasnobaev V. A. Metod ispravleniya odnokratnykh oshibok dannykh, predstavlennykh kodom klassa vychetov / V. A. Krasnobaev, S. A. Koshman, M. A. Mavrina // Elektronnoe modelirovanie. – 2013. – T. 35. – № 5. – S. 43–56.
[9] Barsov V. I. Metodologiya parallel'noi obrabotki informatsii v modulyarnoi sisteme schisleniya: monografiya / V. I. Barsov, L. S. Soroka, V. A. Krasnobaev. – Khar'kov: MON, UIPA, 2009. – 268 s.
[10] Kornilov A. I. Printsipy postroeniya spetsializirovannykh vychislitelei s primeneniem modulyarnoi arifmetiki / A. I. Kornilov, M. Yu. Semenov, O. V. Lastochkin, V. S. Kalashnikov // Institut problem proektirovaniya v mikroelektronike RAN. – 2010. – S. 346–355.
[11] Krasnobayev V. A. A method for increasing the reliability of verification of data represented in a residue number system / V. A. Krasnobayev, S. A. Koshman, M. A. Mavrina // Cybernetics and Systems Analysis. – 2014. – Vol. 50. – Issue 6. – P. 969–976.

Рецензент: В'ячеслав Харченко, д.т.н., проф., академік Академії наук прикладної радіоелектроніки, Національний аерокосмічний університет ім. М. Є. Жуковського, Харків, Україна.
E-mail: v_s_kharchenko@ukr.net

Надійшло: Травень 2017.

Автори:
Віктор Краснобаєв, д.т.н., проф., Харківський національний університет імені В. Н. Каразіна, Харків, Україна.
E-mail: krasnobaev@karazin.ua

Сергій Кошман, к.т.н., доцент, Харківський національний технічний університет сільського господарства імені Петра Василенка, Харків, Україна.
E-mail: s_koshman@ukr.net

Артем Москаленко, к.т.н., доцент, Полтавський інститут бізнесу Міжнародного науково-технічного університету імені академіка Юрія Бугая, Полтава, Україна.
E-mail: moskalenko_artem@ukr.net

Концепція обробки цілочисельних даних, що представлені у системі залишкових класів.

Анотація. Показано, що кодування залишків числа, що представлено відповідними основами системи залишкових класів (СЗК), виконується даними з повної системи найменших невід'ємних лишків (ПСННЛ). У цьому аспекті ПСННЛ є основою для побудови непозиційної кодової структури даних у СЗК. У статті уточнені і систематизовані можливі сфери та напрямки науки і техніки, де є гостра необхідність у швидких, надійних і високоточних цілочислових обчислень. На основі результатів досліджень властивостей СЗК, проаналізовано переваги і недоліки використання модулярної арифметики (МА). Використовуючи результати аналізу завдань цілочислової обробки даних і сукупності позитивних властивостей МА, у статті визначені класи задач і алгоритмів, для яких використання СЗК істотно ефективніше ніж двійкова позиційна система числення.

Ключові слова: система залишкових класів, модулярна арифметика, позиційна система числення, повна система найменших невід'ємних лишків, комп'ютерна система і засоби обробки даних, що представлені у цілочисловому вигляді, клас лишків.

Рецензент: Вячеслав Харченко, д.т.н., проф., академик Академии наук прикладной радиоэлектроники, Национальный аэрокосмический университет им. М. Є. Жуковского, Харьков, Украина.
E-mail: v_s_kharchenko@ukr.net

Поступила: Май 2017.

Авторы:
Виктор Краснобаев, д.т.н., проф., Харьковский национальный университет имени В. Н. Каразина,. Харьков, Украина.
E-mail: krasnobaev@karazin.ua

Сергей Кошман, к.т.н., доцент, Харьковский национальный технический университет сельского хозяйства имени Петра Василенка, Харьков, Украина.
E-mail: s_koshman@ukr.net

Артём Москаленко, к.т.н., доцент, Полтавский институт бизнеса Международного научно-технического университета имени академика Юрия Бугая, Полтава, Украина.
E-mail: moskalenko_artem@ukr.net

Концепция обработки целочисленных данных, представленных в системе остаточных классов.

Аннотация. Показано, что кодирование остатков числа, представленного соответствующими основаниями системы остаточных классов (СОК), производится данными из полной системы наименьших неотрицательных вычетов (ПСННВ). В этом аспекте ПСННВ является основой для построения непозиционной кодовой структуры данных в СОК. В статье уточнены и систематизированы возможные области и направления науки и техники, где есть острая необходимость в быстрых, надежных и высокоточных целочисленных вычислений. На основе результатов исследований свойств СОК, проанализированы преимущества и недостатки использования модулярной арифметики (МА). Используя результаты анализа задач целочисленной обработки данных и совокупности положительных свойств МА, в статье определены классы задач и алгоритмов, для которых использование СОК существенно эффективнее двоичной позиционной системы счисления.

Ключевые слова: система остаточных классов, модулярная арифметика, позиционная система счисления, полная система наименьших неотрицательных вычетов, компьютерная система и средства обработки данных, представленных в целочисленном виде, класс вычетов.