Algorithms for Determining Residues Modulo in a Complex Numerical Domain

Victor Krasnobayev [0000-0001-5192-9918], Alexandr Kuznetsov [0000-0003-2331-6326], Anna Kononchenko [0000-0002-8101-6500] and Tetiana Kuznetsova [0000-0001-6154-7139]

V. N. Karazin Kharkiv National University, Svobody sq., 4, Kharkiv, 61022, Ukraine

v.a.krasnobaev@gmail.com, kuznetsov@karazin.ua, akononpro@gmail.com, kuznetsova.tatiana17@gmail.com

Abstract. An important aspect of improving modern computer systems and their components is an increasing the speed of arithmetic calculations, including due to the use of new mathematical models and methods based on non-positional residue number systems. The increase in the volume of processed data in modern computer systems leads to the additional risks and threats of unintentional failures and denials of service. This is especially important when building fault-tolerant critical information systems in which failure or denial of service can lead to catastrophic consequences. The article discusses arithmetic operations in the ring of residue classes. These techniques make it possible to implement fast and fault-tolerant computing for modern computer systems and telecommunication networks. We propose an algorithm for calculating the residues of integer data in a complex numerical domain. The algorithm is based on the use of the first fundamental Gauss theorem, which establishes an isomorphism between complex and real residues. Examples of determining the residues of integer data in a complex numerical domain are presented, which clearly demonstrate the constructiveness of the proposed techniques.

Keywords: Computer Systems, System of Residual Classes, Reliable Calculations, Arithmetic Operations

1 Introduction and Literature Review

The increase in the volume of processed and transmitted data in modern computer systems leads to the additional risks and threats of non-intentional failures and denials of service [1–3]. In this sense, an important direction of research is to increase the speed of computing devices based on the use of new mathematical models and computation methods [4–6], including non-positional residue number systems.

It is known, that in present time performance increasing of the integer data handling computer system and components (CSC), which are functioning in the binary positioning notation (PN), is connected, first of all, with increasing of the elements working frequencies and using of the formal synthesis patterns and methods, temporary multi parallel systems and programs [7–10]. At the same time it is theoretically

and practically shown, that non-positional notation in the system of residue classes (SRC) usage allows fundamentally performance increasing and other CSC technical features improvement [11–16]. Besides the above-mentioned material, based on the research results, the fact of the efficient SRC usage in a hyper complex numeric area is important.

The integer rational numbers generalization is integer complex (Gaussian) numbers (CN) [8, 10]. Integer Gaussian numbers form a ring: its sum, difference, and multiplication are also (as the numbers in SRC) integer Gaussian numbers [7, 9].

Based on the SRC features, a set of the patentable components of the integer data handling computer system in the complex area was developed [17–20]. Nowadays, there is increasing the interest of the non-positional notation in SRC between information and telecommunication systems developers, which are implementing processes of forming, transferring and handling signals – physical data carriers, cryptographical data transforming, video data compression, etcetera [21–24].

The aim of the article is a consideration of the algorithm of the residues definition of the integer data in the complex numeric area. In particular, an algorithm of the real residue h defining of the integer complex number $A = a + bi$ by complex modulo $m = p + qi$ is considered.

2 Determining Residues Modulo in a Complex Numerical Domain

In SRC there is the possibility for complex numbers to be presented in the form of their real residues, which means establishing the isomorphism between complex and real numbers residues. It gives a possibility of replacing arithmetical operations for integer Gaussian numbers to the same operations for the real numbers system by real modules, which are equal to norms of chosen complex SRC bases. In this aspect, there is an important task of transforming the number's residue in SRC from a complex number area to the area of a real number. The task of transforming the number's residue in SRC from a complex number area to the area of a real number is being solved by the way of the first fundamental Gauss's law usage. Above-mentioned material leads to the first fundamental Gauss's law. The law establishes isomorphism between complex and real residues.

Law formulation. By the given complex modulo $m = p + qi$, norm N of which equals to $N = p^2 + q^2$ and for which p and q are relative primes, each integer CN $A = a + bi$ by complex modulo m is being compared to one and only one real residue from the set of numbers $\overline{0, \mathrm{N}-1}$, which means, that $A \equiv h(\mathrm{mod}\, m)$.

Proof. It is known from the number theory, that for two relatively primes p and q it is possible to find such two integers u and v, that condition

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

is being met.

Showing the correctness of the following equation:

$$i = u \cdot p - v \cdot q + m \cdot (v + ui)\,. \tag{2}$$

Indeed

$$i = u \cdot q - v \cdot p + (\mathrm{p} + q \cdot i) \cdot (v + u \cdot i) = u \cdot q - v \cdot p + (p \cdot v + p \cdot u \cdot i + q \cdot v \cdot i + q \cdot u \cdot i^2) =$$
$$= u \cdot q - v \cdot p + (p \cdot v + p \cdot u \cdot i + q \cdot v \cdot i - q \cdot u) =$$
$$= u \cdot q - q \cdot u - v \cdot p + p \cdot v + p \cdot u \cdot i + q \cdot v \cdot i = (u \cdot p + v \cdot q) \cdot i$$

Basing on the expression (1) $i = i$. Thus, equation (2) is correct.

If CN $A = a + bi$, then basing on the expression (2) there is:

$$a + bi = a + b \cdot [u \cdot q - v \cdot p + m \cdot (v + ui)] = a + (u \cdot q - v \cdot p) \cdot b + m \cdot (v \cdot b + a \cdot bi). \tag{3}$$

Defining h as the smallest positive real residue of number $a + (u \cdot q - v \cdot p) \cdot b$ by modulo N means that

$$h \equiv [a + (u \cdot q - v \cdot p) \cdot b] \bmod N\,. \tag{4}$$

Expression (4) is represented as an equation

$$a + (u \cdot q - v \cdot p) \cdot b = h + s \cdot N \tag{5}$$

Representing the expression (5) in the following form

$$h + s \cdot N = h + s(p + qi) \cdot (p - qi) = h + m \cdot (p \cdot s - q \cdot si). \tag{6}$$

Then, based on expression (3), the equation is being fulfilled:

$$a + bi = h + m \cdot (p \cdot s - q \cdot si) + m \cdot (v \cdot b + u \cdot bi) = h + m \cdot [p \cdot s + v \cdot b + (u \cdot b - q \cdot s)i],$$

or in the form of congruence relation

$$(a + bi) \equiv h (\bmod m)\,.$$

Thus, it is proved, that the smallest complex residue $x + vi$ of CN $a + bi$ is said to be congruent modulo m with one and only one from the real numbers $0, 1, 2, \ldots, \mathrm{N}-1$.

Using the method of indirect proof defines that this number is unique. Assume, that there are two congruent relations as follows

$$(a + bi) \equiv h_1 (\bmod m); \quad (a + bi) \equiv h_2 (\bmod m).$$

Basing on the feature of congruent relations there is

$$h_1 \equiv h_2 (\bmod m)$$

or

$$(h_1 - h_2) \equiv 0(\mathrm{mod}\, m),$$

which means

$$(h_1 - h_2) = m \cdot (e + f \cdot i). \tag{7}$$

Expression (7) leads to fulfilling of the following equation

$$(m = p + qi),\ (h_1 - h_2) = (p + qi) \cdot (e + fi).$$

Multiplying both parts of the equation by the value $p - qi$ leads to

$$(h_1 - h_2) \cdot (p - qi) = (p + qi) \cdot (p - qi) \cdot (e + fi),\ (h_1 - h_2) \cdot (p - qi) = (p^2 + q^2) \cdot (e + fi),$$

$$(h_1 - h_2) \cdot (p - qi) = N \cdot (e + fi),\ (h_1 - h_2) \cdot p - (h_1 - h_2) \cdot qi = N \cdot e + N \cdot fi.$$

The last expression is equivalent to the next two real equation

$$\begin{cases} (h_1 - h_2) \cdot p = N \cdot e, \\ (h_1 - h_2) \cdot q = -N \cdot f. \end{cases} \tag{8}$$

Because CNs are equal, their real and imaginary parts are equal too. Multiplying the first equation of expression (8) by the value u and the second one by the value v, and then summing the results up leads to the following equation

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

Paying attention to an expression (1) $u \cdot p + v \cdot q = 1$, it follows, that

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

or

$$(h_1 - h_2) \equiv 0(\mathrm{mod}\, N). \tag{9}$$

Since there is a suggestion $h_1, h_2 < N$, congruent relation (9) is possible only in the case $h_1 = h_2$. Therefore, the possibility of existing the two different numbers h_1 and h_2 smaller than N, which would be congruent to $a + bi$ modulo m, is eliminated. There is only one such number h, which is defined by the expression (4) and is represented in the form of congruent relation (10)

$$[a + (u \cdot q - v \cdot p) \cdot b] \equiv h(\mathrm{mod}\, N). \tag{10}$$

In this case, there is usage of the following expression $Z = (a + b \cdot \rho)$, in which expression $\rho = u \cdot q - v \cdot p$, by using which the relation between complex and real resi-

due by modulo $m = p + qi$ is being established, is called as coefficient of isomorphism (CI). Thus, expression (10) is going to be presented in the following form

$$Z \equiv h(\mathrm{mod}\, N). \qquad (11)$$

Data from the expressions (10) and (11) allows to define values of real residues

$$Z_i \equiv h_i(\mathrm{mod}\, N),\ (i = \overline{0, \mathrm{N}-1}),$$

corresponding to the smallest complex residues $x + yi$ by modulo $m = 1 + 2i$. At first, there is defining the value of CI

$$p = u \cdot q - v \cdot p = u \cdot 2 - v \cdot 1.$$

Values of v and u are defined by well-known in the number theory equation $u \cdot p - v \cdot q = 1$, meaning $u \cdot 1 - v \cdot 2 = 1$. By the way of selection $u = -1$, $q = 1$ are being defined.

Thus,

$$p = (-1) \cdot 2 - 1 \cdot 1 = -3$$

or

$$(-3) \bmod 5 = 2\ (N = p^2 + q^2 = 1^2 + 2^2 = 5).$$

Defining source values of the smallest real residues h_i, isomorphic to the smallest complex residues, which are represented in table 2.

For $A = 0 + 0i$.

$$Z_0 = a + bp = 0 + 0 \cdot p = 0.\ h_0 = 0(\mathrm{mod}\, 5).$$

For $A = -1 + i$.

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

For $A = i$.

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

For $A = -1 + 2i$.

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

For $A = 2i$.

$$Z_4 = 0 + 2 \cdot (-3) = -6.\ h_4 = 4(\mathrm{mod}\, 5).$$

The results of the calculations of the smallest real remainders (residues) h_i are in table 1.

Table 1. The results of the calculations of the smallest real residues

The smallest complex residues $x + yi$	CI	Value $Z_i = a + b \cdot p$	Real residues $h_i(Z_i \equiv h_i (\mathrm{mod}\, N)\,; i = \overline{0, N-1}$
0	2	0	0
-1+i	2	-4	1
i	2	-3	2
-1+2i	2	-7	3
2i	2	-6	4

Basing on the results of Gauss's law it is simple to show the following relation between the smallest complex and real residue. Considering, that for two numbers $A_1 = a_1 + b_1 i$ and $A_2 = a_2 + b_2 i$ there are such values of numbers h_1 and h_2, $h_{\pm}$ and $h_{\times}$, that if $A_1 \equiv h_1 (\mathrm{mod}\, m)$ and $A_2 \equiv h_2 (\mathrm{mod}\, m)$, then the relations $A_1 \pm A_2 \equiv h_{\pm} (\mathrm{mod}\, m)$ and $A_1 \cdot A_2 \equiv h_{\times} (\mathrm{mod}\, m)$ are being fulfilled. Then, $h_{\pm} \equiv (h_1 \pm h_2) \bmod N$ and $h_{\times} \equiv (h_1 \cdot h_2) \bmod N$, where $N = p^2 + q^2$.

There are examples of solution of congruent relations in complex area, i.e. examples of defining the smallest real residue h of complex numbers $A = a + bi$ by complex modules $m = p + qi$.

Example 1. There is a congruent relation $(16 + 7i) \equiv h \bmod (5 + 2i)$ to be solved. It means, that it is necessary to find the smallest real residue h of complex number $(16 + 7i)$ by complex modulo $(5 + 2i)$.

Because GCD $(5, 2) = 1$, the condition of the first fundamental Gauss's law is fulfilled, accordingly, there is a complete residue system modulo $N = p^2 + q^2 = 5^2 + 2^2 = 29$. Real residue is being defined by congruent relation (11), i.e.

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

Coefficient of isomorphism ρ is equal to

$$\rho = u \cdot q - v \cdot p = u \cdot 2 - v \cdot 5\,.$$

Values of u and v are defined from the expression (1) by selecting values u, v. Thus, $u = 1$ and $v = -2$. Checking the expression (1) shows, that

$$1 \cdot 5 + (-2) \cdot 2 = 5 - 4 = 1\,.$$

In this case, CI is equal to

$$\rho = 1 \cdot 2 - (-2) \cdot 5 = 2 + 10 = 12$$

and

$$Z = (16 + 7 \cdot \rho) = 16 + 7 \cdot 12 = 100 .$$

Solving the congruent relation $100 \equiv h(\mathrm{mod}\, 29)$ shows, that $h \equiv 13(\mathrm{mod}\, 29)$. Thus, $(16 + 7i) \equiv 13 \mathrm{mod}(5 + 2i)$.

Example 2. There is a congruent relation $(1 + i) \equiv h \,\mathrm{mod}(1 + 2i)$ to be solved. Or it is necessary to find the smallest real residue h of complex number $(1 + i)$ by complex modulo $(1 + 2i)$.

In this case, GCD

$$(p, q) = (1, 2) = 1 , \; N = p^2 + q^2 = 1^2 + 2^2 = 5 .$$

$$A \equiv h(\mathrm{mod}\, m) . \; h \equiv (a + b \cdot \rho) \mathrm{mod}\, N .$$

Value of CI is equal to $\rho = u \cdot q - v \cdot p = u \cdot 2 - v \cdot 1$, values of u and v are defined from the expression (1)

$$u \cdot p + v \cdot q = 1 , \; u \cdot 1 + v \cdot 2 = 1 , \text{ i.e. } u = -1 , \; v = 1 .$$

Thus,

$$\rho = (-1) \cdot 2 - 1 \cdot 1 = -2 - 1 = -3 , \; h = 1 + 1 \cdot 2 = 3 , \; x + yi = 4 + 2i, h = 3 ,$$

i.e.

$$(1 + i) \equiv 3 \mathrm{mod}(1 + 2i) .$$

Examples 3 – 8 of defining the complex and real residues of integer complex number by complex modulo $\mathrm{m} = (1 + 2i)$ are going to be considered. Initial data for the examples solving is represented in table 2.

Table 2. Initial data for the examples solving

Γ	$\Gamma' = 3 \cdot \Gamma(\mathrm{mod}\, 5)$, $(t = 3)$	The smallest complex residues $x + yi$ by complex modulo $\dot{m} = 1 + 2i$ of complex number $\dot{A} = a + bi$	Real residues h by modulo $N = p^2 + q^2 = 5$
0	0	$0 + 0i$	0
1	3	$-1 + i$	1
2	1	i	2
3	4	$-1 + 2i$	3
4	2	$2i$	4

Example 3. To define complex residue $x + yi$ of CN $A = 1 + i$ by complex modulo $\mathrm{m} = (1 + 2i)$, i.e. the aim is to find

$$A \equiv (x + yi) \bmod m\,,\ (a = 1,\ b = 1;\ p = 1,\ q = 2;\ N = 5).$$

Because of the famous equation, there is [8, 9]

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

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

$$x = 3 - 2y\,,\ -1 = -2\cdot(3 - 2y) + y\,,\ -1 = -6 + 4y + y\,,\ 5y = 5\,,\ y = 1.$$
$$x = 3 - 2y = 3 - 2 = 1;\ x = 1.$$

Answer: complex residue $x + yi$ of CN $A = 1 + i$ by complex modulo $\mathrm{m} = (1 + 2i)$ equals to complex number $x + yi = 1 + i$.

Example 4. To define the smallest residue $x + yi$ of CN $A = 1 + i$ by complex modulo , i.e. the aim is to find a value

$$1 + i \equiv (x + yi) \bmod (1 + 2i)\,,\ (a = 1,\ b = 1;\ p = 1,\ q = 2;\ N = 5).$$

Because of the famous equation, there is [7–10]

$$\Gamma = (1\cdot 1 + 1\cdot 2) \bmod 5 = 3;\ \Gamma' = (1\cdot 1 - 1\cdot 2) \bmod 5 = (-1) \bmod 5 = 4.$$
$$x + yi = \frac{3\cdot 1 - 4\cdot 2}{5} + \frac{4\cdot 1 + 3\cdot 2}{5} i = -\frac{5}{5} + \frac{10}{5} i = -1 + 2i\,.$$

Thus, the smallest residue $x + yi$ of CN $A = 1 + i$ by complex modulo $\mathrm{m} = (1 + 2i)$ equals to value $x + yi = -1 + 2i$. This solution can be represented in the form

$$(1 + i) \equiv (-1 + 2i) \bmod (1 + 2i)\,.$$

Example 5. To solve congruent relation $A \equiv h \bmod m$ of form

$$(1 + i) \equiv h \bmod (1 + 2i)\,,\ (a = 1,\ b = 1;\ p = 1,\ q = 2;\ N = 5),$$

expressions (1), (10), (11).

$$u\cdot p + v\cdot q = 1,\ u = -1,\ u\cdot 1 + v\cdot 2 = 1.\ v = 1.\ \rho = u\cdot q - v\cdot p\,.$$
$$Z = a + b\cdot\rho,\ Z \equiv h \bmod N.\ \ \rho = (-1)\cdot 2 - 1\cdot 1 = -2 - 1 = -3\,.$$

$$Z = 1 + 1\cdot(-3) = -2.$$
$$\mathrm{h} \equiv (-2) \bmod 5 = 3.$$

Thus, real residue h of CN $A = 1 + i$ by complex modulo $\mathrm{m} = (1 + 2i)$ equals to value $h = 3$.

Solution check. Achieved results should be checked. In example 4 there is the smallest complex residue $(-1+2i)$, and in example 5 there is real residue $h=3$. According to data from table 2 $(-1+2i)$ □ 3. Which is what it had to be shown.

Example 6. To define complex residue $x+yi$ of CN $A=3+4i$ by complex modulo $\mathrm{m}=(1+2i)$.

$$N=p^2+q^2=1^2+2^2=5.$$

Using the famous equation [8, 9], there is system of congruent relations in 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

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

Basing on the system of congruent relations there is system containing two linear equation

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

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

$$x=11-2y,\ -2\cdot(11-2\cdot y)+y=3,\ -22+4y+y=3,$$

$$5y=25,\ y=5.\ x=11-2y=11-10=1.$$

Thus, complex residue $x+yi$ of CN $A=3+4i$ by complex modulo $\mathrm{m}=(1+2i)$ equals to value

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

Example 7. To define the smallest complex residue $x+yi$ of CN $A=3+4i$ by complex modulo $\mathrm{m}=(1+2i)$. $N=5$.

According to famous expressions, the smallest complex residue equals to value

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

Firstly, values Γ and Γ' need to be defined

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

$$\Gamma' = (b \cdot p - a \cdot q) \bmod N = (4 \cdot 1 - 3 \cdot 2) \bmod 5 = (-2) \bmod 5 = 3$$

In this case, there is

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

Thus, the smallest complex residue $x + yi$ of CN $A = 3 + 4i$ by complex modulo $\mathrm{m} = (1 + 2i)$ equals to value $-1 + i$.

Example 8. To define real residue h of CN $A = 3 + 4i$ by complex modulo $\mathrm{m} = (1 + 2i)$. $N = 5$. The task can be formulated in another way. To solve a congruent relation $(3 + 4i) \equiv h \bmod (1 + 2i)$.

According to expression (11), there is $(a + b\rho) \equiv h (\bmod N)$, where CI ρ is equal to $\rho = u \cdot q - v \cdot p$. Based on expression (1), values u and v are defined

$$u \cdot p + v \cdot q = 1 \text{ or } u \cdot 1 + v \cdot 2 = 1 .$$

So, the condition (1) will be fulfilled if $u = -1$ and $v = 1$, i.e. $(-1) \cdot 1 + 1 \cdot 2 = 1$.

Basing on calculations

$$\rho = u \cdot q - v \cdot p = (-1) \cdot 2 - 1 \cdot 1 = -3 . \; \mathrm{Z} = (a + b \cdot \rho) = 3 + 4 \cdot (-3) = -9 .$$

There is $(a + b\rho) \equiv h (\bmod N)$ or $(-9) \equiv 1 (\bmod 5)$, i.e. $h = 1$.

Thus, there is the solution of a congruent relation $(3 + 4i) \equiv 1 \bmod (1 + 2i)$.

Solution check. Achieved results should be checked. In example 7 there is the smallest complex residue $(-1 + i)$ and in example 8 there is real residue $h = 1$. According to data from table 2 $(-1 + i) \; 1$. Which is what it had to be shown.

3 Conclusions

In the article algorithms of defining the residues by modulo in complex numeric area were considered. The main attention was paid to the algorithm of defining real residue of integer complex number by complex modulo, based on usage of first fundamental Gauss's law. The examples of defining residues of integer data in the complex numeric area were provided. The results, achieved in the article, should be considered while implementing tasks and algorithms in SRC for the complex numeric area. Usage of represented methods contributes to performance increasing of SRC using for the quick implementation of integer operations in the complex numeric area. These computing techniques can be useful in various applications, for example, when processing data in complex computer systems, implementing reliable and fault-tolerant computers, and also for implementing cryptographic transformations [21, 25, 26].

The results can be used to build computer devices and components of fault-tolerant critical information systems. Increasing the speed of computing operations due to the

use of non-positional residue number systems leads to a decrease in the risks of unintentional failures or denials of service of computer systems.

References

1. Alford, R.S.: Computer Systems Engineering Management. CRC Press (2018). https://doi.org/10.1201/9781351070829.
2. Wright, S.A.: Performance Modeling, Benchmarking and Simulation of High Performance Computing Systems. Future Generation Computer Systems. 92, 900–902 (2019). https://doi.org/10.1016/j.future.2018.11.020.
3. Yadin, A.: Computer Systems Architecture. Chapman and Hall/CRC (2016). https://doi.org/10.1201/9781315373287.
4. Hodson, R.F.: Real-Time Expert Systems Computer Architecture. CRC Press (2018). https://doi.org/10.1201/9781351076203.
5. Koren, I.: THE RESIDUE NUMBER SYSTEM, https://www.taylorfrancis.com/, last accessed 2020/08/16. https://doi.org/10.1201/9781315275567-18.
6. Nithun Chand O, Mathivanan, S.: A survey on resource inflated Denial of Service attack defense mechanisms. In: 2016 Online International Conference on Green Engineering and Technologies (IC-GET). pp. 1–4 (2016). https://doi.org/10.1109/GET.2016.7916821.
7. Kantor, I.L., Solodovnikov, A.S.: Hypercomplex Numbers: An Elementary Introduction to Algebras. Springer, New York (1989).
8. Olariu, S.: Complex Numbers in n Dimensions. arXiv:math/0011044. (2000).
9. Schutte, H.-D., Wenzel, J.: Hypercomplex numbers in digital signal processing. In: IEEE International Symposium on Circuits and Systems. pp. 1557–1560 vol.2 (1990). https://doi.org/10.1109/ISCAS.1990.112431.
10. Waerden, B.L.V.D.: A History of Algebra: From Al-Khwarizmi to Emmy Noether. Springer Verlag, Berlin ; New York (1985).
11. Barsi, F., Maestrini, P.: Error Correcting Properties of Redundant Residue Number Systems. IEEE Transactions on Computers. C–22, 307–315 (1973). https://doi.org/10.1109/T-C.1973.223711.
12. Fan, C., Ge, G.: A Unified Approach to Whiteman's and Ding-Helleseth's Generalized Cyclotomy Over Residue Class Rings. IEEE Transactions on Information Theory. 60, 1326–1336 (2014). https://doi.org/10.1109/TIT.2013.2290694.
13. Harman, G., Shparlinski, I.E.: Products of Small Integers in Residue Classes and Additive Properties of Fermat Quotients. Int Math Res Notices. 2016, 1424–1446 (2016). https://doi.org/10.1093/imrn/rnv182.
14. Huang, T.-C.: Self-Checking Residue Number System for Low-Power Reliable Neural Network. In: 2019 IEEE 28th Asian Test Symposium (ATS). pp. 37–375 (2019). https://doi.org/10.1109/ATS47505.2019.000-3.
15. Kocherov, Y.N., Samoylenko, D.V., Koldaev, A.I.: Development of an Antinoise Method of Data Sharing Based on the Application of a Two-Step-Up System of Residual Classes. In: 2018 International Multi-Conference on Industrial Engineering and Modern Technologies (FarEastCon). pp. 1–5 (2018). https://doi.org/10.1109/FarEastCon.2018.8602764.
16. Krasnobayev, V., Kuznetsov, A., Koshman, S., Moroz, S.: Improved Method of Determining the Alternative Set of Numbers in Residue Number System. In: Chertov, O., Mylovanov, T., Kondratenko, Y., Kacprzyk, J., Kreinovich, V., and Stefanuk, V. (eds.) Recent Developments in Data Science and Intelligent Analysis of Information. pp. 319–328.

Springer International Publishing, Cham (2019). https://doi.org/10.1007/978-3-319-97885-7_31.
17. Amerbaev, V.M., Soloviev, R.A., Telpukhov, D.V.: Hardware Implementation of Fir Filter Based on Number-theoretic Fast Fourier Transform in Residue Number System. Open Engineering Sciences Journal. 1, (2014). https://doi.org/10.2174/2352628901401010001.
18. Popov, D.I., Gapochkin, A.V.: Development of Algorithm for Control and Correction of Errors of Digital Signals, Represented in System of Residual Classes. In: 2018 International Russian Automation Conference (RusAutoCon). pp. 1–3 (2018). https://doi.org/10.1109/RUSAUTOCON.2018.8501826.
19. Timarchi, S., Navi, K.: Efficient Class of Redundant Residue Number System. In: 2007 IEEE International Symposium on Intelligent Signal Processing. pp. 1–6 (2007). https://doi.org/10.1109/WISP.2007.4447506.
20. Zhang, Y.: An FPGA implementation of redundant residue number system for low-cost fast speed fault-tolerant computations, https://dr.ntu.edu.sg//handle/10356/89387, (2018). https://doi.org/10.32657/10220/47113.
21. Gayoso, C.A., Arnone, L., González, C., Moreira, J.C.: A general construction method for Pseudo-Random Number Generators based on the Residue Number System. In: 2019 XVIII Workshop on Information Processing and Control (RPIC). pp. 25–30 (2019). https://doi.org/10.1109/RPIC.2019.8882147.
22. Kaplun, D.I., Chervyakov, N.I., Lyakhov, P.A., Ionisyan, A.S., Valueva, M.V., Gulvanskiy, V.V., Rangababu, P.: Hardware Implementation of Video Processing Device using Residue Number System. In: 2019 42nd International Conference on Telecommunications and Signal Processing (TSP). pp. 701–704 (2019). https://doi.org/10.1109/TSP.2019.8768827.
23. Karpinski, M., Ivasiev, S., Yakymenko, I., Kasianchuk, M., Gancarczyk, T.: Advanced method of factorization of multi-bit numbers based on Fermat's theorem in the system of residual classes. In: 2016 16th International Conference on Control, Automation and Systems (ICCAS). pp. 1484–1486 (2016). https://doi.org/10.1109/ICCAS.2016.7832500.
24. Kasianchuk, M., Yakymenko, I., Pazdriy, I., Melnyk, A., Ivasiev, S.: Rabin's modified method of encryption using various forms of system of residual classes. In: 2017 14th International Conference The Experience of Designing and Application of CAD Systems in Microelectronics (CADSM). pp. 222–224 (2017). https://doi.org/10.1109/CADSM.2017.7916120.
25. Tao, K., Peng, L., Liang, K., Zhuo, B.: Irregular repeat accumulate low-density parity-check codes based on residue class pair. In: 2017 IEEE 9th International Conference on Communication Software and Networks (ICCSN). pp. 127–131 (2017). https://doi.org/10.1109/ICCSN.2017.8230092.
26. Vassalos, E., Bakalis, D.: Residue-to-Binary Converter for the New RNS Moduli Set ${2^2n-2, \ 2^n-1, \ 2^n+1}$. In: 2019 Panhellenic Conference on Electronics Telecommunications (PACET). pp. 1–4 (2019). https://doi.org/10.1109/PACET48583.2019.8956249.