Determining the rank of a number in the residue number system

Mikhail Babenko[1,2,3††], **Nikolay Kucherov**[1,2†], **Andrei Tchernykh**[3,4,5†††], **Viktor Kuchukov**[1,2‡‡], **Elena Golimblevskaia**[1,2‡], **Ekaterina Kuchukova**[1‡†], **and Irina Vashchenko**[1†‡]

[1] North-Caucasus Center for Mathematical Research, North-Caucasus Federal University,1, Pushkin Street, 355017, Stavropol, Russia
[2] Sirius University of Science and Technology, 1 Olympic Ave, 354340, Sochi, Russia
[3] Institute for System Programming of the Russian Academy of Sciences, 109004 Moscow, Russia
[4] CICESE Research Center, carr. Tijuana-Ensenada 3918, 22860, Ensenada, BC, Mexico
[5] South Ural State University, Prospekt Lenina 76, 454080, Chelyabinsk, Russia

E-mail: [††]mgbabenko@ncfu.ru, [†]nkucherov@ncfu.ru, [†††]chernykh@cicese.mx, [‡‡]vkuchukov@ncfu.ru, [‡]elena.golimblevskaya@gmail.ru, [‡†]ekuchukova@ncfu.ru, [†‡]irishechka.26@mail.ru

Abstract. In this article, the formulation and proof of the theorem on the difference in the ranks of the numbers represented in the Residue Number System is carried out. A method is proposed that allows to reduce the amount of necessary calculations and increases the speed of calculating the rank of a number relative to the method for calculating the rank of a number based on the approximate method. To find the rank of a number in the method for calculating the rank of a number based on the approximate method, it is necessary to calculate n operations with numbers exceeding the modulus value; in the proposed method, it is necessary to calculate $\frac{n\cdot(n-1)}{2}$ operations not exceeding the value of the module.

1. Introduction

The current state of development of infocommunication technologies in the field of data processing and transmission is characterized by the intensive introduction of new principles and approaches to information processing. One of the ways to increase the speed of computing facilities led to the creation of computing systems with a parallel structure. At the same time, it became necessary and expedient to use codes with a parallel structure. These codes include non-weigted codes - codes based on modular arithmetic, that is, codes in which numbers are represented in the Residue Number System (RNS) [1].

The Residue Number System is a number system based on the representation of a number as a set of residues after division by a set of coprime numbers, called the basis of the system. The main feature of the RNS is the non-weighted representation of a number, which ensures the independence of numeric digits and the possibility of parallel processing of numbers [2, 3].

Let the RNS be given by a set of coprime bases $p_1, p_2, \ldots, p_n$. Then the number X can be represented as $X = (x_1, x_2, \ldots, x_n)$, where $x_i = |X|_{p_i}$ for all $i = 1, 2, \ldots, n$ [4]. The numbers x_i will be called the digits of the number X in this RNS. According to the Chinese remainder theorem, the RNS allows a unique representation of any number from the interval $[0, P)$, where $P = p_1 \cdot p_2 \cdot \ldots \cdot p_n$ – is a dynamic range of number representation [5].

The fundamental proposition underlying modular arithmetic is the Chinese Remainder Theorem:

Theorem 1: Let $p_1, p_2, \ldots, p_k$ be some natural coprime numbers and $P = p_1 \cdot p_2 \cdot \ldots \cdot p_k$. Any number X, such that $0 \leq X \leq P$, can be unambiguously represented as a sequence $(x_1, x_2, \ldots, x_n)$, where $x_i = X \bmod p_i$, wherein

$$X = \left| \sum_{i=1}^{n} \left| P_i^{-1} \right|_{p_i} P_i x_i \right|_P , \tag{1}$$

where $P_i = \frac{P}{p_i}$. The numbers $B_i = \left| P_i^{-1} \right|_{p_i} P_i$ is customary to call orthogonal RNS bases since their representation in RNS corresponds to the number 1 in position i and 0 in positions $j \neq i$.

The advantage of the modular representation of a number is that the operations of addition, subtraction and multiplication are very simple and parallel. [6]. Let the numbers A and B be given by the formula (1):

$$A \equiv \alpha_1 \left(\mathrm{mod} p_1\right), \; A \equiv \alpha_2 \left(\mathrm{mod} p_2\right), \; \ldots \; , A \equiv \alpha_n \left(\mathrm{mod} p_n\right)$$
$$B \equiv \beta_1 \left(\mathrm{mod} p_1\right), \; B \equiv \beta_2 \left(\mathrm{mod} p_2\right), \; \ldots \; , B \equiv \beta_n \left(\mathrm{mod} p_n\right)$$

Then the operations of addition, multiplication and subtraction can be performed according to the formulas

$$\begin{gathered} A \pm B = (\alpha_1, \alpha_2, \ldots, \alpha_n) \pm (\beta_1, \beta_2, \ldots, \beta_n) = \\ = \left(\left((\alpha_1 \pm \beta_1) \left(\mathrm{mod} p_1\right)\right), \left((\alpha_2 \pm \beta_2) \left(\mathrm{mod} p_2\right)\right), \ldots, \left((\alpha_n \pm \beta_n) \left(\mathrm{mod} p_n\right)\right)\right) \end{gathered} \tag{2}$$

$$\begin{gathered} A \cdot B = (\alpha_1, \alpha_2, \ldots, \alpha_n) \cdot (\beta_1, \beta_2, \ldots, \beta_n) = \\ = \left(\left((\alpha_1 \cdot \beta_1) \left(\mathrm{mod} p_1\right)\right), \left((\alpha_2 \cdot \beta_2) \left(\mathrm{mod} p_2\right)\right), \ldots, \left((\alpha_n \cdot \beta_n) \left(\mathrm{mod} p_n\right)\right)\right) \end{gathered} \tag{3}$$

The operations of addition, subtraction and multiplication in the RNS are performed independently and in parallel, therefore, based on this number system, it is possible to create a completely homomorphic coding system. Coding systems of this type are required when organizing cloud computing, since they allow protecting data when performing mathematical operations remotely [7].

The range of numbers on which modular arithmetic operations can be performed is the set of numbers P, each of which does not exceed the product of the selected moduli $\prod_{i=1}^{n} p_i$ [8, 9].

2. Algorithm for calculating the rank of a number based on the approximate method

In order to simplify the process of converting numbers from the modular representation to the positional representation of numbers, we will consider an approximate method that allows to go from the expensive operation of taking the remainder in a large modulus to taking the fractional part of a number by replacing the exact value with an approximate one, and completely correctly implement the main classes of decision-making procedures: checking the equality (inequality) of two values; comparison of two values (more, less) that provide a solution to the main range of problems arising from the hardware or software implementation of real processes [10].

The essence of the approximate method is to use the relative value of the original number to the full range of CRT, which connects the positional number X with its representation in the residues $(x_1, x_2, \ldots, x_n)$ by the following expression [6]:

$$X = \left| \sum_{i=1}^{n} \frac{P}{p_i} \left| P_i^{-1} \right|_{p_i} x_i \right|_P , \tag{4}$$

where x_i are the smallest nonnegative residues of a number divided by moduli of the RNS $p_1, p_2, \ldots, p_n$, $P = \prod_{i=1}^{n} p_i$, $\left| P_i^{-1} \right|_{p_i}$ is multiplicative inversion P_i relative to p_i and for all $i = \overline{1,n}$ the equality $P = \frac{P}{p_i}$.

If the formula (4) is divided by the RNS range P, then we get an approximate value:

$$\frac{X}{P} = \left| \sum_{i=1}^{n} \frac{\left| P_i^{-1} \right|_{p_i}}{p_i} x_i \right|_1 , \tag{5}$$

where for all $i = \overline{1,n}$ the equation $\frac{\left| P_i^{-1} \right|_{p_i}}{p_i}$ are the constants of the selected system, and x_i are digits of the number presented in the RNS, while the value of each sum is in the interval [0, 1). The final result of the sum is determined after summing and discarding the integer part of the number, keeping the fractional part of the sum. The fractional part can also be written as $X \bmod 1$, because $X = \lfloor X \rfloor + X \bmod 1$. The number of digits of the fractional part of a number is determined by the maximum possible difference between adjacent numbers. In the work [11] it is shown that with a computational accuracy of N bits, the recovery of numbers by the formula (5 is correct, where $N = \lceil \log_2 (\rho P) \rceil$ and $\rho = -n + \sum_{i=1}^{n} p_i$.

The hardware implementation of the arithmetic operations of multiplication and addition of real numbers requires on average 3.5 times more hardware resources than performing the same operations with integers of the same size, so we make the transition from real numbers to integers, and the formula (5) takes view:

$$X = \left\lfloor \frac{\left| \sum_{i=1}^{n} \overline{k_i} x_i \right|_{2^N} P}{2^N} \right\rfloor , \tag{6}$$

where $\overline{k_i} = \left\lceil \frac{\left| P_i^{-1} \right|_{p_i} 2^N}{p_i} \right\rceil$.

Then the operation of taking the fractional part in the formula (5) will be replaced by the operation of taking the least significant N bits of the number in the formula (6), and the operation of taking the residue from division by the large modulus of the RNS range P will be replaced with multiplication and shift to the right by N bits of the number.

Let us investigate the question of the size N.

Theorem 2: [12] The formula (6) is true if N is chosen equal to:

$$N = \left\lceil \log_2 \left(\left(-2n + \sum_{i=1}^{n} p_i \right) P + SQ \right) \right\rceil , \tag{7}$$

where $SQ = \sum_{i=1}^{n} P_i$.

Proof.

Let $\overline{k_i} = \left\lfloor \frac{\left|P_i^{-1}\right|_{p_i} 2^N}{p_i} \right\rfloor = \frac{\left|P_i^{-1}\right|_{p_i} 2^N}{p_i} + R_i$, where $0 \le R_i < \frac{m_i - 1}{m_1}$.

Let's calculate the value $\sum\limits_{i=1}^{n} \overline{k_i} x_i$:

$$\begin{gathered} \sum_{i=21}^{n} \overline{k_i} x_i \sum_{i=1}^{n-1} \left(\frac{\left|P_i^{-1}\right|_{p_i} 2^N}{p_i} + R_i \right) x_i = \\ = \sum_{i=1}^{n} \frac{\left|P_i^{-1}\right|_{p_i} 2^N}{p_i} x_i + \sum_{i=1}^{n} R_i x_i = 2^N \sum_{i=1}^{n} \frac{\left|P_i^{-1}\right|_{p_i} 2^N}{p_i} x_i + \sum_{i=1}^{n} R_i x_i. \end{gathered} \tag{8}$$

The value $\left| \sum\limits_{i=1}^{n} \overline{k_i} x_i \right|_{2^N}$ is equal to:

$$\left| \sum_{i=1}^{n} \overline{k_i} x_i \right|_{2^N} = \sum_{i=1}^{n} \overline{k_i} x_i - \left\lfloor \sum_{i=1}^{n} \frac{\overline{k_i} x_i}{2^N} \right\rfloor \cdot 2^N \tag{9}$$

Substituting (8) in (9) we get:

$$\left| \sum_{i=1}^{n} \overline{k_i} x_i \right|_{2^N} = 2^N \sum_{i=1}^{n} \frac{\left|P_i^{-1}\right|_{p_i}}{p_i} x_i + \sum_{i=1}^{n} R_i x_i - \left\lfloor \sum_{i=1}^{n} \frac{\left|P_i^{-1}\right|_{p_i}}{p_i} x_i + \frac{\sum\limits_{i=1}^{n} R_i x_i}{2^N} \right\rfloor 2^N \tag{10}$$

Substituting the formula (10) to the right side of the formula (6), we get:

$$\left\lfloor \frac{\left| \sum\limits_{i=1}^{n} \overline{k_i} x_i \right|_{2^n} P}{2^N} \right\rfloor = \left\lfloor P \sum_{i=1}^{n} \frac{\left|P_i^{-1}\right|_{p_i}}{p_i} x_i + \frac{P}{2^N} \sum_{i=1}^{n} R_i x_i \right\rfloor - \left\lfloor \sum_{i=1}^{n} \frac{\left|P_i^{-1}\right|_{p_i}}{p_i} x_i + \frac{\sum\limits_{i=1}^{n} R_i x_i}{2^N} \right\rfloor P \tag{11}$$

Taking into account that by the Chinese remainder theorem:

$$X = P \sum_{i=1}^{n} \frac{\left|P_i^{-1}\right|_{p_i}}{p_i} x_i - \left\lfloor \sum_{i=1}^{n} \frac{\left|P_i^{-1}\right|_{p_i}}{p_i} x_i \right\rfloor P \tag{12}$$

The formula (6) will be equivalent to the formula (12), if two conditions are met:

(i) $\left\lfloor P \sum\limits_{i=1}^{n} \frac{\left|P_i^{-1}\right|_{p_i}}{p_i} x_i + \frac{P}{2^N} \sum\limits_{i=1}^{n} R_i x_i \right\rfloor = P \sum\limits_{i=1}^{n} \frac{\left|P_i^{-1}\right|_{p_i}}{p_i} x_i,$

is equivalent to: $\frac{P}{2^N} \sum\limits_{i=1}^{n} R_i x_i < 1.$

(ii) $\left\lfloor \sum\limits_{i=1}^{n} \frac{\left|P_i^{-1}\right|_{p_i}}{p_i} x_i + \frac{\sum\limits_{i=1}^{n} R_i x_i}{2^N} \right\rfloor = \left\lfloor \sum\limits_{i=1}^{n} \frac{\left|P_i^{-1}\right|_{p_i}}{p_i} x_i \right\rfloor$, is equivalent to $\frac{\sum\limits_{i=1}^{n} R_i x_i}{2^N} < \frac{1}{P}$.

Conditions 1 and 2 are equivalent, therefore, it is necessary and sufficient for the following condition to be satisfied:

$$\frac{\sum\limits_{i=1}^{n} R_i x_i}{2^N} < \frac{1}{P}. \tag{13}$$

It follows from the inequality (13) that a necessary and sufficient condition is:

$$2^N > P\sum_{i=1}^{n} R_i x_i \tag{14}$$

Estimating the right side of the inequality (14), we obtain:

$$\begin{gathered} P\sum_{i=1}^{n} R_i x_i < P\sum_{i=1}^{n} \tfrac{m_i-1}{m_i}(m_i-1) = P\sum_{i=1}^{n}(m_1-1) - P\sum_{i=1}^{n}\left(1-\tfrac{1}{m_i}\right) = \\ = -nP + P\sum_{i=1}^{n} m_i - nP + SQ = \left(-2n + \sum_{i=1}^{n} m_i\right)P + SQ. \end{gathered} \tag{15}$$

It follows from the formula (15) and inequality (14), that if we choose

$$N = \left\lceil \log_2\left(\left(-2n + \sum_{i=1}^{n} p_i\right)P + SQ\right)\right\rceil,$$

then the formula (6) is equal.

The theorem is proved.

We show that $N = \left\lceil \log_2\left(\left(-2n + \sum\limits_{i=1}^{n} p_i\right)P + SQ\right)\right\rceil \le \lceil \log_2(\rho P)\rceil$.

To do this, let's find the difference

$$\rho P - \left(\left(-2n + \sum_{i=1}^{n} p_i\right)P + SQ\right) = nP - SQ = \sum_{i=1}^{n}(P - P_i) > 0. \tag{16}$$

From the formula (16) it follows that the obtained estimate of the value of N is more accurate than the estimate from the work [11].

According to the Chinese Remainder Theorem, the value of X can be calculated by the formula (4) or:

$$X = \sum_{i=1}^{n} P_i \left|P_i^{-1}\right|_{p_i} x_i - \underbrace{\left\lfloor \sum_{i=1}^{n} \frac{\left|P_i^{-1}\right|_{p_i}}{p_i} x_i \right\rfloor}_{r_X} P. \tag{17}$$

where r_X is the rank of a number, a positive integer showing how many times the range of the system was exceeded in transition from the representation of a number in the Residue Number System to its representation in a system of orthogonal bases [11].

From the formula (17) it follows that calculating r_X requires either using an expensive integer division or working with real numbers with precision N to correctly determine the rank of a number.

To effectively implement the algorithm for calculating the rank of a number, we use an approach based on the simultaneous use of an approximate method and a modular adder, which will significantly reduce the accuracy of calculations:

$$r = \left\lfloor \sum_{i=1}^{n} \overline{\overline{k}}_i x_i / 2^{N_1} \right\rfloor, \tag{18}$$

where $\overline{\overline{k}}_i = \left\lceil \frac{\left|P_i^{-1}\right|_{p_i} 2^{N_1}}{p_i} \right\rceil$.

Let us examine the question of the relationship between the values N_1, r and r_X.

Theorem 3:

(i) If $N_1 = N$, then $r_X = r$.

(ii) If $N_1 = \lceil \log_2 \rho \rceil$, then $r_X = r$ or $r_X = r - 1$, where $\rho = \sum\limits_{i=1}^{n} p_i - n$.

Proof

Let $\overline{\overline{k_i}} = \left\lceil \dfrac{\left|P_i^{-1}\right|_{p_i} 2^{N_1}}{p_i} \right\rceil = \dfrac{\left|P_i^{-1}\right|_{p_i} 2^{N_1}}{p_i} + R'$ where $0 \le R'_i \le \frac{m_i - 1}{m_i}$.

We calculate the value $\sum\limits_{i=1}^{n} \overline{\overline{k_i}} x_i$:

$$\sum_{i=1}^{n} \overline{\overline{k_i}} x_i = \sum_{i=1}^{n} \left(\frac{\left|P_i^{-1}\right|_{p_i} 2^{N_1}}{p_i} + R' \right) x_i = \sum_{i=1}^{n} \frac{\left|P_i^{-1}\right|_{p_i} 2^{N_1}}{p_i} x_i + \sum_{i=1}^{n} R'_i x_i = \\ = 2^{N_1} \sum_{i=1}^{n} \frac{\left|P_i^{-1}\right|_{p_i}}{p_i} x_i + \sum_{i=1}^{n} R'_i x_i \tag{19}$$

Substituting the formula (18) in (19), we get

$$r = \left\lfloor \frac{\sum\limits_{i=1}^{n} \overline{\overline{k_i}} x_i}{2^{N_1}} \right\rfloor = \left\lfloor \sum_{i=1}^{n} \frac{\left|P_i^{-1}\right|_{p_i}}{p_i} x_i + \frac{\sum\limits_{i=1}^{n} R'_i x_i}{2^{N_1}} \right\rfloor \tag{20}$$

From formulas (17) and (20) it follows, that $r = r_x$ for $\frac{\sum\limits_{i=1}^{n} R'_i x_i}{2^{N_1}} < \frac{1}{P}$. According to the theorem 3, this inequality holds for $N_1 = N$.

If $r_x = r$ or $r_x = r - 1$, than from the formula (20) it follows that a sufficient condition is $\frac{\sum\limits_{i=1}^{n} R'_i x_i}{2^{N_1}} < 1$, therefore, $\sum\limits_{i=1}^{n} R'_i x_i < 2^{N_1}$.

Since $\sum\limits_{i=1}^{n} R'_i x_i < \sum\limits_{i=1}^{n} (p_i - 1) = -n + \sum\limits_{i=1}^{n} p_i = \rho$, then $N_1 = \lceil \log_2 \rho \rceil$ will be sufficient to satisfy the second condition of the theorem 3.

Example 1. Let the RNS moduli be $p_1 = 17$, $p_2 = 19$, $p_3 = 23$, $p_4 = 25$. RNS range is $P = 17 \cdot 19 \cdot 23 \cdot 25 = 185\,725$.

We calculate P_i: $P_1 = \frac{P}{p_1} = 10\,925$, $P_2 = \frac{P}{p_2} = 9\,775$, $P_3 = \frac{P}{p_3} = 8\,075$, $P_4 = \frac{P}{p_4} = 7\,429$.

We find the value SQ : $SQ = 10\,925 + 9\,775 + 8\,075 + 7\,429$.

We calculate the parameters of the approximate method:

$$N = \lceil \log_2 14151304 \rceil = 24,\ N_1 = \lceil \log_2 80 \rceil = 7$$
$$k_1 = \left|P_1^{-1}\right|_{p_1} P_1 = 152950,\ k_2 = \left|P_2^{-1}\right|_{p_2} P_2 = 166175$$
$$k_3 = \left|P_3^{-1}\right|_{p_3} P_3 = 96900,\ k_4 = \left|P_4^{-1}\right|_{p_4} P_4 = 141151$$
$$\overline{k_1} = \left\lceil \frac{\left|P_1^{-1}\right|_{p_1} 2^N}{p_1} \right\rceil = 13816531,\ \overline{k_2} = \left\lceil \frac{\left|P_2^{-1}\right|_{p_2} 2^N}{p_2} \right\rceil = 15011194$$
$$\overline{k_3} = \left\lceil \frac{\left|P_3^{-1}\right|_{p_3} 2^N}{p_3} \right\rceil = 8753331,\ \overline{k_4} = \left\lceil \frac{\left|P_4^{-1}\right|_{p_4} 2^N}{p_4} \right\rceil = 12750685$$
$$\overline{\overline{k_1}} = \left\lceil \frac{\left|P_1^{-1}\right|_{p_1} 2^{N_1}}{p_1} \right\rceil = 106,\ \overline{\overline{k_2}} = \left\lceil \frac{\left|P_2^{-1}\right|_{p_2} 2^{N_1}}{p_2} \right\rceil = 115$$
$$\overline{\overline{k_3}} = \left\lceil \frac{\left|P_3^{-1}\right|_{p_3} 2^{N_1}}{p_3} \right\rceil = 67,\ \overline{\overline{k_4}} = \left\lceil \frac{\left|P_4^{-1}\right|_{p_4} 2^{N_1}}{p_4} \right\rceil = 98$$

Let the numbers $X \to \{16, 18, 22, 24\}$ and $Y \to \{1, 2, 3, 4\}$ be given in the RNS.

1. We calculate the values X and Y using the approximate method.

$$16 \cdot 13816531 + 18 \cdot 15011194 + 22 \cdot 8753331 + 24 \cdot 2750685 = 749855710.$$
$$|749855710|_{2^{24}} = 16777182.$$
$$X = \left\lfloor \frac{16777182 \cdot 185725}{2^{24}} \right\rfloor = 185724.$$
$$1 \cdot 13816531 + 2 \cdot 15011194 + 3 \cdot 8753331 + 4 \cdot 2750685 = 81101652.$$
$$|81101652|_{2^{24}} = 3661140.$$
$$Y = \left\lfloor \frac{3661140 \cdot 185725}{2^{24}} \right\rfloor = 40529.$$

2. We calculate the values X and Y based on theorem 1 and the rank of the function by the formula (18).

$$\sum_{i=1}^{n} k_i x_i = 16 \cdot 152950 + 18 \cdot 166175 + 22 \cdot 96900 + 24 \cdot 141151 = 10957774.$$
$$r_X = \left\lfloor \frac{10957774}{185725} \right\rfloor = 58$$
$$X = 10957774 - 58 \cdot 185725 = 185724$$
$$\sum_{i=1}^{n} k_i y_i = 1 \cdot 152950 + 2 \cdot 166175 + 3 \cdot 96900 + 4 \cdot 141151 = 1340604.$$
$$r_Y = \left\lfloor \frac{1340604}{185725} \right\rfloor = 7$$
$$Y = 1340604 - 7 \cdot 185725 = 40529$$

3. We calculate the values X and Y using the 1 theorem and the rank of the number calculated using the approximate method with accuracy N.

$$\sum_{i=1}^{n} \overline{\overline{k_i}} x_i = 16 \cdot 13816531 + 18 \cdot 15011194 + 22 \cdot 8753331 + 24 \cdot 12750685 = 989855710$$
$$r = \left\lfloor \frac{989855710}{2^{24}} \right\rfloor = 58 = r_X,$$
$$X = 10957774 - 58 \cdot 185725 = 185724$$
$$\sum_{i=1}^{n} \overline{\overline{k_i}} y_i = 1 \cdot 13816531 + 2 \cdot 15011194 + 3 \cdot 8753331 + 4 \cdot 12750685 = 121101652$$
$$r = \left\lfloor \frac{121101652}{2^{24}} \right\rfloor = 7 = r_Y,$$
$$Y = 1340604 - 7 \cdot 185725 = 40529$$

4. We calculate the values X and Y using the CRT and the rank of the number calculated using the approximate method with an accuracy N_1.

$$\sum_{i=1}^{n} \overline{\overline{k_i}} x_i = 16 \cdot 106 + 18 \cdot 115 + 22 \cdot 67 + 24 \cdot 98 = 7592$$
$$r = \left\lfloor \frac{7592}{2^7} \right\rfloor = 59,$$
$$X = 10957774 - 59 \cdot 185725 = -1, \text{ as } X < 0 \text{ then } X = -1 + 185725 = 185724$$
$$\sum_{i=1}^{n} \overline{\overline{k_i}} y_i = 1 \cdot 106 + 2 \cdot 115 + 3 \cdot 67 + 4 \cdot 98 = 929$$
$$r = \left\lfloor \frac{929}{2^7} \right\rfloor = 7$$
$$X = 1340604 - 7 \cdot 185725 = 40529, \text{ as } X < 0 \text{ then } X = -1 + 185725 = 185724.$$

Since $Y \geq 0$, then the result remains unchanged.

3. Algorithm for calculating the difference in the ranks of a number in the Residue Number System

Let a system be given with bases $p_1, p_2, \ldots, p_n$, the range P of which is defined as $P = \prod_{i=n}^{n} p_i$. Any number A from the range $[0, P)$ can be represented uniquely for the chosen bases $A = (\alpha_1, \alpha_2, \ldots, \alpha_n)$.

The given system of bases uniquely corresponds to the system of orthogonal bases $B_1, B_2, \ldots, B_n$ such that the value A in weigted number system can be represented as

$$A \equiv \sum_{i=1}^{n} \alpha_i B_i \pmod{P}$$

or

$$A = \sum_{i=1}^{n} \alpha_i B_i - r(A)P, \tag{21}$$

where $r(A)$ is a positive integer showing how many times the range of the system P was exceeded in transition the representation of a number from the RNS to its positional representation in a system of orthogonal bases.

The positive integer r_A will be called the rank of the number A.

The rank of a number is used for implementation of the following operations: detection of dynamic range overflow, converting a number from RNS to binary representation, comparing a number, etc. The increasing demands for the speed of devices lead to the need to improve the performance of all operations. This work is devoted to the development of an effective method for calculating the rank of a number in RNS.

Theorem 4: If $X \to (x_1, x_2, \ldots, x_n)$ and $Y \to (y_1, y_2, \ldots, y_n)$ given in RNS with bases $p_1, p_2, \ldots, p_n$ satisfy the following conditions: $0 \le X < P$, $0 \le Y < P$ and $X + Y < P$, then the formula (22) is correct.

$$r(X+Y) = r(X) + r(Y) - \sum_{x_i + y_i \ge 0} \left| P_i^{-1} \right|_{p_i} \tag{22}$$

Let us formulate a theorem on the rank of the difference of two numbers.

Theorem 5: If $X \to (x_1, x_2, \ldots, x_n)$ and $Y \to (y_1, y_2, \ldots, y_n)$ given in RNS with bases $p_1, p_2, \ldots, p_n$ satisfy the following conditions: $0 \le X < P$, $0 \le Y < P$ and $0 \le X - Y < P$, then the formula (23) is correct.

$$r(X-Y) = r(X) - r(Y) + \sum_{x_i < y_i} \left| P_i^{-1} \right|_{p_i} \tag{23}$$

Proof: Calculating $r(X-Y)$, we get:

$$r(X-Y) = \left\lfloor \frac{\sum_{i=1}^{n} P_i \left| P_i^{-1} \right|_{p_i} |x_i - y_i|_{p_i}}{P} \right\rfloor \tag{24}$$

Since $|x_i - y_i|_{p_i}$ can be calculated by the formula:

$$|x_i - y_i|_{p_i} = \begin{cases} x_i - y_i + p_i & if\ x_i < y_i, \\ x_i - y_i & otherwise, \end{cases} \tag{25}$$

then (24) is transformed to:

$$r(X-Y) = \left\lfloor \frac{\sum_{i=1}^{n} P_i \left| P_i^{-1} \right|_{p_i} (x_i - y_i) + P \cdot \sum_{x_i < y_i} \left| P_i^{-1} \right|_{p_i}}{P} \right\rfloor \tag{26}$$

Considering that for any $m \in Z$ and $a \in R$ the equality holds $\lfloor m + a \rfloor = m + \lfloor a \rfloor$ and $\sum_{x_i < y_i} \left| P_i^{-1} \right|_{p_i} \in Z$, the formula (26) takes the form:

$$r\left(X-Y\right)=\left\lfloor\frac{\sum_{i=1}^{n}P_i\left|P_i^{-1}\right|_{p_i}\cdot x_i}{P}-\frac{\sum_{i=1}^{n}P_i\left|P_i^{-1}\right|_{p_i}\cdot y_i}{P}\right\rfloor+\sum_{x_i<y_i}\left|P_i^{-1}\right|_{p_i} \tag{27}$$

Since $P\in Z$, then

$$\sum_{i=1}^{n}P_i\left|P_i^{-1}\right|_{p_i}\cdot x_i = \left|\sum_{i=1}^{n}P_i\left|P_i^{-1}\right|_{p_i}\cdot x_i\right|_P+P\cdot\left\lfloor\frac{\sum_{i=1}^{n}P_i\left|P_i^{-1}\right|_{p_i}\cdot x_i}{P}\right\rfloor \tag{28}$$

$$\sum_{i=1}^{n}P_i\left|P_i^{-1}\right|_{p_i}\cdot y_i = \left|\sum_{i=1}^{n}P_i\left|P_i^{-1}\right|_{p_i}\cdot y_i\right|_P+P\cdot\left\lfloor\frac{\sum_{i=1}^{n}P_i\left|P_i^{-1}\right|_{p_i}\cdot y_i}{P}\right\rfloor \tag{29}$$

Substituting (28) and (29) in (27), we get:

$$\begin{aligned} r\left(X-Y\right) &= \left\lfloor\frac{\sum_{i=1}^{n}P_i\left|P_i^{-1}\right|_{p_i}\cdot x_i}{P}\right\rfloor-\left\lfloor\frac{\sum_{i=1}^{n}P_i\left|P_i^{-1}\right|_{p_i}\cdot y_i}{P}\right\rfloor \\ &+ \left\lfloor\frac{\left|\sum_{i=1}^{n}P_i\left|P_i^{-1}\right|_{p_i}\cdot x_i\right|_P}{P}-\frac{\left|\sum_{i=1}^{n}P_i\left|P_i^{-1}\right|_{p_i}\cdot y_i\right|_P}{P}\right\rfloor \\ &+ \sum_{x_i<y_i}\left|P_i^{-1}\right|_{p_i} \end{aligned} \tag{30}$$

According to the Chinese Remainder Theorem, $\left|\sum_{i=1}^{n}P_i\left|P_i^{-1}\right|_{p_i}\cdot x_i\right|_P = X$ and $\left|\sum_{i=1}^{n}P_i\left|P_i^{-1}\right|_{p_i}\cdot y_i\right|_P = Y$, therefore (30) takes the form:

$$\begin{aligned} r\left(X-Y\right) &= \left\lfloor\frac{\sum_{i=1}^{n}P_i\left|P_i^{-1}\right|_{p_i}\cdot x_i}{P}\right\rfloor-\left\lfloor\frac{\sum_{i=1}^{n}P_i\left|P_i^{-1}\right|_{p_i}\cdot y_i}{P}\right\rfloor+ \\ &+ \left\lfloor\frac{X}{P}-\frac{Y}{P}\right\rfloor+\sum_{x_i<y_i}\left|P_i^{-1}\right|_{p_i} \end{aligned} \tag{31}$$

Since by the condition of the theorem $0\leq X-Y<0$, then the term $\left\lfloor\frac{X}{P}-\frac{Y}{P}\right\rfloor$ in (31) s equal to zero. Considering that

$$r\left(X\right) = \left\lfloor\frac{\sum_{i=1}^{n}P_i\left|P_i^{-1}\right|_{p_i}\cdot x_i}{P}\right\rfloor \tag{32}$$

$$r\left(Y\right) = \left\lfloor\frac{\sum_{i=1}^{n}P_i\left|P_i^{-1}\right|_{p_i}\cdot y_i}{P}\right\rfloor \tag{33}$$

we get:

$$r\left(X-Y\right)=r\left(X\right)-r\left(Y\right)+\sum_{x_i<y_i}\left|P_i^{-1}\right|_{p_i} \tag{34}$$

The theorem is proved.

Theorem 6: Let the RNS moduli $p_1, p_2, \ldots, p_n$ and two integer numbers $X, Y \in Z_P$ in RNS be given: $X \to (x_1, x_2, \ldots, x_n)$ and $Y \to (y_1, y_2, \ldots, y_n)$. If there is such $j \in \overline{1,n}$ for which the equality $X = p_j \cdot Y$ holds, then

$$r\left(X\right)=p_j\cdot r\left(Y\right)-\sum_{i=1}^{n}\left|P_i^{-1}\right|_{p_i}\cdot\left\lfloor\frac{p_j\cdot y_i}{p_i}\right\rfloor \tag{35}$$

Proof: Calculating the value $r\left(X\right)$ by the formula (32), we get:

$$r\left(X\right)=\left\lfloor\frac{\sum_{i=1}^{n}P_i\left|P_i^{-1}\right|_{p_i}\cdot x_i}{P}\right\rfloor \tag{36}$$

Since for any i the equation $x_i=\left|p_j\cdot y_i\right|_{p_i}=p_j\cdot y_i-p_i\cdot\left\lfloor\frac{p_j\cdot y_i}{p_i}\right\rfloor$ holds, then (36) is transformed to:

$$\begin{aligned}
r\left(X\right) &= \left\lfloor\frac{\sum_{i=1}^{n}P_i\left|P_i^{-1}\right|_{p_i}\cdot\left(p_j\cdot y_i-p_i\cdot\left\lfloor\frac{p_j\cdot y_i}{p_i}\right\rfloor\right)}{P}\right\rfloor= \\
&= \left\lfloor\frac{p_j\cdot\sum_{i=1}^{n}P_i\left|P_i^{-1}\right|_{p_i}\cdot y_i-P\cdot\sum_{i=1}^{n}\left|P_i^{-1}\right|_{p_i}\cdot\left\lfloor\frac{p_j\cdot y_i}{p_i}\right\rfloor}{P}\right\rfloor= \\
&= \left\lfloor\frac{p_j\cdot\sum_{i=1}^{n}P_i\left|P_i^{-1}\right|_{p_i}\cdot y_i}{P}\right\rfloor-\sum_{i=1}^{n}\left|P_i^{-1}\right|_{p_i}\cdot\left\lfloor\frac{p_j\cdot y_i}{p_i}\right\rfloor
\end{aligned} \tag{37}$$

According to the Chinese remainder theorem, $\sum_{i=1}^{n}P_i\left|P_i^{-1}\right|_{p_i}\cdot y_i$ can be represented in the form $\sum_{i=1}^{n}P_i\left|P_i^{-1}\right|_{p_i}\cdot y_i=P\cdot r\left(Y\right)+Y$, therefore the formula (37) is transformed to:

$$\begin{aligned}
r\left(X\right) &= \left\lfloor\frac{p_j\cdot P\cdot r\left(Y\right)+p_j\cdot Y}{P}\right\rfloor-\sum_{i=1}^{n}\left|P_i^{-1}\right|_{p_i}\cdot\left\lfloor\frac{p_j\cdot y_i}{p_i}\right\rfloor= \\
&= p_j\cdot r\left(Y\right)+\left\lfloor\frac{p_j\cdot Y}{P}\right\rfloor-\sum_{i=1}^{n}\left|P_i^{-1}\right|_{p_i}\cdot\left\lfloor\frac{p_j\cdot y_i}{p_i}\right\rfloor
\end{aligned} \tag{38}$$

It follows from the condition of the theorem that $X = p_j \cdot Y$ and $X \in Z_P$, therefore X satisfies the inequality $0 \le X < P$, hence the term $\left\lfloor\frac{p_j\cdot Y}{P}\right\rfloor$ in the formula (38) is equal to zero, and the formula (38) is transformed to:

$$r\left(X\right)=p_j\cdot r\left(Y\right)-\sum_{i=1}^{n}\left|P_i^{-1}\right|_{p_i}\cdot\left\lfloor\frac{p_j\cdot y_i}{p_i}\right\rfloor$$

The theorem is proved.

Using the theorems 5, 6 and the formula (22) we propose an algorithm for calculating the rank of a number.

Algorithm 1 calculating the rank of a number $r(X)$.

Input $X \to (x_1, x_2, \ldots, x_n)$, p_1, p_2,..., p_{n-1}, p_n,
$w_{i,j} = \left|p_i^{-1}\right|_{p_j} \ \forall : i \neq j \ \& \ i,j = \overline{1,n}$, $B_i = \left|P_i^{-1}\right|_{p_i} \ \forall : i = \overline{1,n}$,
$r_i = r(i) \ \forall : i = \overline{1,p_n}$, where $P_i = P/p_i \ \forall : i = \overline{1,n}$.
Output $r(X)$.
$x_1^{(1)} = 0$;
For $j = 2$, $j \leq n$, $j++$ **do**
$x_j^{(1)} = |x_j - x_1|_{p_j}$; $y_j^{(1)} = \left|w_{1,j} \cdot x_j^{(1)}\right|_{p_j}$; Parallel processing
For $i = 2$, $i < n$, $i++$ **do**
$x_i^{(i)} = 0$;
For $j = i+1$, $j \leq n$, $j++$ **do**
$x_j^{(i)} = \left|y_j^{(i-1)} - y_i^{(i-1)}\right|_{p_j}$; $y_j^{(i)} = \left|w_{i,j} \cdot x_j^{(i)}\right|_{p_j}$; Parallel processing
$r = p_{n-1} \cdot r\left(y_n^{(n-1)}\right) = p_{n-1} \cdot r_{y_n^{(n-1)}}$;
For $j = 1$, $j < n$, $j++$ **do**
$y_j^{(n-1)} = \left|y_n^{(n-1)}\right|_{p_j}$; Parallel processing
$x_j^{(n-1)} = \left|p_{n-1} \cdot y_j^{(n-1)}\right|_{p_j}$; $r = r - B_j \cdot \left\lfloor \frac{p_{n-1} \cdot y_j^{(n-1)}}{p_j} \right\rfloor$; Parallel processing
For $i = n-2$, $i \geq 1$, $i--$ **do**
$r_{mult} = 0$;
$r_{add} = 0$;
For $j = 1$, $j \leq n$, $j++$ **do**
$y_j^{(i)} = \left|x_j^{(i)} + y_{i+1}^{(i)}\right|_{p_j}$; Parallel processing
If $x_j^{(i)} + y_{i+1}^{(i)} \geq p_j$ **Then**
$r_{add} = r_{add} + B_j$;
$x_j^{(i)} = \left|p_i \cdot y_j^{(i)}\right|_{p_j}$; $r_{mult} = r_{mult} + B_j \cdot \left\lfloor \frac{p_i \cdot y_j^{(i)}}{p_j} \right\rfloor$; Parallel processing
$r = r + r_{y_{i+1}^{(i)}} - r_{add}$; $r = p_i \cdot r - r_{mult}$;
For $j = 1$, $j \leq n$, $j++$ **do**
If $x_j^{(1)} + x_1 \geq p_j$ **Then**
$r = r - B_j$;
$r = r + r_{x_1}$;
Result r

Let's consider an example of how the rank of a number can be calculated using the formulas (22), (23) and (35).

Example. Let the RNS moduli $p_1 = 2, p_2 = 3, p_3 = 5$ be given, calculate the rank of the number $X \to (1,,2,3)$.

(i) RNS range is equal to $P = \prod_{i=1}^{n} p_i = 30$.

(ii) Calculating the values of constants P_i and $\left|P_i^{-1}\right|_{p_i}$, we get: $P_1 = P/p_1 = 15$, $\left|P_1^{-1}\right|_{p_1} = \left|15^{-1}\right|_2 = 1$, $P_2 = P/p_2 = 10$, $\left|P_2^{-1}\right|_{p_2} = \left|10^{-1}\right|_3 = 1$, $P_3 = P/p_3 = 6$ and $\left|P_3^{-1}\right|_{p_3} = \left|6^{-1}\right|_5 = 1$,

(iii) We calculate the values of constants $\left|p_i^{-1}\right|_{p_j}$:
$\left|p_1^{-1}\right|_{p_2} = \left|2^{-1}\right|_3 = 2$, $\left|p_1^{-1}\right|_{p_3} = \left|2^{-1}\right|_5 = 3$, $\left|p_2^{-1}\right|_{p_3} = \left|3^{-1}\right|_5 = 2$,

(iv) Calculating the ranks of the numbers $0, \ldots, (p_n - 1)$, we get: $r(0) = 0$,
$r(1) = \left\lfloor \frac{\sum_{i=1}^{n} \left|P_i^{-1}\right|_{p_i} \cdot P_i \cdot x_i}{P} \right\rfloor = \left\lfloor \frac{1 \cdot 15 \cdot 1 + 1 \cdot 10 \cdot 1 + 1 \cdot 6 \cdot 1}{30} \right\rfloor = 1$,
$r(2) = r(1) + r(1) - \left|P_1^{-1}\right|_{p_1} = 1 + 1 - 1 = 1$,
$r(3) = r(2) + r(1) - \left|P_2^{-1}\right|_{p_2} = 1 + 1 - 1 = 1$,
$r(4) = r(3) + r(1) - \left|P_1^{-1}\right|_{p_1} = 1 + 1 - 1 = 1$.

(v) For convenience, we enter the calculation results in the table:

Table 1. Calculations of $X = \left\lfloor \frac{X}{p_1 \cdot p_2} \right\rfloor$

		$p_1 = 2$	$p_2 = 3$	$p_3 = 5$
X		$x_1 = 1$	$x_2 = 2$	$x_3 = 3$
$X^{(1)} = X - x_1$	$-x_1$	0	1	2
$Y^{(1)} = \left\lfloor \frac{X^{(1)}}{p_1} \right\rfloor$	$\times \left\lvert p_1^{-1} \right\rvert_{p_i}$	–	2	1
$X^{(2)} = Y^{(1)} - y_2^{(1)}$	$-y_2^{(1)}$	–	0	4
$Y^{(2)} = \left\lfloor \frac{X^{(2)}}{p_2} \right\rfloor$	$\times \left\lvert p_2^{-1} \right\rvert_{p_i}$	–	–	3

It follows from the table 1, that $X = \left\lfloor \frac{X}{p_1 \cdot p_2} \right\rfloor = Y^{(2)} = 3$.
Reverse:
From the calculations presented in the table 2 it follows that $r(X) = 1$.

4. Conclusion

In this paper, a new method for calculating the rank of a number in the Residue Number System was presented, and a theorem on the difference in the ranks of numbers in the Residue Number System was proved. The proposed method allows reducing the amount of necessary calculations and increase the speed of calculating the rank of a number relative to the method for calculating the rank of a number based on the approximate method. To find the rank of a number in the method for calculating the rank of a number based on the approximate method, it is necessary to calculate n operations with numbers exceeding the modulus value; in the proposed method, it is necessary to calculate $\frac{n \cdot (n-1)}{2}$ operations not exceeding the value of the modulus.

Acknowledgements The reported study was funded by RFBR, Sirius University of Science and Technology, JSC Russian Railways and Educational Fund "Talent and success", project number 20-37-51004, and Russian Federation President Grant MK-24.2020.9, and SP-3149.2019.5

Table 2. Calculations of the rank $r(X)$

		$p_1=2$	$p_2=3$	$p_3=5$	$r(X)$
$Y^{(2)}$		$y_1^{(2)}=1$	$y_2^{(2)}=0$	$y_3^{(2)}=3$	$r\left(Y^{(2)}\right)=r(3)=1$
$X^{(2)}=p_2\cdot Y^{(2)}$	$\times p_2$	1	0	4	$r\left(X^{(2)}\right)=p_2\cdot r\left(Y^{(2)}\right)-\sum_{i=1}^{n}\left\|P_i^{-1}\right\|_{p_i}\left\lfloor\frac{p_2\cdot y_i^{(2)}}{p_i}\right\rfloor=3\cdot 1-1\cdot 1-1\cdot 0-1\cdot 1=1$
$Y^{(1)}=X^{(2)}+y_2^{(1)}$	$+y_2^{(1)}$	1	2	1	$r\left(Y^{(1)}\right)=r\left(X^{(2)}\right)+r\left(y_2^{(1)}\right)-\sum_{x_i^{(2)}+y_2^{(1)}\geq p_i}\left\|P_i^{-1}\right\|_{p_i}=1+1-1=1$
$X^{(1)}=p_1\cdot Y^{(1)}$	$\times p_1$	0	1	2	$r\left(X^{(1)}\right)=p_1\cdot r\left(Y^{(1)}\right)-\sum_{i=1}^{n}\left\|P_i^{-1}\right\|_{p_i}\left\lfloor\frac{p_1\cdot y_i^{(1)}}{p_i}\right\rfloor=2\cdot 1-1\cdot 1-1\cdot 1-1\cdot 0=0$
$X=X^{(1)}+x_1$	$+x_1$	1	2	3	$r(X)=r\left(X^{(1)}\right)+r(x_1)-\sum_{x_i^{(1)}+x_1\geq p_i}\left\|P_i^{-1}\right\|_{p_i}=0+1=1$

References

[1] Babenko M, Tchernykh A, Chervyakov N, Kuchukov V, Miranda-López V, Rivera-Rodriguez R, Du Z and Talbi E G 2019 *Programming and Computer Software* **45** 532–543

[2] Garner H L 1959 The residue number system *Papers presented at the the March 3-5, 1959, western joint computer conference* pp 146–153

[3] Patel R A, Benaissa M and Boussakta S 2007 *IEEE Transactions on Computers* **56** 1484–1492

[4] Wang Y 1998 New chinese remainder theorems *Conference Record of Thirty-Second Asilomar Conference on Signals, Systems and Computers (Cat. No. 98CH36284)* vol 1 (IEEE) pp 165–171

[5] Vun C H, Premkumar A B and Zhang W 2013 *IEEE Transactions on Circuits and Systems I: Regular Papers* **60** 2139–2152

[6] Tchernykh A, Babenko M, Chervyakov N, Miranda-López V, Avetisyan A, Drozdov A Y, Rivera-Rodriguez R, Radchenko G and Du Z 2020 *IEEE Internet of Things Journal* **7** 10171–10188

[7] Bi S and Gross W J 2008 *IEEE Transactions on Computers* **57** 1624–1632

[8] Babenko M, Tchernykh A, Chervyakov N, Kuchukov V, Miranda-López V, Rivera-Rodriguez R, Du Z and Talbi E G 2019 *Programming and Computer Software* **45** 532–543

[9] Sousa L, Antão S and Chaves R 2012 *IEEE transactions on very large scale integration (VLSI) systems* **21** 1945–1949

[10] Krasnobayev V, Kuznetsov A, Koshman S and Moroz S 2018 Improved method of determining the alternative set of numbers in residue number system *XVIII International Conference on Data Science and Intelligent Analysis of Information* (Springer) pp 319–328

[11] Chervyakov N, Babenko M, Lyakhov P and Lavrinenko I 2014 *Cybernetics and Systems Analysis* **50** 977–984

[12] Chervyakov N, Babenko M, Tchernykh A, Kucherov N, Miranda-López V and Cortés-Mendoza J M 2019 *Future Generation Computer Systems* **92** 1080–1092