Processing of the residuals of numbers in real and complex numerical domains

A. Yanko [1], V. Krasnobayev Victor [2], A. Kuznetsov[2], B. Akhmetov[2], T. Kuznetsova[2]

[1] Poltava National Technical Yuri Kondratyuk University, Poltava, Ukraine
[2] V. N. Karazin Kharkiv National University, Kharkiv, Ukraine

Abstract. The chapter discusses the procedures for the formation and use of real residuals of real numbers on a real module, as well as complex and real residues of an integer complex number on a complex module. The chapter focuses on the processing of complex and real residuals of an integer complex number by a complex module. This procedure is based on using the results of the first fundamental Gauss theorem. The chapter of the proposed procedure provides examples of determining deductions in a complex numerical domain. On the basis of the considered procedure, an algorithm was developed for determining the real deduction of an integral complex number using a complex module in accordance with which the device was synthesized for its technical implementation. The device received a patent of Ukraine for the invention, which confirms the novelty and practical value of research results. The results obtained in the chapter are advisable to be used when implementing tasks and algorithms in real and complex numerical domains. In particular, the use of real numbers for cryptographic applications was considered.

Keywords: Complete System of the Smallest Non-negative Residues; Computer System and a Data Processing Means which Represented in Integer Form; Modular Arithmetic; Positional Numeral Systems; Residual Classes; Residual Classes system.

1 First Section

1.1 A Subsection Sample

The modern stage of the development of science and technology is characterized by increasingly complex tasks that require their solution. However, the complexity of the tasks being solved is ahead of the growth rate of the power of universal computers. In this aspect, the main areas of improvement of real-time processing of information processing systems (IPS) are the improvement of user productivity and faultless functioning, due to providing the required level of fault-tolerance.

Depending on the architectural decisions taken, the entire set of computing systems in positional numeral systems (PNS), usually binary, can be divided into four main groups: thus, the use of SISD architecture (single stream of instructions and single

data stream) provides a dominant position in the classical von Neumann architecture. In such machines, information is processed sequentially, teams are executed one after another, with each instruction initiating, as a rule, one scalar operation. In this case, the use of parallel operation for the information input-output interface and the processor, the combination of operations performed by separate units and nodes of the arithmetic logic unit do not allow the effective realization of real-time parallel computing systems. Thus, the possibilities for increasing the speed of modern positional computers, which are based on the classical architecture of the successive implementation of operators, virtually reached their limit value; computer systems of the second group – MISD-architecture (multiple stream of commands and single data stream) did not get a lot of practical implementation; these tasks, in which several processors could effectively process one stream of data are still unknown to modern science and technology; the basis of the third group of computing systems consists of devices developed on the basis of SIMD-architecture (single stream of commands and multiple data streams); using SIMD-architecture allows to realize high-speed real-time IPS; with their help, the problems of vector and matrix calculations are effectively solved, the problem of determining the roots of systems of algebraic and differential equations, etc.; a special place is occupied by digital signal processing tasks, which are the most optimal for the SIMD structure. This architecture of the computer system is oriented on parallel-conveyor execution of the most laborious computational operations. To provide the limit for the given level of technology of the productivity of the computer system is possible only at the expense of the use of non-traditional arithmetic, in which the parallelization process is carried out at the level of arithmetic operations (microoperations); An alternative solution to the problem of solving real-time high-performance computing is the use of MIMD architecture (multiple stream of commands and multiple data streams). This class assumes that there are several command processing units in the computer system, united in a single complex and each with its own data and commands (multi-microprocessor, multi-machine, cluster and other similar computing systems). However, in spite of all the advantages mentioned above, such as the availability of memory for each processor element and the independence of the computing process, systems with mass parallelism generated a number of problems associated with the description and programming of process switching and their management. At the same time, the lack of a mathematical device, which allows solving the problem of increasing the productivity of computing systems, is a major deterrent to the widespread use of MIMD-systems with massive parallelism.

Thus, it is obvious that further progressive development of computer technology and information processing tools in PNS is directly related to the transition to parallel computing. This transition, of course, opens up new opportunities in the field of improving and developing computing devices [1].

Reserves for increasing reliability, fault tolerance and durability of functioning, as well as user-generated computing performance are the use of computing structures, specialized calculators and special processors, created on the principle of parallelization of the problem solved (algorithm) at the level of one micro-operation.

The concept of parallelism has long attracted the attention of specialists to its

potential capabilities to increase the productivity and reliability of computing systems. The conducted theoretical, experimental and industrial developments in this direction have allowed to substantiate the basic principles of construction of parallel computing systems. It is precisely with such systems the current perspective of further increasing the computing power and reliability is connected.

In 2005, it turned out 50 years from the date of the publication of the article by the Czech engineer M. Valah, in which it was first proposed to apply for operations on computer numbers instead of operations of the rings of the residual modulo $M = 2^n$ the operation of the rings of the residual modulo $M = m_1 m_2 ... m_n$, where $m_1, m_2, ..., m_n$ – pairwise mutually simple numbers. In computational practice, this was an outstanding idea, since all ring operations modulo $M = m_1 m_2 ... m_n$ were reduced to a homomorphic parallel implementation of the same operations on small modules $m_1, m_2, ..., m_n$. The well-known Chinese theorem on residual, which was previously treated as a structural theorem of abstract algebra, guaranteed this parallelism in calculations over integer numbers, provided that the result of ring operations belongs to the range of integers, which is determined by the product of the modules $M = m_1 m_2 ... m_n$. This idea attracted the attention of a large group of scientists. A new scientific direction arose - modular arithmetic [2].

Over the past 50 years, modular arithmetic (numeral systems in residual classes (NSRC), the class of residuals) has survived periods of rapid development and serious recessions. Currently, there is a progressive increase in interest in modular arithmetic among developers of complex systems related to the processing of signals and images, with cryptographic transformations, etc.

It is known that the non-positional numerical system in the system of residual classes (NSRC) is used in computer systems (CS) to increase the speed of the implementation of integer arithmetic operations. This is due to the presence and influence of the properties of the NSRC both in the structure of the data processing CS, represented in the integer-type, and on the principles of functioning (the numerical system influences the principles of the implementation of arithmetic operations more) of CS. In turn, the structure and principles of the functioning of the CS affect the characteristics of computing systems.

However, there are a number of factors, such as properties of the NSRC, influencing the structure of the CS, as well as the principles of the implementation of arithmetic operations. The use of the results of such research makes it possible to more accurately and precisely estimate the possibility of practical application of non-positional code structures (NPCS) in computational technology.

The creation of NPCS $A = (a_1 \| a_2 \| ... \| a_n)$ in the NSRC is based on the use of the principles of parallelism and independence of the formation of residues a_i. These principles determine the three main properties of the NSRC. Let's analyze each of these properties [3].

1. Independence of each residual in the structure of the NPCS NSRC. This property enables to form the structures of the CS in the NSRC in aggregate form (by the number of *n* bases (modules) of the NSRC) of informatively independent, low-level

computing paths (CP) that function independently of each other and in parallel in time.

At the same time, note that:

- in the general case, the time of execution of arithmetic operations by the CS in the NSRC is determined by the time of execution of operations for the largest bit grid CP;

- the CS in the NSRC has a modular design consisting of separate independent CPs; it allows to carry out repairs and maintenance, as well as carry out operations of control, diagnostics and correction of data errors in the CP CS in the NSRC without interrupting the process of solving the problem, that is, without stopping the calculations;

- errors occurring in the CP CS with base m_i, do not "multiply" to other CPs; It does not matter whether there was a single or multiple error in the CP with base m_i, or even a set of errors of length no greater than the binary digits $\left[\log_2(m_i-1)+1\right]$ [4]. Thus, an error that arose in an arbitrary CP CS with base m_i, or persists in this CP before the end of the calculation, or in the process of subsequent calculations will be self-abolished (for example, if the erroneous value of residual a_i with base m_i of the first number is multiplied by zero second of the second on the same m_i NSRC basis);

2. The equality of residuals in NPCS NSRC. An arbitrary residual a_i of nu,ber $A=(a_1 \| a_2 \| ... \| a_n)$ in the NSRC contains information about the entire output number. This makes it possible, subject to the equation $m_i < m_j$, to replace the out of order CP of CS modulo m_i by the programmed methods, to workable CP modulo m_i, without stopping the task solution [5].

This property is conditioned by the fact that the structure of the CS in the NSRC provides an opportunity to exchange, based on the application of program methods, such characteristics of the CS as the speed of execution of arithmetic operations, the accuracy of the execution of arithmetic operations and the reliability of the execution of arithmetic operations without stopping the calculations in the process of solving the problem. In this aspect, the CS in the NSRC can have different reliability depending on requirements, for example, the accuracy or speed of the calculations. In addition, the structure of the CS in the NSRC allows the organization of degradation of the computer system. This allows (subject to the refusal of the specified elements of the structure) to continue functioning without one or more functions of the CS, or to continue to function with deteriorated quality, for example, with a decrease in speed, or with a decrease in the accuracy of computing, etc.

The use of the first and second properties of the NSRC determines the availability of three types of reservation at the same time in the CS: structural, informational and functional. This, in turn, allows to synthesize mathematical models of fault-tolerance with a more accurate estimate of the required characteristics of the CS [6].

3. The low bitness of residuals, the totality of which determines the NPCS in the NSRC. This property allows to significantly improve the speed of the implementation of arithmetic operations both due to the low-level representation of the remains of the

number in the NSRC, and due to the possibility (in contrast to the positional systems of the calculus) to use table arithmetic; application of the methods of table arithmetic allows to realize the basic arithmetic operations in the NSRC in fact for one cycle of the work of the CS.

The low bitness of the residuals of numbers in the NSRC provides a wide choice of variants of system-technical solutions to the tasks of implementing arithmetic modular operations, based on the following principles:

– adder principle (based on the use of low-level binary adder);

– tabular principle (based on the use of memory elements);

– the circular shift principle (based on the use of shift registers).

Based on the use of the properties of the NSRC, the following (in comparison with positional numerical systems (PNS)) advantages become evident:

– possibility of realization of asynchronous arithmetic calculations at the level of decomposition of numbers, which increases the speed of CS computing;

– the possibility of organizing tabular (matrix) execution of arithmetic operations and sampling of the result of a modular operation in one cycle;

– the ability to create a CS and component with effective detection and correction of errors without interruption in calculations, as well as the ability to synthesize fault-tolerant digital devices;

– the possibility of creating a system for monitoring and correcting errors in the dynamics of the computational process CS;

– providing high active fault tolerance of computing structures based on operative reconfiguration of the structure of the CS;

– the possibility of increasing the reliability of the CS due to the effective use of passive and active fault tolerance.

The set of properties of NSRC determines the possible directions of its effective application. First of all, these are:

– modular and cryptographic integer transformations;

– signal processing;

– processing integer data of large (hundreds and thousands of bits) bitness in real-time;

– processing large data arrays represented in a matrix form;

– data processing in optoelectronic and neurocomputer scientific and technical areas;

– application of NSRC for implementation of algorithms of mobile communication processors, in which it is necessary to provide high speed of data processing with insignificant energy consumption; indeed, the data processing algorithms for mobile communication processors mainly consist of arithmetic operations of compilation and multiplication, thus, the fact of the absence of transfers in performing arithmetic operations in the NSRC allows to reduce the energy consumed by mobile communication processors.

The influence of the properties of the NSRC on the structure and principles of the implementation of arithmetic operations is as follows.

1. Increasing the speed of implementation of arithmetic operations is determined by the parallel structure of data processing in the NSRC and using the principle of

tabular execution of basic arithmetic operations.

2. Improved reliability, fault-tolerance, and survivability of the CS is possible, firstly, by using the property of passive fault-tolerance, which a priori exists in the initial structure of the CS, which operates in the NSRC. In this case, the original natural structure of the CS in the NSRC has the form of a computing structure that is similar to the artificial permanent structural reservation in the PNS. Secondly, increasing the reliability of the CS can be due to the use of active fault-tolerance (dynamic structural redundancy) computing structures in the NSRC.

3. The use of the first and second properties of the NSRC causes more effective than the PNS, the simultaneous application of passive and active fault tolerance, which makes the computer components of the CS a priori more suited to the control and diagnosis of data errors.

4. The influence of the first and second properties of the NSRC determines the possibility of the structure to adapt to the mode of operation of the CS. This circumstance allows directly, in the course of calculations, to perform exchange operations between the reliability of the functioning of the CS, the speed of the implementation of arithmetic operations and the accuracy of the solution of the problem.

The results of the study of the influence of the properties of the NSRC on the structure of the CS and the principles of implementation of arithmetic operations have shown that the use of NSRC can increase the speed of arithmetic operations and increase the failure-resistance of the functioning of the CS. In addition, the use of NSRC allows to create a unique system for monitoring, diagnosis and correction of data errors in CS without stopping calculations, which has no analogues in PNS.

1. Increasing the speed of implementation of arithmetic operations in the NSRC is achieved through the possibility of organizing parallel processing of data, as well as by using the tabular principle of the implementation of arithmetic operations.

2. The use of the properties of the NSRC determines the existence of three types of reservation at the same time in the CS: structural, informational and functional. This, in turn, allows us to increase the failure-resistance of non-positional computing structures in the NSRC through the application of methods based on passive (permanent structural reservation) and active (structural reserve replacement) fault-tolerance.

3. It was discovered that the CS and components in the NSRC belong to computational structures that are easy to control and diagnose. This feature facilitates the development of methods for effective control and diagnostics of data in the NSRC. Thus, the use of the properties of the NSRC makes it possible to create a unique system for monitoring and correcting data errors without stopping calculations, which is especially important for the CS, which function as part of complex technical real-time systems.

In the 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 [2].

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 PNS, it is practically impossible to achieve it. 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 [2].

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 [2].

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 $m_1, m_2, \ldots m_n$ 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 residues:

Actually, there is an opinion [2], 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 [3].

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 re-

searches, 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 analysis of the methods for increasing of the efficiency of SEC in the HEC Jacobian allowed to theoretically substantiate and to practically demonstrate the dependence of the realization of the efficiency of SEC operations in the Jacobian of HEC upon the aggregate of the following basic characteristics - type of realization of cryptographic transformations (software, hardware and software-hardware); algorithm type of the SEC divisors; the prescribed base field, over which the given curve is set; the type of the curve; the values of the curve coefficients; the selected system of coordinates, in which the HEC Jacobian divisors (affinity, projective, weighted and mixed) are represented; the accepted method of arithmetical transformations etc. The known methods of realization of the SEC algorithm (the Quantor divisor summation method, the Kobliz method, the method of arithmetic transformations of divisors in the HEC Jacobian of the second, the third and the fourth kinds, methods of summation of divisors with different weights, the Karatsuba method for multiplication and reduction of the polynomial functions by the module in the field, the method based upon several results of the Chinese remainder theorem etc.) do not always satisfy the requirements with respect to the efficiency of cryptographic transformations. At the same time, the reference sources [4] demonstrate high efficiency of the modular arithmetic (MA) codes, i.e., the system of computation in remainder classes (CRC) while solving separate problems of digital data processing (solving of filtering problems, problems of realization of FFT, DFT etc.) from the point of view of the high efficiency of their realizations. Thus, it is known that the Fourier transformation is related to calculation of the polynomial of the kind $P(x) = \sum_{i=1}^{n-1} \alpha_i x^i$. One of the applications of the Fourier transformation lies in calculation of the convolution $\sum_{i=1}^{n} \alpha_i \beta_i$ of two n-dimensional vectors $A = (\alpha_1, \alpha_2, ..., \alpha_n)$ and $B = (\beta_1, \beta_2, ..., \beta_n)$. In the given case the convolution operation is the complete analogue to the realization of arithmetic operations of multiplication of two numbers *A* and *B* in MA with consequent summation of the components of the kind $\alpha_i \beta_i (\mathrm{mod}\, m_i) + \alpha_j \beta_j (\mathrm{mod}\, m_j)$

In the given aspect this phenomenon stipulates the importance and actuality of the search for the methods for increasing of the efficiency, reliability and validity of the public-key cryptographic transformations on the basis of the using the properties of the position-independent MA code structures.

The objective of the paper is to develop a highly efficient method for realization of public-key cryptographic transformations on the basis of the using the position-independent MA codes of position-independent structures, i.e., CRC codes.

The influence of the CRC main parameters (independence, equality and short form of the operand-representing remainders) upon the structure and the principles of operation of the data processing system (DPS) in MA are considered in details in [5]. In particular, it is demonstrated that short form of the rests in representation of numbers in modular arithmetic provides for the possibility of wide selection between the options of system engineering solutions at realization of the modular arithmetic operations.

It is known that there exist four principles of realization of arithmetic operations in MA – the summation principles (SP) (on the base of short binary summators); the table principle (TP) (on the base of using ROM); the direct logical principle of realization of arithmetic operations based on description of module operations at the level of the systems of switching functions by means of which the values of binary digits of the resulting deductions are formed (it is reasonable to use systolic and programmable logical matrices as well as EPLD as the element base for technical realization of the given principle); the principle of ring shift (PRS) based on using of the ring shift register (RSR) [6].

The absence of bit-to-bit associations (the absence of the transport process) between the binary digits in operands processed in DPS during the process of cryptographic transformations (at realization of module operations) on the basis of TP or PRS is one of the main and the most attractive particularities of modular arithmetic. Within the base notation system (BNS) the performance of an arithmetic operation assumes the subsequent processing of operands digits upon the rules determined by the contents of the given operation and cannot be finished up to the moment until the values of all of the intermediate results considering all the relationships between the bits, are sequentially determined. Thus, BNS in which the information is represented and processed in the present-day DPS, have a substantial drawback – the presence of bit-to-bit associations which impose their imprint upon the methods of realization of arithmetic operations; make the hardware more complicated, decrease the trustworthiness of calculations and restrict the computing speed of crypto-graphic transformations realization. Therefore, it is only natural to seek for the opportunities of creation of the kind of arithmetic, in which the bit-by-bit associations would be absent. In this connection it is worth to pay attention to the base notation system in the residual classes. The system of residual classes possesses a valuable parameter of independence of the remainders upon each other pursuant to the accepted system of bases. This independence opens up wide opportunities to the development of not only the new kind of machine arithmetic but also to the principally new structural realization of DPS, which, in its turn, is substantially extending the sphere of application of the machine arithmetic. In most of the reference sources it is noted that implementation of non-traditional methods for data representation and processing in the numerical systems with parallel structure and, in particular, within the so-called modular base notation systems possessing the maximal level of the internal parallelism in organization of the data processing procedures is one of the practical trends in increasing of the user efficiency of computing equipment. The position-independent computing system in the residual classes is also referred to the above systems.

Short form of the rests, which represent the operand, is one of the CRC properties.

It is just this property that allows to substantially increase the computing speed at execution of the arithmetic operations due to the possibility of application (unlike in BNS) of the table arithmetic where the arithmetic operations of addition, deduction and multiplication are performed practically in one and the same cycle [4]. The search for the way of increasing of the data processing efficiency led to the necessity of development of the table method for realization of modular operations on the basis of PRS.

Thus, despite the difference in the digital structure of the tables of modular operations of summation deduction and multiplication there was created a new original table method for realization of arithmetic operations in MA. On the basis of the method it is possible to synthesize a structurally simple, highly reliable and super-efficient DPS in MA, the basis of which is formed by three separated switches each of them realizing only 0.25 part of the relevant complete table of modular operations of multiplication and deduction (the first switch is the II quadrant of the multiplication table; the second and the third switches are respectively I and II quadrants. In this sense the table multiplication code obtained a new quality and became the universal table code for performance of the three arithmetic operations in MA.

At the table option of realization of arithmetic operations the bit-to-bit assotiations between the processed operands are absent completely. However, for a quite large-digit grid of DPS (for larger in value modules of TMC) the number and complexity of equipment units in operation devices are sharply increased.

It is important and actual to consider the intermediate option of realization of arithmetic operation in TMC based on application of the ring shift principle.

In [4] it is considered the principle of realization of arithmetic operations in TMC – the ring shift principle, the particularity of which lies in the fact that the result of the arithmetic operation $(\alpha_i \pm \beta_i) \bmod m_i$ upon the arbitrary module of TMC set by the aggregate of bases $\{m_j\}$ $(j = \overline{1,n})$ is determined only at the expense of cyclic shifts of the set digital structure. Actually, the well-known Kally theorem is setting the isomorphism between the elements of the finite Abelian group and the elements of the permutation group.

One of the consequences of the Kaly theorem is the conclusion that reflection of the elements of the Abelian group upon the group of all of the integer numbers is homomorphous. This circumstance allows to organize the process of determination of the result of arithmetic operations in TMC by means of using PRS.

Thus, the operand in MA is represented by the set of *n* remainders $\{\alpha_i\}$ formed by means of subsequent division of the initial number *A* by *n* mutually paired prime integers $\{m_i\}$ for $(i = \overline{1,n})$. In this case the aggregate of remainders $\{m_i\}$ is directly equaled to the amount *n* of prime Galois fields having the form of $\sum_{i=1}^{n} GF(m_i)$.

In order to consider the method of realization of arithmetic operations in TMC it would be sufficient to consider the option of for an arbitrary finite Galois field *GF* (m_i) at $i = const$, i.e., for the specific reduced system of deductions upon the module m_i.

Let the Kally table is made for the set operation of modular summation $(\alpha_i + \beta_i) \bmod m_i$, in the field GF (m_i). From the existence of a neutral element in the field GF (m_i), which the elements of the given field are arranged in the ascending order. And from the fact that in the field of deductions GF (m_i) these elements are different (the order of the group is equal to m_i) it follows that each row (column) of table contains all of the field elements exactly one time each. The use of the above particularities allows to realize the operations of modular summation and deduction in TMC by applying PRS with the help of n ring $M = m_i \left(\left[\log_2 (m_i - 1) \right] + 1 \right)$ – digit shifting registers.

Let the arbitrary algebraic system be represented in the form $S = \langle G, \otimes \rangle$, where G is the non-empty set; $\otimes$ is the type of operation determined for any of two elements $\alpha_i, \beta_i \in G$. The operation of summation $\oplus$ in the set of the classes of deductions R generated by the ideal J forms up a new ring called the class of deductions ring R/J. It can be represented in the form of Z/m_i where Z is the set of integers 0, ±1, ±2, …. (If the base of TMC m_i is the prime integer, then Z/m_i is the field). As it is indicated above just this circumstance is stipulating the possibility of realization of the arithmetic operation of summation in TMC without any bit-to-bit transfers by means of the ring shift [4].

On the basis of the principle suggested in [4] there was developed the method of realization of arithmetic operations in TMC (the method of binary position and remainder encoding). The essence of the developed method lies in the fact that the initial digital structure for each module (base) of TMS is represented in the form of the contents of the first row (column) of the modular summation (deduction) table $(\alpha_i \pm \beta_i) \bmod m_i$ of the form $P_{init}^{(m_i)} = \left[P_0(\alpha_0) \| P_1(\alpha_1) \| ... \| P_{m_i - 1}(\alpha_{m_i - 1}) \right]$ where $\|$ is the operation of concatenation (gluing); $P_v(\alpha_v)$ is the k-bit binary code correspondent to the value of the a_v-th remainder $(\alpha_v = \overline{0, m_i - 1})$ of the number upon the module m_i; $k = \left[\log_2 (m_i - 1) + 1 \right]$. For the set specific module $m_i = 5$ the initial digital structure of the RSR content has the following representation $P_U^{(5)} = \left[000 \| 001 \| 010 \| 011 \| 100 \right]$.

Thus, by means of the ring shift registers used in BNS it is easy to realize the arithmetic operations in TMC, where the degrees of cyclic permutations as considered on the basis of are determined by the following expressions:

$$\left[P_0(\alpha_0) \| P_1(\alpha_1) \| ... \| P_{m_i - 1}(\alpha_{m_i - 1}) \right] = \left[P_z(\alpha_z) \| P_{z+1}(\alpha_{z+1}) \| ... \| P_0(\alpha_0) \| ... \| P_{m_i - 1}(\alpha_{m_i - 1}) \right]^Z, \quad (1)$$

$$\left[P_0(\alpha_0) \| P_1(\alpha_1) \| ... \| P_{m_i - 1}(\alpha_{m_i - 1}) \right]^{-Z} = \left[P_{m_i - 1 - z}(\alpha_{m_i - 1 - z}) \| ... \| P_{m_i - z}(\alpha_{m_i - z1}) \| \right. \\ \left. \| ... \| P_0(\alpha_0) \| P_1(\alpha_1) \| ... \| P_{m_i - z - 2}(\alpha_{m_i - z - 2}) \right]. \quad (2)$$

We note that $\left[P_0(\alpha_0)\left(P_1(\alpha_1)\right\|...\left\|P_{m_i-1}(\alpha_{m_i-1})\right]^{m_i}=\varepsilon$, i.e., at $z=m_i$ all the elements of the ordered set $\left\{P_j(\alpha_j)\right\}$ for $(j=\overline{0,m_i-1})$ remain at the initial position. During the technical realization of the given method the first operand a_i is determining the number α_i of the digit $P_{\alpha_i}(\alpha_{\alpha_i})$ with the content of the modular operation result upon the module mi and the second operand β_i – the number of RSR digits (of $\beta_i k$ – bit binary digits) upon which it is necessary to perform the shifts of the initial content of the RSR pursuant to the algorithms (1), (2). The main drawbacks of the suggested method for realization of arithmetic operations in TMC include comparatively larger time for execution of integer-number arithmetic modular operations that increases the efficiency of using of PRS. This drawback is stipulated by the fact that the structure $P_{init}^{(m_i)}$ is represented by the set of initial remainders of the first row of the matrix $(\alpha_i+\beta_i)\bmod m_i$, which are reflected by the binary code. In this case the time for realization of the modular summation of two operands $A=(\alpha_1,\alpha_2,...,\alpha_{n-1},\alpha_n)$ and $B=(\beta_1,\beta_2,...,\beta_{n-1},\beta_n)$ in TMC is determined by the expression:

$$t=k\beta_{\max i}\tau\,, \tag{3}$$

where τ is the time of shift of one binary digit of RSR.

We consider the method for realization of arithmetic operations in TMC, which is deprived of the above drawback. It is the method of unitary position and residual encoding according to which the informational structure $P_{init}^{(m_i)}$ of the arbitrary module m_i, of TMC is represented in the form of a unitary (m_i-1) –bit code.

$$P_{init}^{(m_i)}=\left[P(\alpha_{i-1})\left\|P(\alpha_{i-2})\right\|...\left\|P(1)\right\|P(0)\right], \tag{4}$$

where $P(\alpha_j)$ is the binary digit of the digital structure (4), the unitary condition of which corresponds to the value of the operand α_j represented by a unitary code $(\alpha_j=\overline{0,m_i-1})$. In this case the initial condition of RSR includes m_i-1 binary digits and schematically can be represented in the form of.

As this takes place, the first operand $\{\alpha\}$ represented by a unitary code upon an arbitrary module m_i of TMC is entered into the *j*-th digit of RSR, i.e., transfers the *j*-th binary digit into the unitary condition. The second operand β_1 is pointing out to the number by the shift z of the RSR content determining the time of realization of arithmetic operations upon the module m_1 of TMC, i.e.,

$$t_{next}=\beta_i\tau\,. \tag{5}$$

We note that the time of realization of arithmetic operation *A*+*B* in TMC will be determined by the time of performing of the operation for the maximal value

$\left(\beta_{\max i}(i=\overline{1,n})\right)$ of the remainder from the set $\{\beta_i\}$ for the given operand $B=(\beta_1,\beta_2,...,\beta_n)$, i.e.

$$t_{next}=\beta_i\tau. \tag{5}$$

Analysis of the expressions (5) and (6) demonstrates that the developed method of unitary representation reduces by $k=\left[\log_2(m_i-1)+1\right]$ times the time of performing of the arithmetic operations as compared to the method of binary encoding.

Let us consider one of the most interesting and important questions in the theory of whole complex numbers – the definition of the class of least residues and the related first fundamental Gauss theorem. This theorem establishes an isomorphism between the set of real and complex residuals of numbers.

The above material leads to the first fundamental Gauss theorem. This theorem establishes an isomorphism between complex and real residues.

Theorem. Given a complex module $\dot{m}=p+qi$, whose norm N is equal to $N=p^2+q^2$ and for which p and q are mutually prime numbers, each integer complex number is $\dot{A}=a+bi$ by the complex module $\dot{m}$ is comparable to one and only one real residual from the $\overline{0,N-1}$ number series, i.e. we have $\dot{A}\equiv h(\mathrm{mod}\,\dot{m})$ [5].

Proof. From the theory of numbers it is known that for two mutually simple numbers p and q you can find such two integers u and v, that the following condition is true:

$$u\cdot p+v\cdot q=1. \tag{6}$$

First we show that the following identity exists:

$$i=u\cdot p-v\cdot q+\dot{m}\cdot(v+ui). \tag{7}$$

Then:

$$\begin{gathered}i=u\cdot q-v\cdot p+(p+q\cdot i)\cdot(v+u\cdot i)=\\=u\cdot q-v\cdot p+(p\cdot v+p\cdot u\cdot i+q\cdot v\cdot i+q\cdot u\cdot i^2)=\\=u\cdot q-v\cdot p+(p\cdot v+p\cdot u\cdot i+q\cdot v\cdot i-q\cdot u)=\\=u\cdot q-q\cdot u-v\cdot p+p\cdot v+p\cdot u\cdot i+q\cdot v\cdot i=\\=(u\cdot p+v\cdot q)\cdot i.\end{gathered}$$

Let there be a complex number $\dot{A}=a+bi$. Then, taking (7) into account, we get:

$$a+bi=a+b\cdot[u\cdot q-v\cdot p+\dot{m}\cdot(v+ui)]=a+(u\cdot q-v\cdot p)\cdot b+\dot{m}\cdot(v\cdot b+u\cdot bi)]. \tag{8}$$

We denote by h the smallest positive real residue of number $a+(u\cdot q-v\cdot p)\cdot b$ modulo N, i.e.

$$h \equiv [a + (u \cdot q - v \cdot p) \cdot b] \bmod N . \quad (9)$$

In view of expression (6) we have that $i = i$. Thus, identity (7) is true.
We write the expression (9) in the form:

$$a + (u \cdot q - v \cdot p) \cdot b = h + s \cdot N = h + s(p + qi) \cdot (p - qi) = h + \dot{m} \cdot (p \cdot s - q \cdot si) . \quad (10)$$

Then, in view of (8), the following will be true:

$$a + bi = h + \dot{m} \cdot (p \cdot s - q \cdot si) + \dot{m} \cdot (v \cdot b + u \cdot bi) = h + \dot{m} \cdot \left[p \cdot s + v \cdot b + (u \cdot b - q \cdot s)i \right], \quad (11)$$

or in the following form:

$$(a + bi) \equiv h (\bmod \dot{m}) . \quad (12)$$

Thus, it is proved that the smallest complex residue $x + yi$ of a complex number $a + bi$ is comparable modulo m_i to one and only one of the real numbers $0, 1, 2, ..., N - 1$.

Let us prove by contradiction that this number is unique. Assume that there are two comparisons:

$$\begin{aligned} (a + bi) &\equiv h_1 (\bmod \dot{m}), \\ (a + bi) &\equiv h_2 (\bmod \dot{m}). \end{aligned} \quad (13)$$

Based on the property of comparisons, we have $h_1 \equiv h_2 (\bmod \dot{m})$ or $(h_1 - h_2) \equiv 0 (\bmod \dot{m})$, i e.

$$(h_1 - h_2) = \dot{m} \cdot (e + f \cdot i) . \quad (14)$$

From (14) we get the following:

$$\begin{gathered} (h_1 - h_2) = (p + qi) \cdot (e + fi), \\ (h_1 - h_2) \cdot (p - qi) = (p + qi) \cdot (p - qi) \cdot (e + fi), \\ (h_1 - h_2) \cdot (p - qi) = (p^2 + q^2) \cdot (e + fi), \\ (h_1 - h_2) \cdot (p - qi) = N \cdot (e + fi), \\ (h_1 - h_2) \cdot p - (h_1 - h_2) \cdot qi = N \cdot e + N \cdot fi. \end{gathered}$$

which is equivalent to the following two real equalities:

$$\begin{cases} (h_1 - h_2) \cdot p = N \cdot e, \\ (h_1 - h_2) \cdot q = -N \cdot f, \end{cases} \quad (15)$$

since complex numbers are equal to each other, their real and imaginary parts are equal. Multiplying the first equality (15) by the value u and the second by the value v and adding them, we get:

$$(h_1 - h_2) \cdot (u \cdot p + v \cdot q) = N \cdot (e \cdot u - f \cdot v),$$

from where, taking into account the expression (6):

$$(h_1 - h_2) \equiv N \cdot (e \cdot u - f \cdot v),$$

or

$$(h_1 - h_2) \equiv 0 (\mathrm{mod}\, N). \quad (16)$$

So, as by assumption $h_1, h_2 < N$, the comparison (16) is possible only in the case when $h_1 = h_2$. Thus, the possibility of the existence of two different numbers h_1 and h_2, smaller than N, which would be comparable with the number $a + bi$ modulo $\dot{m}$. There is only one such number h, which is determined from the comparison:

$$[a + (u \cdot q - v \cdot p) \cdot b] \equiv h (\mathrm{mod}\, N), \quad (17)$$

or

$$\mathrm{Z} = (a + b \cdot \rho) \equiv h (\mathrm{mod}\, N). \quad (18)$$

The expression $\rho = u \cdot q - v \cdot p$, by means of which a correspondence is established between the complex and real residue modulo $\dot{m} = p + qi$, is called the isomorphism coefficient (IC).

As an example, using formulas (17) and (18), we define the values of real residues $Z_i \equiv h_i (\mathrm{mod}\, N)$ $(i = \overline{0, N-1})$, corresponding to the smallest complex residues $x + yi$ modulo $\dot{m} = 1 + 2i$.

First, we define the value of the isomorphism coefficient $\rho = u \cdot q - v \cdot p = u \cdot 2 - v \cdot 1$. Values u and are determined from the relation known in number theory $u \cdot p + v \cdot q = 1$, i.e. $u \cdot 1 + v \cdot 2 = 1$. By selection (search) we determine that $u = -1$, and $q = 1$. Thus, $\rho = (-1) \cdot 2 - 1 \cdot 1 = -3$, or $(-3) \bmod 5 = 2$ $(N = p^2 + q^2 = 1^2 + 2^2 = 5)$.

Determine the values of the smallest real positive residues h_i, that are isomorphic to the smallest complex residues.

For $\dot{A} = 0 + 0i$. $Z_0 = a + b\rho = 0 + 0 \cdot \rho = 0$. $h_0 \equiv 0 (\mathrm{mod}\, 5)$.

For $\dot{A} = -1 + i$. $Z_1 = -1 + 1 \cdot (-3) = -4$. $h_1 \equiv 1 (\mathrm{mod}\, 5)$.

For $\dot{A} = i$. $Z_2 = 0 + 1 \cdot (-3) = -3$. $h_2 \equiv 2 (\mathrm{mod}\, 5)$.

For $\dot{A} = -1 + 2 \cdot i$. $Z_3 = -1 + 2 \cdot (-3) = -1 - 6 = -7$. $h_3 \equiv 3 (\mathrm{mod}\, 5)$.

For $\dot{A} = 2 \cdot i$. $Z_4 = 0 + 2 \cdot (-3) = -6$. $h_3 \equiv 4 (\mathrm{mod}\, 5)$.

Based on the results of the Gauss theorem, it is not difficult to show the following relation between the smallest complex and real residues. Assume that for two numbers $\dot{A}_1 = a_1 + b_1 i$ and $\dot{A}_2 = a_2 + b_2 i$ there are such values h_1 and h_2, $h_{\pm}$ and $h_{\times}$, that if $\dot{A}_1 \equiv h_1 (\mathrm{mod}\, \dot{m})$ and $\dot{A}_2 \equiv h_2 (\mathrm{mod}\, \dot{m})$, then the following are true $\dot{A}_1 \pm \dot{A}_2 \equiv h_{\pm} (\mathrm{mod}\, \dot{m})$ and $\dot{A}_1 \cdot \dot{A}_2 \equiv h_{\times} (\mathrm{mod}\, \dot{m})$. Then $h_{\pm} \equiv (h_1 \pm h_2) \bmod N$ and $h_{\times} \equiv (h_1 \cdot h_2) \bmod N$, where $N = p^2 + q^2$.

Let us give specific examples of the determination of the real deduction of an integer complex number by the complex module.

Example 1. Solve the comparison $(16 + 7i) \equiv h \bmod (5 + 2i)$.

Since GCD $(5, 2) = 1$, the condition of the first fundamental Gauss theorem holds, therefore, there is a complete system of real residues modulo $N = p^2 + q^2 = 5^2 + 2^2 = 29$. The real deduction h is determined from the comparison (18), i.e.

$$16 + 7 \cdot \rho \equiv h (\mathrm{mod}\, 29).$$

The isomorphism coefficient ρ is $\rho = u \cdot q - v \cdot p = u \cdot 2 - v \cdot 5$, where the values u and v are determined from the condition of equality (6).

In this case we have that $u = 1$ and $v = -2$, i.e. $1 \cdot 5 + (-2) \cdot 2 = 5 - 4 = 1$.

In this case IC $\rho = 1 \cdot 2 - (-2) \cdot 5 = 2 + 10 = 12$. Therefore $16 + 7 \cdot \rho = = 16 + 7 \cdot 12 \equiv h (\mathrm{mod}\, 29)$ and $h \equiv 13 (\mathrm{mod}\, 29)$. We can write that as $16 + 7i \equiv 13 \bmod (5 + 2i)$.

Example 2. Solve the comparison $(1 + i) \equiv h \bmod (1 + 2i)$.

Since GCD $(p, q) = (1, 2) = 1$. $N = p^2 + q^2 = 1 + 2^2 = 5$. $\dot{A} \equiv h (\mathrm{mod}\, \dot{m})$. $h \equiv (a + b \cdot \rho) \bmod N$.

The value of IC is $\rho = u \cdot q - v \cdot p = u \cdot 2 - v \cdot 1$, and the values of u and v are determined from the relation (6). We get that $u = -1$, $v = 1$. In this case, the IC is $\rho = (-1) \cdot 2 - 1 \cdot 1 = -2 - 1 = -3 \equiv 2 (\mathrm{mod}\, 5)$.

$$Z = a + b \cdot \rho = 1 + 1 \cdot (-3) = -2.$$
$$Z \equiv h (\mathrm{mod}\, N).$$
$$(-2) \equiv h (\mathrm{mod}\, 5).$$
$$h = 3.$$
$$x + yi = 4 + 2i \Rightarrow h = 3,$$
$$(1 + i) \equiv 3 \bmod (1 + 2i).$$

Consider the examples of determining the complex and real deductions of an integral complex number with respect to a complex module $\dot{m}=1+2i$ with the control of the correctness of the solution of the problem.

Example 3. Determine the complex deduction $x+yi$ of complex number $\dot{A}=1+i$ by the complex modulus $\dot{m}=1+2i$, i.e. find $\dot{A}\equiv(x+yi)\bmod\dot{m}$ ($a=1$, $b=1$; $p=1$, $q=2$; $N=5$). By the formula (12) we have that:

$$\begin{cases}(1\cdot1+1\cdot2)\equiv(x\cdot1+y\cdot2)\bmod5,\\(1\cdot1-1\cdot2)\equiv(y\cdot1-x\cdot2)\bmod5.\end{cases}$$

$$\begin{cases}3=x+2y,\\-1=-2x+y.\end{cases}$$

$$x=3-2y,$$

$$-1=-2\cdot(3-2y)+y,$$

$$-1=-6+4y+y,$$

$$5y=5,$$

$$y=1.$$

$$x=3-2y=3-2=1;\ x=1.$$

Answer: the complex deduction $x+yi$ of complex number $\dot{A}=1+i$ in a complex modulus $\dot{m}=1+2i$ is equal to a complex number $x+yi=1+i$.

Example 4. Determine the smallest deduction $x+yi$ of number $\dot{A}=1+i$ modulo $\dot{m}=1+2i$, i.e. define the value of $\dot{A}\equiv(x+yi)\bmod(1+2i)$ ($a=1$, $b=1$; $p=1$, $q=2$; $N=5$). By the formula (8) we have that: $R=(1\cdot1+1\cdot2)\bmod5=3$; $R'=(1\cdot1-1\cdot2)\bmod5=(-1)\bmod5=4$.

$$x+yi=\frac{3\cdot1-4\cdot2}{5}+\frac{4\cdot1+3\cdot2}{5}i=-\frac{5}{5}+\frac{10}{5}i=-1+2i.$$

Thus, $x+yi=-1+2i$ or $\dot{A}\equiv(-1+2i)\bmod(1+2i)$.

Example 5. Solve the comparison $\dot{A}\equiv h\bmod\dot{m}$, where $(1+i)\equiv h\bmod(1+2i)$ ($a=1$, $b=1$; $p=1$, $q=2$; $N=5$); formulas (6), (17), (18):

$$u\cdot p+v\cdot q=1,\ u=-1,$$

$$u\cdot1+v\cdot2=1,\ v=1.$$

$$\rho=u\cdot q-v\cdot p.$$

$$Z=a+b\cdot\rho\to Z\equiv h\bmod N.$$

$$\rho=(-1)\cdot2-1\cdot1=-2-1=-3.$$

$$Z=[1+1\cdot(-3)]\bmod5=(-2)\bmod5=3.$$

Check. We will check the results. In example 4, the smallest complex deduction $(-1+2i)$ was obtained, and in example 5, a real deduction $h=3$ was obtained. In accordance with the data of table 2, we have that $(-1+2i) \sim 3$.

Example 6. Determine the complex deduction $x+yi$ of complex number $\dot{A}=3+4i$ by complex module $\dot{m}=1+2i$. $N=p^2+q^2=1^2+2^2=5$.

In accordance with the well-known (12) rule, we compose a system of comparisons in the form:

$$\begin{cases}(3\cdot 1+4\cdot 2)\equiv(x\cdot 1+y\cdot 2)\bmod 5,\\(4\cdot 1-3\cdot 2)\equiv(y\cdot 1-x\cdot 2)\bmod 5.\end{cases}$$

or

$$\begin{cases}11\equiv(x+2y)\bmod 5,\\(-2)\equiv(-2x+y)\bmod 5.\end{cases}$$

Based on the system of comparisons, we will compose a system of two linear equations:

$$\begin{cases}x+2y=11,\\-2x+y=+3,\end{cases}$$

because $(-2)=3\bmod 5$.

$$\begin{gathered}x=11-2y,\\-2\cdot(11-2\cdot y)+y=3,\\-22+4y+y=3,\\5y=25,\\y=5.\\x=11-2y=11-10=1.\end{gathered}$$

Thus, $x+yi=1+5i$.

Example 7. Determine the smallest complex deduction $x+yi$ of complex number $\dot{A}=3+4i$ by complex module $\dot{m}=1+2i$; $N=5$.

In accordance with the expression in (8), we have that the smallest complex deduction is equal to:

$$(x+yi)=\frac{R\cdot p-R'\cdot q}{N}+\frac{R'\cdot p+R\cdot q}{N}i.$$

Pre-define the values R and R':

$$R = (a \cdot p + b \cdot q) \bmod N = (3 \cdot 1 + 4 \cdot 2) \bmod 5 = 11 (\bmod 5) = 1;$$
$$R' = (b \cdot p - a \cdot q) \bmod N = (4 \cdot 1 - 3 \cdot 2) \bmod 5 = (-2) \bmod 5 = 3.$$

In this case, we have that:

$$(x + yi) = \frac{1 \cdot 1 - 3 \cdot 2}{5} + \frac{3 \cdot 1 + 1 \cdot 2}{5} = -\frac{5}{5} + \frac{5}{5} = -1 + i.$$

So the smallest complex deduction is $-1+i$.

Example 8. Determine the real deduction h of complex number $\dot{A} = 3 + 4i$ modulo $\dot{m} = 1 + 2i$; $N = 5$. Or you can formulate the task as follows. Solve the comparison $(3 + 4i) \equiv h \bmod (1 + 2i)$.

In accordance with expression (18), we have that $(a + b\rho) \equiv h (\bmod N)$, where the isomorphism coefficient ρ is $\rho = u \cdot q - v \cdot p$. Based on formula (6), we define the values u and v, i.e. $u \cdot p + v \cdot q = 1$ or $u \cdot 1 + v \cdot 2 = 1$.

So, with the values $u = -1$ and $v = 1$, the condition (6) is true, i.e. $(-1) \cdot 1 + 1 \cdot 2 = 1$.

Based on the calculations we get that $\rho = u \cdot q - v \cdot p = (-1) \cdot 2 - 1 \cdot 1 = -3$.

$$\mathrm{h} = (a + b \cdot \rho) = (3 + 4 \cdot (-3)) \bmod 5,$$

or

$$(-9) \bmod 5 = 1.$$

Check. We will check the results. In example 7, the smallest complex deduction $(-1+i)$, was obtained, and in example 8 we obtain a real deduction $h = 1$. In accordance with the data of table 1 we have that $(-1+i) \sim 1$.

Conclusion

In the presented chapter, the approach and the procedure for determining real residuals in a real number domain was considered. The main attention was paid to the description of the procedure for processing residuals of complex numbers by a complex module based on the use of the results of the first fundamental Gauss theorem. Many examples of determining the deduction of integer data in a complex number domain are given. Based on the procedure described, a device was developed for its technical implementation. The device for determining residuals of real and complex numbers in the system of residual classes (SRC) received a patent of Ukraine for invention. This confirms the global novelty and practical significance of the research results presented in this chapter. The examples of the implementation of real deductions for performing arithmetic modular operations in cryptography are shown. The results shown in the chapter are advisable to be used when solving problems and algorithms in the SRC in the complex numerical domain. The use of the considered procedure will help to increase the efficiency of the use of SRCs for the implementation of integer operations in a complex number domain.

References

1. Akushskii, I. Ya., Yuditskii, D. I.: Machine Arithmetic in Residual Classes [in Russian]. Sov. Radio, Moscow (1968).
2. Yanko, A., Koshman, S., Krasnobayev, V.: Algorithms of data processing in the residual classes system. In: 4th International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T), pp. 117-121. Kharkov (2017).
3. Krasnobayev, V.A., Yanko, A.S., Koshman, S.A.: A Method for arithmetic comparison of data represented in a residue number system. Cybernetics and Systems Analysis 52(1), pp. 145-150 (2016).
4. Krasnobayev, V.A., Koshman, S.A., Yanko, A.S.: Conception of realization of criptographic RSA transformations with using of the residue number system. ISCI'2017: Information Security in Critical Infrastructures. Collective monograph. Edited by Ivan D. Gorbenko and Alexandr A. Kuznetsov. LAP Lambert Academic Publishing, Omni Scriptum GmbH & Co. KG. ISBN: 978-3-330-06136-1. [Chapter № 3 in monograph, pp. 81-92]. Germany (2017).
5. Ponochovniy, Y., Bulba, E., Yanko, A., Hozbenko E.: Influence of diagnostics errors on safety: Indicators and requirements. In: 2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT), pp. 53-57. Kyiv, (2018).