Chapter 9

METHODS OF DATA VERIFICATION IN RESIDUE NUMBER SYSTEM, BASED ON THE NULLIFICATION PROCEDURE

Viktor Krasnobayev[1], Sergey Koshman[1], Valery Kurchanov[2]

[1] V. N. Karazin Kharkiv National University, Svobody sq., 4,
Kharkov, 61022, Ukraine,
[2] Poltava National Technical Yuri Kondratyuk University, 24,
Pershotravneva Avenue, Poltava, 36011, Ukraine
v.a.krasnobaev@gmail.com, s_koshman@ukr.net, kvnkvn@meta.ua

Abstract: *As is well known, the main advantage or Residue Number System (RNS) usage if compared to the positional number system, is that RNS allows rapid implementation of arithmetic operations of addition, subtraction and multiplication. However, while solving one particular computational problem a necessity to implement operation result verification appears, i.e. there's a necessity to implement the nullification procedure of non-positional code structure (NCS). Performing nullification procedure takes up to 90% of data verification time in RNS, requires considerable time, therefore it denies main purpose of RNS usage. Thus, the development of fast nullification procedure is a crucial task.*

Keywords*: residual classes system, positional numeral systems, computer system and a data processing means, nullification procedure, non-positional code structure.*

1 Successive subtraction method

We'll consider the nullification procedure from a point of its implementation time. The essence of the basic in RNS first (N1) nullification procedure (successive nullification (SN) procedure) consists of the sequence of subtraction operations:

$$A^{(i+1)} = A^{(i)} - CN^{(i)}, \quad (1)$$

utilizing aggregate of nullification constants (NC)

$$NC^{(0)} = [t_1^{(0)} \| t_2^{(0)} \| t_3^{(0)} \| \ldots \| t_{i-1}^{(0)} \| t_i^{(0)} \| t_{i+1}^{(0)} \| \ldots \| t_{n-3}^{(0)} \| t_{n-2}^{(0)} \| t_{n-1}^{(0)} \| t_n^{(0)} \| t_{n+1}^{(0)}],$$

$$t_1^{(0)} = a_1^{(0)},\ t_1^{(0)} = \overline{0, m_1 - 1};$$

$$NC^{(1)} = [0 \| t_2^{(1)} \| t_3^{(1)} \| \ldots \| t_{i-1}^{(1)} \| t_i^{(1)} \| t_{i+1}^{(1)} \| \ldots \| t_{n-3}^{(1)} \| t_{n-2}^{(1)} \| t_{n-1}^{(1)} \| t_n^{(1)} \| t_{n+1}^{(1)}],$$

$$t_2^{(1)} = a_2^{(1)},\ t_2^{(1)} = \overline{0, m_2 - 1};$$

$$NC^{(2)} = [0 \| 0 \| t_3^{(2)} \| \ldots \| t_{i-1}^{(2)} \| t_i^{(2)} \| t_{i+1}^{(2)} \| \ldots \| t_{n-3}^{(2)} \| t_{n-2}^{(2)} \| t_{n-1}^{(2)} \| t_n^{(2)} \| t_{n+1}^{(2)}],$$

$$t_3^{(2)} = a_3^{(2)},\ t_3^{(2)} = \overline{0, m_3 - 1};$$

$$NC^{(i-1)} = [0 \| 0 \| 0 \| \ldots \| 0 \| t_i^{(i-1)} \| t_{i+1}^{(i-1)} \| \ldots \| t_{n-3}^{(i-1)} \| t_{n-2}^{(i-1)} \| t_{n-1}^{(i-1)} \| t_n^{(i-1)} \| t_{n+1}^{(i-1)}],$$

$$t_i^{(i-1)} = a_i^{(i-1)},\ t_i^{(i-1)} = \overline{0, m_i - 1};$$

$$NC^{(n-2)} = [0 \| 0 \| 0 \| \ldots \| 0 \| 0 \| 0 \| \ldots \| 0 \| 0 \| t_{n-1}^{(n-2)} \| t_n^{(n-2)} \| t_{n+1}^{(n-2)}],$$

$$t_{n-1}^{(n-2)} = a_{n-1}^{(n-2)},\ t_{n-1}^{(n-2)} = \overline{0, m_{n-1} - 1};$$

$$NC^{(n-1)} = [0 \| 0 \| 0 \| \ldots \| 0 \| 0 \| 0 \| \ldots \| 0 \| 0 \| 0 \| t_n^{(n-1)} \| t_{n+1}^{(n-1)}],$$

$$t_n^{(n-1)} = a_n^{(n-1)},\ t_n^{(n-1)} = \overline{0, m_n - 1}, \qquad (2)$$

from the corresponding numbers:

$$A^{(0)} = [a_1^{(0)} \| a_2^{(0)} \| a_3^{(0)} \| \ldots \| a_{i-1}^{(0)} \| a_i^{(0)} \| a_{i+1}^{(0)} \| \ldots \| a_{n-3}^{(0)} \| a_{n-2}^{(0)} \| a_{n-1}^{(0)} \| a_n^{(0)} \| a_{n+1}^{(0)}],$$

$$A^{(1)} = [0 \| a_2^{(1)} \| a_3^{(1)} \| \ldots \| a_{i-1}^{(1)} \| a_i^{(1)} \| a_{i+1}^{(1)} \| \ldots \| a_{n-3}^{(1)} \| a_{n-2}^{(1)} \| a_{n-1}^{(1)} \| a_n^{(1)} \| a_{n+1}^{(1)}],$$

$$A^{(2)} = [0 \| 0 \| a_3^{(2)} \| \ldots \| a_{i-1}^{(2)} \| a_i^{(2)} \| a_{i+1}^{(2)} \| \ldots \| a_{n-3}^{(2)} \| a_{n-2}^{(2)} \| a_{n-1}^{(2)} \| a_n^{(2)} \| a_{n+1}^{(2)}],$$

$$A^{(i-1)} = [0 \| 0 \| 0 \| \ldots \| 0 \| a_i^{(i-1)} \| a_{i+1}^{(i-1)} \| \ldots \| a_{n-3}^{(i-1)} \| a_{n-2}^{(i-1)} \| a_{n-1}^{(i-1)} \| a_n^{(i-1)} \| a_{n+1}^{(i-1)}],$$

so on.

For example: the execution of the first subtraction operation

$$A^{(1)} = A^{(0)} - NC^{(0)} = [a_1^{(0)} \| a_2^{(0)} \| a_3^{(0)} \| \ldots \| a_{i-1}^{(0)} \| a_i^{(0)} \| a_{i+1}^{(0)} \| \ldots$$

$$\ldots \| a_{n-3}^{(0)} \| a_{n-2}^{(0)} \| a_{n-1}^{(0)} \| a_n^{(0)} \| a_{n+1}^{(0)}] - [t_1^{(0)} \| t_2^{(0)} \| t_3^{(0)} \| \ldots \| t_{i-1}^{(0)} \| t_i^{(0)} \| t_{i+1}^{(0)} \| \ldots$$

$$\ldots \| t_{n-3}^{(0)} \| t_{n-2}^{(0)} \| t_{n-1}^{(0)} \| t_n^{(0)} \| t_{n+1}^{(0)}] = \{[a_1^{(0)} - t_1^{(0)}] \bmod m_1 \| [a_2^{(0)} - t_2^{(0)}] \bmod m_2 \|$$

$$\| [a_3^{(0)} - t_3^{(0)}] \bmod m_3 \| \ldots \| [a_{i-1}^{(0)} - t_{i-1}^{(0)}] \bmod m_{i-1} \| [a_i^{(0)} - t_i^{(0)}] \bmod m_i \|$$

$$\| [a_{i+1}^{(0)} - t_{i+1}^{(0)}] \bmod m_{i+1} \| \ldots \| [a_{n-3}^{(0)} - t_{n-3}^{(0)}] \bmod m_{n-3} \| [a_{n-2}^{(0)} - t_{n-2}^{(0)}] \bmod m_{n-2} \|$$
$$\| [a_{n-1}^{(0)} - t_{n-1}^{(0)}] \bmod m_{n-1} \| [a_n^{(0)} - t_n^{(0)}] \bmod m_n \| [a_{n+1}^{(0)} - t_{n+1}^{(0)}] \bmod m_{n+1} \} =$$
$$= [0 \| a_2^{(1)} \| a_3^{(1)} \| \ldots \| a_{i-1}^{(1)} \| a_i^{(1)} \| a_{i+1}^{(1)} \| \ldots \| a_{n-3}^{(1)} \| a_{n-2}^{(1)} \| a_{n-1}^{(1)} \| a_n^{(1)} \| a_{n+1}^{(1)}];$$

the execution of the second subtraction operation

$$A^{(2)} = A^{(1)} - NC^{(1)} =$$
$$= [0 \| a_2^{(1)} \| a_3^{(1)} \| \ldots \| a_{i-1}^{(1)} \| a_i^{(1)} \| a_{i+1}^{(1)} \| \ldots \| a_{n-3}^{(1)} \| a_{n-2}^{(1)} \| a_{n-1}^{(1)} \| a_n^{(1)} \| a_{n+1}^{(1)}] -$$
$$- [0 \| t_2^{(1)} \| t_3^{(1)} \| \ldots \| t_{i-1}^{(1)} \| t_i^{(1)} \| t_{i+1}^{(1)} \| \ldots \| t_{n-3}^{(1)} \| t_{n-2}^{(1)} \| t_{n-1}^{(1)} \| t_n^{(1)} \| t_{n+1}^{(1)}] =$$
$$= \{0 \| [a_2^{(1)} - t_2^{(1)}] \bmod m_2 \| [a_3^{(1)} - t_3^{(1)}] \bmod m_3 \| \ldots \| [a_{i-1}^{(1)} - t_{i-1}^{(1)}] \bmod m_{i-1} \|$$
$$\| [a_i^{(1)} - t_i^{(1)}] \bmod m_i \| [a_{i+1}^{(1)} - t_{i+1}^{(1)}] \bmod m_{i+1} \| \ldots \| [a_{n-3}^{(1)} - t_{n-3}^{(1)}] \bmod m_{n-3} \|$$
$$\| [a_{n-2}^{(1)} - t_{n-2}^{(1)}] \bmod m_{n-2} \| [a_{n-1}^{(1)} - t_{n-1}^{(1)}] \bmod m_{n-1} \| [a_n^{(1)} - t_n^{(1)}] \bmod m_n \|$$
$$\| [a_{n+1}^{(1)} - t_{n+1}^{(1)}] \bmod m_{n+1} \} =$$
$$= [0 \| 0 \| a_3^{(2)} \| \ldots \| a_{i-1}^{(2)} \| a_i^{(2)} \| a_{i+1}^{(2)} \| \ldots \| a_{n-3}^{(2)} \| a_{n-2}^{(2)} \| a_{n-1}^{(2)} \| a_n^{(2)} \| a_{n+1}^{(2)}];$$

the execution of the third subtraction operation

$$A^{(3)} = A^{(2)} - NC^{(2)} =$$
$$= [0 \| 0 \| a_3^{(2)} \| \ldots \| a_{i-1}^{(2)} \| a_i^{(2)} \| a_{i+1}^{(2)} \| \ldots \| a_{n-3}^{(2)} \| a_{n-2}^{(2)} \| a_{n-1}^{(2)} \| a_n^{(2)} \| a_{n+1}^{(2)}] -$$
$$- [0 \| 0 \| t_3^{(2)} \| \ldots \| t_{i-1}^{(2)} \| t_i^{(2)} \| t_{i+1}^{(2)} \| \ldots \| t_{n-3}^{(2)} \| t_{n-2}^{(2)} \| t_{n-1}^{(2)} \| t_n^{(2)} \| t_{n+1}^{(2)}] =$$
$$= [0 \| 0 \| 0 \| a_4^{(3)} \| a_5^{(3)} \| \ldots \| a_{i-1}^{(3)} \| a_i^{(3)} \| a_{i+1}^{(3)} \| \ldots \| a_{n-3}^{(3)} \| a_{n-2}^{(3)} \| a_{n-1}^{(3)} \| a_n^{(3)} \| a_{n+1}^{(3)}],$$

and so on.

The algorithm of the nullification procedure is shown in the Table 1 and in fig. 1.

Table 1 – Nullification procedure algorithm

Operation №	Operation content
1	Reference by meaning $a_1^{(0)}$ and number $A^{(0)}$ in NCB_0 via $NC^{(0)}$.
2	Executing subtraction operation $A^{(1)} = A^{(0)} - NC^{(0)}$.
3	Referencing by value $a_2^{(1)}$ and number $A^{(1)}$ in NCB_1 via $NC^{(1)}$.
4	Executing subtraction operation $A^{(2)} = A^{(1)} - NC^{(1)}$.
5	Referencing by value $a_3^{(2)}$ and number $A^{(2)}$ in NCB_2 via $NC^{(2)}$.
6	Executing subtraction operation $A^{(3)} = A^{(2)} - NC^{(2)}$.
7	Referencing by value $a_4^{(3)}$ and number $A^{(3)}$ in NCB_3 via $NC^{(3)}$.
8	Executing subtraction operation $A^{(4)} = A^{(3)} - NC^{(3)}$.
⋮	…
$2n-3$	Referencing by value $a_{n-1}^{(n-2)}$ and number $A^{(n-2)}$ in NCB_{n-2} via $NC^{(n-2)}$.
$2n-2$	Executing subtraction operation $A^{(n-1)} = A^{(n-2)} - NC^{(n-2)}$.
$2n-1$	Referencing by value $a_n^{(n-1)}$ and number $A^{(n-1)}$ in NCB_{n-1} via $NC^{(n-1)}$.
$2n$	Executing subtraction operation $A^{(n)} = A^{(n-1)} - NC^{(n-1)}$. Obtaining nullified number: $A^{(N)} = A^{(n)} = [0 \,\|\|\, 0 \,\|\|\, \ldots \,\|\|\, 0 \,\|\|\, \ldots \,\|\|\, 0 \,\|\|\, 0 \,\|\|\, \gamma_{n+1} = a_{n+1}^{(n)}]$.

Operation № (cycle)	Operation content
1	Referencing residue value $a_1^{(0)}$ of number $A = A^{(0)} = [a_1^{(0)} \| a_2^{(0)} \|$ $\| a_3^{(0)} \| \ldots \| a_{i-1}^{(0)} \| a_i^{(0)} \| a_{i+1}^{(0)} \| \ldots \| a_{n-3}^{(0)} \| a_{n-2}^{(0)} \| a_{n-1}^{(0)} \| a_n^{(0)} \| a_{n+1}^{(0)}]$ in NCB_0 via nullification constant $NC^{(0)} = [t_1^{(0)} \| t_2^{(0)} \| t_3^{(0)} \| \ldots \| t_{i-1}^{(0)} \| t_i^{(0)} \| t_{i+1}^{(0)} \| \ldots$ $\ldots \| t_{n-3}^{(0)} \| t_{n-2}^{(0)} \| t_{n-1}^{(0)} \| t_n^{(0)} \| t_{n+1}^{(0)}]$; $t_1^{(0)} = a_1^{(0)}$; $t_1^{(0)} = \overline{0, m_1 - 1}$.
2	Executing subtraction operation $A^{(1)} = A^{(0)} - NC^{(0)} = [a_1^{(0)} \| a_2^{(0)} \|$ $\| a_3^{(0)} \| \ldots \| a_{i-1}^{(0)} \| a_i^{(0)} \| a_{i+1}^{(0)} \| \ldots \| a_{n-3}^{(0)} \| a_{n-2}^{(0)} \| a_{n-1}^{(0)} \| a_n^{(0)} \| a_{n+1}^{(0)}] -$ $-[t_1^{(0)} \| t_2^{(0)} \| t_3^{(0)} \| \ldots \| t_{i-1}^{(0)} \| t_i^{(0)} \| t_{i+1}^{(0)} \| \ldots \| t_{n-3}^{(0)} \| t_{n-2}^{(0)} \| t_{n-1}^{(0)} \| t_n^{(0)} \| t_{n+1}^{(0)}] =$ $= \{[a_1^{(0)} - t_1^{(0)}] \bmod m_1 \| [a_2^{(0)} - t_2^{(0)}] \bmod m_2 \| [a_3^{(0)} - t_3^{(0)}] \bmod m_3 \| \ldots$ $\ldots \| [a_{i-1}^{(0)} - t_{i-1}^{(0)}] \bmod m_{i-1} \| [a_i^{(0)} - t_i^{(0)}] \bmod m_i \| [a_{i+1}^{(0)} - t_{i+1}^{(0)}] \bmod m_{i+1} \| \ldots$ $\ldots \| [a_{n-3}^{(0)} - t_{n-3}^{(0)}] \bmod m_{n-3} \| [a_{n-2}^{(0)} - t_{n-2}^{(0)}] \bmod m_{n-2} \| [a_{n-1}^{(0)} - t_{n-1}^{(0)}] \bmod m_{n-1} \|$ $\| [a_n^{(0)} - t_n^{(0)}] \bmod m_n \| [a_{n+1}^{(0)} - t_{n+1}^{(0)}] \bmod m_{n+1}\} = [0 \| a_2^{(1)} \| a_3^{(1)} \| \ldots \| a_{i-1}^{(1)} \| a_i^{(1)} \|$ $\| a_{i+1}^{(1)} \| \ldots \| a_{n-3}^{(1)} \| a_{n-2}^{(1)} \| a_{n-1}^{(1)} \| a_n^{(1)} \| a_{n+1}^{(1)}]$.

Fig. 1.

3	Referencing residue value $a_2^{(1)}$ of number $A^{(1)} = [0 \,\|\|\, a_2^{(1)} \,\|\, a_3^{(1)} \,\|\| \ldots$ $\ldots \,\|\| \, a_{i-1}^{(1)} \,\|\, a_i^{(1)} \,\|\, a_{i+1}^{(1)} \,\|\| \ldots \,\|\| \, a_{n-3}^{(1)} \,\|\, a_{n-2}^{(1)} \,\|\| \, a_{n-1}^{(1)} \,\|\, a_n^{(1)} \,\|\, a_{n+1}^{(1)}]$ in NCB_1 via nullification constant $NC^{(1)} = [0 \,\|\| \, t_2^{(1)} \,\|\, t_3^{(1)} \,\|\| \ldots \,\|\| \, t_{i-1}^{(1)} \,\|\, t_i^{(1)} \,\|\, t_{i+1}^{(1)} \,\|\| \ldots \,\|\| \, t_{n-3}^{(1)} \,\|\, t_{n-2}^{(1)} \,\|\|$ $\,\|\| \, t_{n-1}^{(1)} \,\|\, t_n^{(1)} \,\|\, t_{n+1}^{(1)}]$; $t_2^{(1)} = a_2^{(1)}$; $t_2^{(1)} = \overline{0, m_2 - 1}$.
4	Executing subtraction operation $A^{(2)} = A^{(1)} - NC^{(1)} = \left[0 \,\|\| \, a_2^{(1)} \,\|\, a_3^{(1)} \,\|\| \ldots \right.$ $\left. \ldots \,\|\| \, a_{i-1}^{(1)} \,\|\, a_i^{(1)} \,\|\, a_{i+1}^{(1)} \,\|\| \ldots \,\|\| \, a_{n-3}^{(1)} \,\|\, a_{n-2}^{(1)} \,\|\| \, a_{n-1}^{(1)} \,\|\, a_n^{(1)} \,\|\, a_{n+1}^{(1)} \right] - \left[0 \,\|\| \, t_2^{(1)} \,\|\, t_3^{(1)} \,\|\| \ldots \,\|\| \, t_{i-1}^{(1)} \,\|\right.$ $\left. t_i^{(1)} \,\|\, t_{i+1}^{(1)} \,\|\| \ldots \,\|\| \, t_{n-3}^{(1)} \,\|\, t_{n-2}^{(1)} \,\|\, t_{n-1}^{(1)} \,\|\, t_n^{(1)} \,\|\, t_{n+1}^{(1)} \right] = \left\{0 \,\|\| \, [a_2^{(1)} - t_2^{(1)}] \bmod m_2 \,\|\right.$ $\|\, [a_3^{(1)} - t_3^{(1)}] \bmod m_3 \,\|\| \ldots \,\|\| \, [a_{i-1}^{(1)} - t_{i-1}^{(1)}] \bmod m_{i-1} \,\|\, [a_i^{(1)} - t_i^{(1)}] \bmod m_i \,\|\|$ $\|\, [a_{i+1}^{(1)} - t_{i+1}^{(1)}] \bmod m_{i+1} \,\|\| \ldots \,\|\| \, [a_{n-3}^{(1)} - t_{n-3}^{(1)}] \bmod m_{n-3} \,\|\, [a_{n-2}^{(1)} - t_{n-2}^{(1)}] \bmod m_{n-2} \,\|\|$ $\|\, [a_{n-1}^{(1)} - t_{n-1}^{(1)}] \bmod m_{n-1} \,\|\, [a_n^{(1)} - t_n^{(1)}] \bmod m_n \,\|\, [a_{n+1}^{(1)} - t_{n+1}^{(1)}] \bmod m_{n+1} \right\} =$ $= [0 \,\|\, 0 \,\|\, a_3^{(2)} \,\|\| \ldots \,\|\, a_{i-1}^{(2)} \,\|\, a_i^{(2)} \,\|\, a_{i+1}^{(2)} \,\|\| \ldots \,\|\, a_{n-3}^{(2)} \,\|\, a_{n-2}^{(2)} \,\|\, a_{n-1}^{(2)} \,\|\, a_n^{(2)} \,\|\, a_{n+1}^{(2)}]$.

Fig. 1 (continuation)

5	Referencing residue value $a_3^{(2)}$ of number $A^{(2)} = [0 \,\|\| \, 0 \,\|\| \, a_3^{(2)} \,\|\| \ldots$ $\ldots \|\| \, a_{i-1}^{(2)} \,\|\| \, a_i^{(2)} \,\|\| \, a_{i+1}^{(2)} \,\|\| \ldots \|\| \, a_{n-3}^{(2)} \,\|\| \, a_{n-2}^{(2)} \,\|\| \, a_{n-1}^{(2)} \,\|\| \, a_n^{(2)} \,\|\| \, a_{n+1}^{(2)}]$ in NCB_2 via nullification constant $NC^{(2)} = [0 \,\|\| \, 0 \,\|\| \, t_3^{(2)} \,\|\| \ldots \|\| \, t_{i-1}^{(2)} \,\|\| \, t_i^{(2)} \,\|\| \, t_{i+1}^{(2)} \,\|\| \ldots \|\| \, t_{n-3}^{(2)} \,\|\| \, t_{n-2}^{(2)} \,\|\| \, t_{n-1}^{(2)} \,\|\|$ $\|\| \, t_n^{(2)} \,\|\| \, t_{n+1}^{(2)}]$; $t_3^{(2)} = a_3^{(2)}$; $t_3^{(2)} = \overline{0, m_3 - 1}$.
6	Executing subtraction operation $A^{(3)} = A^{(2)} - NC^{(2)} = [0 \,\|\| \, 0 \,\|\| \, a_3^{(2)} \,\|\| \ldots$ $\ldots \|\| \, a_{i-1}^{(2)} \,\|\| \, a_i^{(2)} \,\|\| \, a_{i+1}^{(2)} \,\|\| \ldots \|\| \, a_{n-3}^{(2)} \,\|\| \, a_{n-2}^{(2)} \,\|\| \, a_{n-1}^{(2)} \,\|\| \, a_n^{(2)} \,\|\| \, a_{n+1}^{(2)}] - [0 \,\|\| \, 0 \,\|\| \, t_3^{(2)} \,\|\| \ldots \|\| \, t_{i-1}^{(2)} \,\|\|$ $\|\| \, t_i^{(2)} \,\|\| \, t_{i+1}^{(2)} \,\|\| \ldots \|\| \, t_{n-3}^{(2)} \,\|\| \, t_{n-2}^{(2)} \,\|\| \, t_{n-1}^{(2)} \,\|\| \, t_n^{(2)} \,\|\| \, t_{n+1}^{(2)}] = \{0 \,\|\| \, 0 \,\|\| [a_3^{(2)} - t_3^{(2)}] \bmod m_3 \,\|\| \ldots$ $\ldots \|\| \, [a_{i-1}^{(2)} - t_{i-1}^{(2)}] \bmod m_{i-1} \,\|\| \, [a_i^{(2)} - t_i^{(2)}] \bmod m_i \,\|\| \, [a_{i+1}^{(2)} - t_{i+1}^{(2)}] \bmod m_{i+1} \,\|\| \ldots$ $\ldots \|\| \, [a_{n-3}^{(2)} - t_{n-3}^{(2)}] \bmod m_{n-3} \,\|\| \, [a_{n-2}^{(2)} - t_{n-2}^{(2)}] \bmod m_{n-2} \,\|\| \, [a_{n-1}^{(2)} - t_{n-1}^{(2)}] \bmod m_{n-1} \,\|\|$ $\|\| \, [a_n^{(2)} - t_n^{(2)}] \bmod m_n \,\|\| \, [a_{n+1}^{(2)} - t_{n+1}^{(2)}] \bmod m_{n+1}\} =$ $= [0 \,\|\| \, 0 \,\|\| \, 0 \,\|\| \, a_4^{(3)} \,\|\| \, a_5^{(3)} \,\|\| \ldots \|\| \, a_{i-1}^{(3)} \,\|\| \, a_i^{(3)} \,\|\| \, a_{i+1}^{(3)} \,\|\| \ldots \|\| \, a_{n-3}^{(3)} \,\|\| \, a_{n-2}^{(3)} \,\|\| \, a_{n-1}^{(3)} \,\|\| \, a_n^{(3)} \,\|\| \, a_{n+1}^{(3)}]$.

Fig. 1 (continuation)

7	Referencing residue value $a_4^{(3)}$ of number $A^{(3)} = [0 \,\|\|\, 0 \,\|\|\, 0 \,\|\|\, a_4^{(3)} \,\|\|$ $\|\| \, a_5^{(3)} \,\|\| \ldots \|\| \, a_{i-1}^{(3)} \,\|\| \, a_i^{(3)} \,\|\| \, a_{i+1}^{(3)} \,\|\| \ldots \|\| \, a_{n-3}^{(3)} \,\|\| \, a_{n-2}^{(3)} \,\|\| \, a_{n-1}^{(3)} \,\|\| \, a_n^{(3)} \,\|\| \, a_{n+1}^{(3)}]$ in NCB_3 via nullification constant $NC^{(3)} = [0 \,\|\|\, 0 \,\|\|\, 0 \,\|\|\, t_4^{(3)} \,\|\| \, t_5^{(3)} \,\|\| \ldots \|\| \, t_{i-1}^{(3)} \,\|\| \, t_i^{(3)} \,\|\| \, t_{i+1}^{(3)} \,\|\| \ldots$ $\|\| \, t_{n-3}^{(3)} \,\|\| \, t_{n-2}^{(3)} \,\|\| \, t_{n-1}^{(3)} \,\|\| \, t_n^{(3)} \,\|\| \, t_{n+1}^{(3)}]$; $t_4^{(3)} = a_4^{(3)}$; $t_4^{(3)} = \overline{0, m_4 - 1}$.
8	Executing subtraction operation $A^{(4)} = A^{(3)} - NC^{(3)} = [0 \,\|\|\, 0 \,\|\|\, 0 \,\|\|\, a_4^{(3)} \,\|\|$ $\|\| \, a_5^{(3)} \,\|\| \ldots \|\| \, a_{i-1}^{(3)} \,\|\| \, a_i^{(3)} \,\|\| \, a_{i+1}^{(3)} \,\|\| \ldots \|\| \, a_{n-3}^{(3)} \,\|\| \, a_{n-2}^{(3)} \,\|\| \, a_{n-1}^{(3)} \,\|\| \, a_n^{(3)} \,\|\| \, a_{n+1}^{(3)}] - [0 \,\|\|\, 0 \,\|\|\, 0 \,\|\|\, t_4^{(3)} \,\|\|$ $\|\| \, t_5^{(3)} \,\|\| \ldots \|\| \, t_{i-1}^{(3)} \,\|\| \, t_i^{(3)} \,\|\| \, t_{i+1}^{(3)} \,\|\| \ldots \|\| \, t_{n-3}^{(3)} \,\|\| \, t_{n-2}^{(3)} \,\|\| \, t_{n-1}^{(3)} \,\|\| \, t_n^{(3)} \,\|\| \, t_{n+1}^{(3)}] =$ $= \{0 \,\|\|\, 0 \,\|\|\, 0 \,\|\| \, [a_4^{(3)} - t_4^{(3)}] \bmod m_4 \,\|\| \, [a_5^{(3)} - t_5^{(3)}] \bmod m_5 \,\|\| \ldots \|\| \, [a_{i-1}^{(3)} - t_{i-1}^{(3)}] \bmod m_{i-1} \,\|\|$ $\|\| \, [a_i^{(3)} - t_i^{(3)}] \bmod m_i \,\|\| \, [a_{i+1}^{(3)} - t_{i+1}^{(3)}] \bmod m_{i+1} \,\|\| \ldots \|\| \, [a_{n-3}^{(3)} - t_{n-3}^{(3)}] \bmod m_{n-3} \,\|\|$ $\|\| \, [a_{n-2}^{(3)} - t_{n-2}^{(3)}] \bmod m_{n-2} \,\|\| \, [a_{n-1}^{(3)} - t_{n-1}^{(3)}] \bmod m_{n-1} \,\|\| \, [a_n^{(3)} - t_n^{(3)}] \bmod m_n \,\|\|$ $\|\| \, [a_{n+1}^{(3)} - t_{n+1}^{(3)}] \bmod m_{n+1} \} = [0 \,\|\|\, 0 \,\|\|\, 0 \,\|\|\, a_5^{(4)} \,\|\| \ldots \|\| \, a_{i-1}^{(4)} \,\|\| \, a_i^{(4)} \,\|\| \, a_{i+1}^{(4)} \,\|\| \ldots$ $\ldots \|\| \, a_{n-3}^{(4)} \,\|\| \, a_{n-2}^{(4)} \,\|\| \, a_{n-1}^{(4)} \,\|\| \, a_n^{(4)} \,\|\| \, a_{n+1}^{(4)}]$.

Fig. 1 (continuation)

For a value of $A^{(i)}$	Referencing residue value $a_i^{(i-1)}$ of number $A^{(i-1)} = [0 \,\|\|\, 0 \,\|\|\, 0 \,\|\| \ldots \|\| \, 0 \,\|\|$ $\|\| \, a_i^{(i-1)} \,\|\| \, a_{i+1}^{(i-1)} \,\|\| \ldots \|\| \, a_{n-3}^{(i-1)} \,\|\| \, a_{n-2}^{(i-1)} \,\|\| \, a_{n-1}^{(i-1)} \,\|\| \, a_n^{(i-1)} \,\|\| \, a_{n+1}^{(i-1)}]$ in NCB_{i-1} via nullification constant $NC^{(i-1)} = [0 \,\|\|\, 0 \,\|\|\, 0 \,\|\| \ldots \|\| \, 0 \,\|\| \, t_i^{(i-1)} \,\|\| \, t_{i+1}^{(i-1)} \,\|\| \ldots \|\| \, t_{n-3}^{(i-1)} \,\|\| \, t_{n-2}^{(i-1)} \,\|\| \, t_{n-1}^{(i-1)} \,\|\| \, t_n^{(i-1)} \,\|\| \, t_{n+1}^{(i-1)}]$; $t_i^{(i-1)} = a_i^{(i-1)}$; $t_i^{(i-1)} = \overline{0, m_i - 1}$. Executing subtraction operation $A^{(i)} = A^{(i-1)} - NC^{(i-1)} = [0 \,\|\, 0 \,\|\, 0 \,\|\| \ldots$ $\ldots \|\| \, 0 \,\|\| \, a_i^{(i-1)} \,\|\| \, a_{i+1}^{(i-1)} \,\|\| \ldots \|\| \, a_{n-3}^{(i-1)} \,\|\| \, a_{n-2}^{(i-1)} \,\|\| \, a_{n-1}^{(i-1)} \,\|\| \, a_n^{(i-1)} \,\|\| \, a_{n+1}^{(i-1)}] - [0 \,\|\, 0 \,\|\, 0 \,\|\| \, 0 \,\|\| \ldots \|\| \, 0 \,\|\|$ $\|\| \, t_i^{(i-1)} \,\|\| \, t_{i+1}^{(i-1)} \,\|\| \ldots \|\| \, t_{n-3}^{(i-1)} \,\|\| \, t_{n-2}^{(i-1)} \,\|\| \, t_{n-1}^{(i-1)} \,\|\| \, t_n^{(i-1)} \,\|\| \, t_{n+1}^{(i-1)}] = \{0 \,\|\, 0 \,\|\, 0 \,\|\| \, 0 \,\|\| \ldots \|\| \, 0 \,\|\|$ $\|\| [a_i^{(i-1)} - t_i^{(i-1)}] \bmod m_i \,\|\| [a_{i+1}^{(i-1)} - t_{i+1}^{(i-1)}] \bmod m_{i+1} \,\|\| \ldots \|\| [a_{n-3}^{(i-1)} - t_{n-3}^{(i-1)}] \bmod m_{n-3} \,\|\|$ $\|\| [a_{n-2}^{(i-1)} - t_{n-2}^{(i-1)}] \bmod m_{n-2} \,\|\| [a_{n-1}^{(i-1)} - t_{n-1}^{(i-1)}] \bmod m_{n-1} \,\|\| [a_n^{(i-1)} - t_n^{(i-1)}] \bmod m_n \,\|\|$ $\|\| [a_{n+1}^{(i-1)} - t_{n+1}^{(i-1)}] \bmod m_{n+1} \} = [0 \,\|\, 0 \,\|\, 0 \,\|\| \ldots \|\| \, 0 \,\|\| \, 0 \,\|\| \, a_{i+1}^{(i)} \,\|\| \ldots \|\| \, a_{n-3}^{(i)} \,\|\| \, a_{n-2}^{(i)} \,\|\| \, a_{n-1}^{(i)} \,\|\|$ $\|\| \, a_n^{(i)} \,\|\| \, a_{n+1}^{(i)}]$.
$2n-3$	Referencing residue value $a_{n-1}^{(n-2)}$ and number $A^{(n-2)} = [0 \,\|\, 0 \,\|\, 0 \,\|\| \ldots$ $\ldots \|\| \, 0 \,\|\| \, 0 \,\|\| \ldots \|\| \, 0 \,\|\| \, a_{n-1}^{(n-2)} \,\|\| \, a_n^{(n-2)} \,\|\| \, a_{n+1}^{(n-2)}]$ in NCB_{n-2} via nullification constant $NC^{(n-2)} = [0 \,\|\, 0 \,\|\, 0 \,\|\| \ldots \|\| \, 0 \,\|\| \, 0 \,\|\| \ldots \|\| \, 0 \,\|\| \, 0 \,\|\| \, t_{n-1}^{(n-2)} \,\|\| \, t_n^{(n-2)} \,\|\|$ $\|\| \, t_{n+1}^{(n-2)}]$; $t_{n-1}^{(n-2)} = a_{n-1}^{(n-2)}$; $t_{n-1}^{(n-2)} = \overline{0, m_{n-1} - 1}$.

Fig. 1 (continuation)

$2n-2$	Executing subtraction operation $A^{(n-1)} = A^{(n-2)} - NC^{(n-2)} = [0 \| 0 \| 0 \| 0 \| \dots$ $\dots \| 0 \| 0 \| 0 \| \dots \| 0 \| 0 \| 0 \| a_{n-1}^{(n-2)} \| a_n^{(n-2)} \| a_{n+1}^{(n-2)}] - [0 \| 0 \| 0 \| 0 \| \dots \| 0 \| 0 \| 0 \| 0 \| \dots$ $\dots \| 0 \| 0 \| 0 \| t_{n-1}^{(n-2)} \| t_n^{(n-2)} \| t_{n+1}^{(n-2)}] = \{0 \| 0 \| 0 \| 0 \| \dots \| 0 \| 0 \| 0 \| 0 \| \dots \| 0 \| 0 \| 0 \| 0 \|$ $\| [a_{n-1}^{(n-2)} - t_{n-1}^{(n-2)}] \bmod m_{n-1} \| [a_n^{(n-2)} - t_n^{(n-2)}] \bmod m_n \|$ $\| [a_{n+1}^{(n-2)} - t_{n+1}^{(n-2)}] \bmod m_{n+1} \} = [0 \| 0 \| 0 \| 0 \| \dots \| 0 \| 0 \| 0 \| 0 \| \dots \| 0 \| 0 \| 0 \| 0 \| a_n^{(n-1)} \| a_{n+1}^{(n-1)}].$
$2n-1$	Referencing residue value $a_n^{(n-1)}$ of number $A^{(n-1)} = [0 \| 0 \| 0 \| 0 \| \dots$ $\dots \| 0 \| 0 \| 0 \| \dots \| 0 \| 0 \| 0 \| 0 \| a_n^{(n-1)} \| a_{n+1}^{(n-1)}]$ in NCB_{n-1} via nullification constant $NC^{(n-1)} = [0 \| 0 \| 0 \| 0 \| \dots \| 0 \| 0 \| 0 \| 0 \| \dots \| 0 \| 0 \| 0 \| 0 \| \| t_n^{(n-1)} \| t_{n+1}^{(n-1)}]$; $t_n^{(n-1)} = a_n^{(n-1)}$; $t_n^{(n-1)} = \overline{0,\, m_n - 1}$.
$2n$	Getting the nullified number $A^{(N)} = A^{(n)} = A^{(n-1)} - NC^{(n-1)} =$ $= [0 \| 0 \| 0 \| 0 \| \dots \| 0 \| 0 \| 0 \| 0 \| \dots \| 0 \| 0 \| 0 \| 0 \| 0 \| a_n^{(n-1)} \| a_{n+1}^{(n-1)}] - [0 \| 0 \| 0 \| 0 \| \dots \| 0 \| 0 \| 0 \| 0 \| \dots$ $\dots \| 0 \| 0 \| 0 \| 0 \| t_n^{(n-1)} \| t_{n+1}^{(n-1)}] = \{0 \| 0 \| 0 \| 0 \| \dots \| 0 \| 0 \| 0 \| 0 \| \dots \| 0 \| 0 \| 0 \| 0 \|$ $\| [a_n^{(n-1)} - t_n^{(n-1)}] \bmod m_n \| [a_{n+1}^{(n-1)} - t_{n+1}^{(n-1)}] \bmod m_{n+1} \} = [0 \| 0 \| 0 \| 0 \| \dots \| 0 \| 0 \| 0 \| 0 \| \dots$ $\dots \| 0 \| 0 \| 0 \| 0 \| 0 \| a_{n+1}^{(n)}]$, where $a_{n+1}^{(n)} = \gamma_{n+1}$.
	$T_{N1} = 2 \cdot n \cdot \tau_{snbr}$

Fig. 1 (continuation)

Declaring time of NC extraction from the corresponding nullification constant block (NCB) in computer systems and components of integral data computation (CSCIDC), that compute in RNS, as t_1, and a time for subtracting $A^{(i-1)}$ from $NC^{(i-1)}$, i.e. performing operation $A^{(i)} = A^{(i-1)} - \mathrm{NC}^{(i-1)} -$ as t_2, we'll get overall time to be T_{N1} for executing nullification procedure for the first N1 method.

$$T_{N1} = n\,(t_1 + t_2). \tag{3}$$

When nullification block (NB) is implemented as a table, can be assumed that in practice $t_1 = t_2 = \tau_{subtr}$. In this case for the nullification procedure the nullification time is equal to $T_{N1} = 2n\tau_{subtr}$, where: τ_{subtr} – time for subtracting $A^{(i)}$ from nullification constant $NC^{(i)}$; n – the amount of information RNS bases. Beside that, in order to implement nullification procedure using first method N1 nullification block must be storing

$$K_{N1} = \sum_{i=1}^{n} m_i - n$$

of nullification constants. In this case the amount N_{N1} of nullification constants' binary bits, that in turn defines the scale of equipment (capacity) for NCB of computer system, is described using expression

$$N_{N1} = \left(\sum_{i+1}^{n} m_i - 1 \right)(n-i)\,.$$

Apparently, the reviewed basic nullification procedure does not deplete the capability to increase processing speed of nullification procedure of numbers, because the execution of subtraction operation $A^{(i+1)} = A^{(i)} - NC^{(i)}$ and the extraction of the following nullification constant (NC) are separated in time. This was dictated by the fact, that while the subtraction operation is not finished, the residue value is unknown,

which will be later used to pick NC for the next stage of nullification procedure [1-3].

2 Parallel subtraction method

Essentially, the introduced method is based on parallel execution of nullification procedure for two residues. For n – even number we get $a_i^{(i-1)}$, $a_{n-i+1}^{(i-1)}$ ($i=\overline{1,n/2}$), specifically $a_1^{(0)}$, $a_n^{(0)}$; $a_2^{(1)}$, $a_{n-1}^{(1)}$; $a_3^{(2)}$, $a_{n-2}^{(2)}$;… $a_{n/2}^{(n/2)}$, $a_{n/2+1}^{(n/2)}$ (fig. 2). For n – odd number we get $a_1^{(0)}$, $a_n^{(0)}$; $a_2^{(1)}$, $a_{n-1}^{(1)}$; $a_3^{(2)}$, $a_{n-2}^{(2)}$; … $a_{(n+1)/2}^{((n+1)/2-1)}$ (fig. 3). In this case for the arbitrary of i the NC for the corresponding number appears as

$$A^{(i)}=[\overbrace{0\|0\|\ldots\|0}^{i-\text{zeros}}\|a_{i+1}^{(i)}\|a_{i+2}^{(i)}\|\ldots\|a_{n-i-1}^{(i)}\|a_{n-i}^{(i)}\|\overbrace{0\|\ldots\|0\|0}^{i-\text{zeros}}\|a_{n+1}^{(i)}],$$

$$NC^{(i)}=[0\|0\|\ldots\|0\|t_{i+1}^{(i)}\|t_{i+2}^{(i)}\|\ldots\|t_{n-i-1}^{(i)}\|t_{n-i}^{(i)}\|0\|\ldots\|0\|0\|t_{n+1}^{(i)}];$$

$$t_{i+1}^{(i)}=\overline{0,m_{i+1}},\ t_{n-i}^{(i)}=\overline{0,m_{n-i}};\ t_{i+1}^{(i)}=a_{i+1}^{(i)},\ t_{n-i}^{(i)}=a_{n-i}^{(i)}.$$

For the arbitrary value of i we get

$$A^{(i+1)}=A^{(i)}-NC^{(i)}=$$

$$=[0\|0\|\ldots\|0\|a_{i+1}^{(i)}\|a_{i+2}^{(i)}\|a_{i+3}^{(i)}\|\ldots\|a_{n-i-2}^{(i)}\|a_{n-i-1}^{(i)}\|a_{n-i}^{(i)}\|0\|\ldots\|0\|a_{n+1}^{(i)}]-$$

$$-[0\|0\|\ldots\|0\|t_{i+1}^{(i)}\|t_{i+2}^{(i)}\|t_{i+3}^{(i)}\|\ldots\|t_{n-i-2}^{(i)}\|t_{n-i-1}^{(i)}\|t_{n-1}^{(i)}\|0\|\ldots\|0\|t_{n+1}^{(i)}]=$$

$$=\{0\|0\|\ldots\|0\|[a_{i+1}^{(i)}-t_{i+1}^{(i)}]\bmod m_{i+1}\|[a_{i+2}^{(i)}-t_{i+2}^{(i)}]\bmod m_{i+2}\|[a_{i+3}^{(i)}-t_{i+3}^{(i)}]\bmod m_{i+3}\|\ldots$$

$$\ldots\|[a_{n-i-2}^{(i)}-t_{n-i-2}^{(i)}]\bmod m_{n-i-2}\|[a_{n-i-1}^{(i)}-t_{n-i-1}^{(i)}]\bmod m_{n-i-1}\|$$

$$\|[a_{n-i}^{(i)}-t_{n-i}^{(i)}]\bmod m_{n-i}\|0\|\ldots\|0\|[a_{n+1}^{(i)}-t_{n+1}^{(i)}]\bmod m_{n+1}\}=$$

$$=[0\|0\|\ldots\|0\|0\|a_{i+2}^{(i+1)}\|a_{i+3}^{(i+1)}\|\ldots\|a_{n-i-2}^{(i+1)}\|a_{n-i-1}^{(i+1)}\|0\|0\|\ldots\|0\|0\|a_{n+1}^{(i+1)}].$$

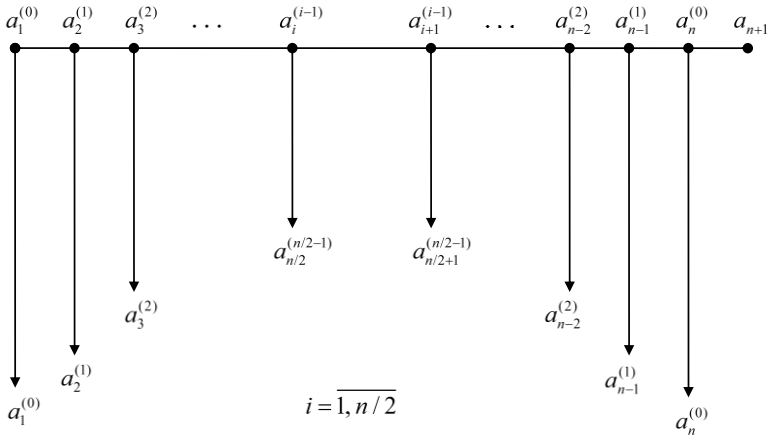

Fig. 2. – Nullification constants extraction diagram for the parallel subtraction (PS) method (*n* is an even number)

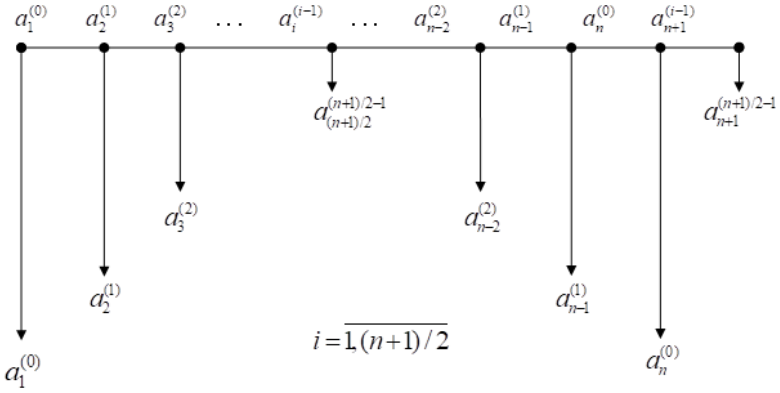

Fig. 3. – Nullification constants extraction diagram for the PS method (*n* is an odd number)

The algorithm for the PSM execution is shown in the Table 2.

Before calculating the values $\gamma_{n+1} = a_{n+1}^{(n/2)}$ for *n* (even number) we get

$$A^{(n/2-1)} = [\overbrace{0 \| 0 \| \ldots \| 0}^{n/2-1\text{zeros}} \| a_{n/2}^{(n/2-1)} \| a_{n/2+1}^{(n/2-1)} \| \overbrace{0 \| \ldots \| 0 \| 0}^{n/2-1\text{zeros}} \| a_{n+1}^{(n/2-1)}].$$

$$NC^{(n/2-1)} = [\overbrace{0 \| 0 \| \ldots \| 0}^{n/2-1\text{zeros}} | t_{n/2}^{(n/2-1)} \| t_{n/2+1}^{(n/2-1)} \| \overbrace{0 \| \ldots \| 0 \| 0}^{n/2-1\text{zeros}} \| t_{n+1}^{(n/2-1)}],$$

$$t_{n/2}^{(n/2-1)} = \overline{0, m_{n/2}},\ t_{n/2+1}^{(n/2-1)} = \overline{0, m_{n/2+1}},\ t_{n/2}^{(n/2-1)} = a_{n/2}^{(n/2-1)},\ t_{n/2+1}^{(n/2-1)} = a_{n/2+1}^{(n/2-1)}.$$

$$A^{(N)} = A^{(n/2)} = A^{(n/2-1)} - NC^{(n/2-1)} = \left\{0 \| 0 \| \ldots \| 0 \| \left[a_{n/2}^{(n/2-1)} - t_{n/2}^{(n/2-1)}\right] \bmod m_{n/2} \| \right.$$

$$\left. \| \left[a_{n/2+1}^{(n/2-1)} - t_{n/2+1}^{(n/2-1)}\right] \bmod m_{n/2+1} \| 0 \| 0 \| \ldots \| 0 \| 0 \| \left[a_{n+1}^{(n/2-1)} - t_{n+1}^{(n/2-1)}\right] \bmod m_{n+1} \right\} =$$

$$= \left[0 \| 0 \| \ldots \| 0 \| 0 \| 0 \| \ldots \| 0 \| 0 \| 0 \| a_{n+1}^{(n/2)}\right], \text{ where } \gamma_{n+1} = a_{n+1}^{(n/2)}.$$

Before calculating the values $\gamma_{n+1} = a_{n+1}^{(n/2)}$ for n (odd number), we get

$$A^{((n+1)/2-1)} = [\overbrace{0 \| 0 \| \ldots \| 0}^{\frac{n+1}{2}-1\text{ zeros}} \| a_{(n+1)/2}^{((n+1)/2-1)} \overbrace{\| 0 \| \ldots \| 0}^{\frac{n+1}{2}-1\text{ zeros}} \| a_{n+1}^{((n+1)/2-1)}].$$

$$NC^{((n+1)/2-1)} = [0 \| 0 \| \ldots \| 0 \| t_{(n+1)/2}^{((n+1)/2-1)} \| 0 \| \ldots \| 0 \| t_{n+1}^{((n+1)/2-1)}],$$

$$t_{(n+1)/2}^{((n+1)/2-1)} = \overline{0, m_{(n+1)/2}};\ t_{(n+1)/2}^{((n+1)/2-1)} = a_{(n+1)/2}^{((n+1)/2-1)}.$$

$$A^{(N)} = A^{(n+1)/2} = A^{((n+1)/2-1)} - NC^{((n+1)/2-1)} =$$

$$= \left\{0 \| 0 \| \ldots \| 0 \| \left[a_{(n+1)/2}^{((n+1)/2-1)} - t_{(n+1)/2}^{((n+1)/2-1)}\right] \bmod m_{(n+1)/2} \| 0 \| ... 0 \| 0 \| \ldots \| 0 \| 0 \| \right.$$

$$\left. \| \left[a_{n+1}^{((n+1)/2-1)} - t_{n+1}^{((n+1)/2-1)}\right] \bmod m_{n+1} \right\} = \left[0 \| 0 \| \ldots \| 0 \| \ldots \| 0 \| 0 \| a_{n+1}^{(n+1)/2}\right], \text{ where}$$

$$\gamma_{n+1} = a_{n+1}^{(n+1)/2}.$$

The method of parallel subtraction in RNS is shown in the Fig. 4

Table 2 – PS algorithm

Operation №	Operation content
1	Referencing residue values $a_1^{(0)}$ and $a_n^{(0)}$ of number $A^{(0)}$ in NCB_0 via $NC^{(0)}$.
2	Executing subtraction operation $A^{(1)} = A^{(0)} - NC^{(0)}$.
3	Referencing residue values $a_2^{(1)}$ and $a_{n-1}^{(1)}$ of number $A^{(1)}$ in NCB_1 via $NC^{(1)}$.
4	Executing subtraction operation $A^{(2)} = A^{(1)} - NC^{(1)}$.
5	Referencing residue values $a_2^{(2)}$ and $a_{n-2}^{(2)}$ of number $A^{(2)}$ in NCB_2 via $NC^{(2)}$.
6	Executing subtraction operation $A^{(3)} = A^{(2)} - NC^{(2)}$.
…	…
i	Executing subtraction operation $A^{(i)} = A^{(i-1)} - NC^{(i-1)}$.
$i+1$	Referencing residue values $a_{i+1}^{(i)}$ and $a_{n-i}^{(i)}$ of number $A^{(i)}$ in NCB_i via $NC^{(i)}$.
$i+2$	Executing subtraction operation $A^{(i+1)} = A^{(i)} - NC^{(i)}$.
…	…
$n-3$	Referencing residue values $a_{n/2-1}^{(n/2-2)}$ and $a_{n/2+2}^{(n/2-2)}$ of number $A^{(n/2-2)}$ in $NCB_{n/2-2}$ via $NC^{(n/2-2)}$.
$n-2$	Executing subtraction operation $A^{(n/2-1)} = A^{(n/2-2)} - NC^{(n/2-2)}$.
$n-1$	Referencing residue values $a_{n/2}^{(n/2-1)}$ and $a_{n/2+1}^{(n/2-1)}$ of number $A^{(n/2-1)}$ in $NCB_{n/2-1}$ via $NC^{(n/2-1)}$.
n	Executing subtraction operation $A^{(n/2)} = A^{(n/2-1)} - NC^{(n/2-1)}$. Getting mollified number $A^{(N)}$ $A^{(N)} = A^{(n/2)} = [0 \,\|\|\, 0 \,\|\| \ldots \|\| \, 0 \,\|\| \ldots \|\| \, 0 \,\|\| \, 0 \,\|\| \, \gamma_{n+1} = a_{n+1}^{(n/2)}]$.

Operation № (cycle)	Operation content
1	Referencing residue values $a_1^{(0)}$ and $a_n^{(0)}$ of number $A = A^{(0)}$ in NCB_0 via nullification constant $NC^{(0)} = [t_1^{(0)} \| t_2^{(0)} \| t_3^{(0)} \| \dots \| t_{i-1}^{(0)} \| t_i^{(0)} \| t_{i+1}^{(0)} \| \dots$ $\dots \| t_{n-3}^{(0)} \| t_{n-2}^{(0)} \| t_{n-1}^{(0)} \| t_n^{(0)} \| t_{n+1}^{(0)}]$; $t_1^{(0)} = a_1^{(0)}$, $t_n^{(0)} = a_n^{(0)}$; $t_1^{(0)} = \overline{0, m_1 - 1}$, $t_n^{(0)} = \overline{0, m_n - 1}$
2	Executing subtraction operation $A^{(1)} = A^{(0)} - NC^{(0)} = [a_1^{(0)} \| a_2^{(0)} \|$ $\| a_3^{(0)} \| \dots \| a_{i-1}^{(0)} \| a_i^{(0)} \| a_{i+1}^{(0)} \| \dots \| a_{n-3}^{(0)} \| a_{n-2}^{(0)} \| a_{n-1}^{(0)} \| a_n^{(0)} \| a_{n+1}^{(0)}] - [t_1^{(0)} \| t_2^{(0)} \|$ $\| t_3^{(0)} \| \dots \| t_{i-1}^{(0)} \| t_i^{(0)} \| t_{i+1}^{(0)} \| \dots \| t_{n-3}^{(0)} \| t_{n-2}^{(0)} \| t_{n-1}^{(0)} \| t_n^{(0)} \| t_{n+1}^{(0)}] =$ $= \{[a_1^{(0)} - t_1^{(0)}] \bmod m_1 \| [a_2^{(0)} - t_2^{(0)}] \bmod m_2 \| [a_3^{(0)} - t_3^{(0)}] \bmod m_3 \| \dots$ $\dots \| [a_{i-1}^{(0)} - t_{i-1}^{(0)}] \bmod m_{i-1} \| [a_i^{(0)} - t_i^{(0)}] \bmod m_i \| [a_{i+1}^{(0)} - t_{i+1}^{(0)}] \bmod m_{i+1} \| \dots$ $\dots \| [a_{n-3}^{(0)} - t_{n-3}^{(0)}] \bmod m_{n-3} \| [a_{n-2}^{(0)} - t_{n-2}^{(0)}] \bmod m_{n-2} \| [a_{n-1}^{(0)} - t_{n-1}^{(0)}] \bmod m_{n-1} \| \dots$ $\dots \| [a_n^{(0)} - t_n^{(0)}] \bmod m_n \| [a_{n+1}^{(0)} - t_{n+1}^{(0)}] \bmod m_{n+1}\} = [0 \| a_2^{(1)} \| a_3^{(1)} \| \dots$ $\dots \| a_{i-1}^{(1)} \| a_i^{(1)} \| a_{i+1}^{(1)} \| \dots \| a_{n-3}^{(1)} \| a_{n-2}^{(1)} \| a_{n-1}^{(1)} \| 0 \| a_{n+1}^{(1)}]$.

Fig. 4. – Parallel nullification method in RNS

3	Referencing residue values $a_2^{(1)}$ and $a_{n-1}^{(1)}$ of number $A^{(1)}$ in NCB_1 via nullification constant $NC^{(1)} = [0 \,\|\| \, t_2^{(1)} \,\|\| \, t_3^{(1)} \,\|\| \ldots \,\|\| \, t_{i-1}^{(1)} \,\|\| \, t_i^{(1)} \,\|\| \, t_{i+1}^{(1)} \,\|\| \ldots$ $\ldots \,\|\| \, t_{n-3}^{(1)} \,\|\| \, t_{n-2}^{(1)} \,\|\| \, t_{n-1}^{(1)} \,\|\| \, 0 \,\|\| \, t_{n+1}^{(1)}]$; $t_2^{(1)} = a_2^{(1)}$, $t_{n-1}^{(1)} = a_{n-1}^{(1)}$; $t_2^{(1)} = \overline{0, m_2 - 1}$, $t_{n-1}^{(1)} = \overline{0, m_{n-1} - 1}$.
4	Executing subtraction operation $A^{(2)} = A^{(1)} - NC^{(1)} = [0 \,\|\| \, a_2^{(1)} \,\|\|$ $\|\| \, a_3^{(1)} \,\|\| \ldots \,\|\| \, a_{i-1}^{(1)} \,\|\| \, a_i^{(1)} \,\|\| \, a_{i+1}^{(1)} \,\|\| \ldots \,\|\| \, a_{n-3}^{(1)} \,\|\| \, a_{n-2}^{(1)} \,\|\| \, a_{n-1}^{(1)} \,\|\| \, 0 \,\|\| \, a_{n+1}^{(1)}] - [0 \,\|\| \, t_2^{(1)} \,\|\| \, t_3^{(1)} \,\|\| \ldots$ $\ldots \,\|\| \, t_{i-1}^{(1)} \,\|\| \, t_i^{(1)} \,\|\| \, t_{i+1}^{(1)} \,\|\| \ldots \,\|\| \, t_{n-3}^{(1)} \,\|\| \, t_{n-2}^{(1)} \,\|\| \, t_{n-1}^{(1)} \,\|\| \, 0 \,\|\| \, t_{n+1}^{(1)}] = \{0 \,\|\| \, [a_2^{(1)} - t_2^{(1)}] \bmod m_2 \,\|\|$ $\|\| \, [a_3^{(1)} - t_3^{(1)}] \bmod m_3 \,\|\| \, [a_4^{(1)} - t_4^{(1)}] \bmod m_4 \,\|\| \ldots \,\|\| \, [a_{i-1}^{(1)} - t_{i-1}^{(1)}] \bmod m_{i-1} \,\|\|$ $\|\| \, [a_i^{(1)} - t_i^{(1)}] \bmod m_i \,\|\| \, [a_{i+1}^{(1)} - t_{i+1}^{(1)}] \bmod m_{i+1} \,\|\| \ldots \,\|\| \, [a_{n-3}^{(1)} - t_{n-3}^{(1)}] \bmod m_{n-3} \,\|\|$ $\|\| \, [a_{n-2}^{(1)} - t_{n-2}^{(1)}] \bmod m_{n-2} \,\|\| \, [a_{n-1}^{(1)} - t_{n-1}^{(1)}] \bmod m_{n-1} \,\|\| \, 0 \,\|\| \, [a_{n+1}^{(1)} - t_{n+1}^{(1)}] \bmod m_{n+1}\} =$ $= [0 \,\|\| \, 0 \,\|\| \, a_3^{(2)} \,\|\| \, a_4^{(2)} \,\|\| \ldots \,\|\| \, a_{i-1}^{(2)} \,\|\| \, a_i^{(2)} \,\|\| \, a_{i+1}^{(2)} \,\|\| \ldots \,\|\| \, a_{n-3}^{(2)} \,\|\| \, a_{n-2}^{(2)} \,\|\| \, 0 \,\|\| \, 0 \,\|\| \, a_{n+1}^{(2)}]$.
5	Referencing residue values $a_3^{(2)}$ and $a_{n-2}^{(2)}$ of number $A^{(2)} = [0 \,\|\| \, 0 \,\|\|$ $\|\| \, a_3^{(2)} \,\|\| \ldots \,\|\| \, a_{i-1}^{(2)} \,\|\| \, a_i^{(2)} \,\|\| \, a_{i+1}^{(2)} \,\|\| \ldots \,\|\| \, a_{n-3}^{(2)} \,\|\| \, a_{n-2}^{(2)} \,\|\| \, 0 \,\|\| \, 0 \,\|\| \, a_{n+1}^{(2)}]$ in NCB_2 via nullification constant $NC^{(2)} = [0 \,\|\| \, 0 \,\|\| \, t_3^{(2)} \,\|\| \ldots \,\|\| \, t_{i-1}^{(2)} \,\|\| \, t_i^{(2)} \,\|\| \, t_{i+1}^{(2)} \,\|\| \ldots \,\|\| \, t_{n-3}^{(2)} \,\|\| \, t_{n-2}^{(2)} \,\|\|$ $\|\| \, 0 \,\|\| \, 0 \,\|\| \, t_{n+1}^{(2)}]$, $t_3^{(2)} = a_3^{(2)}$, $t_{n-2}^{(2)} = a_{n-2}^{(2)}$; $t_3^{(2)} = \overline{0, m_3 - 1}$, $t_{n-2}^{(2)} = \overline{0, m_{n-2} - 1}$.

Fig. 4. (continuation)

	Executing subtraction operation $A^{(3)} = A^{(2)} - NC^{(2)} = [0 \,\|\| \, 0 \,\|\| \, a_3^{(2)} \,\|\| \dots$
	$\dots \,\|\| \, a_{i-1}^{(2)} \,\|\| \, a_i^{(2)} \,\|\| \, a_{i+1}^{(2)} \,\|\| \dots \,\|\| \, a_{n-3}^{(2)} \,\|\| \, a_{n-2}^{(2)} \,\|\| \, 0 \,\|\| \, 0 \,\|\| \, a_{n+1}^{(2)}] - [0 \,\|\| \, 0 \,\|\| \, t_3^{(2)} \,\|\| \dots \,\|\| \, t_{i-1}^{(2)} \,\|\| \, t_i^{(2)} \,\|\|$
	$\|\| \, t_{i+1}^{(2)} \,\|\| \dots \,\|\| \, t_{n-3}^{(2)} \,\|\| \, t_{n-2}^{(2)} \,\|\| \, 0 \,\|\| \, 0 \,\|\| \, t_{n+1}^{(2)}] = \{0 \,\|\| \, 0 \,\|\| [a_3^{(2)} - t_3^{(2)}] \bmod m_3 \,\|\|$
6	$\|\| [a_4^{(2)} - t_4^{(2)}] \bmod m_4 \,\|\| \dots \,\|\| [a_{i-1}^{(2)} - t_{i-1}^{(2)}] \bmod m_{i-1} \,\|\| [a_i^{(2)} - t_i^{(2)}] \bmod m_i \,\|\|$
	$\|\| [a_{i+1}^{(2)} - t_{i+1}^{(2)}] \bmod m_{i+1} \,\|\| \dots \,\|\| [a_{n-3}^{(2)} - t_{n-3}^{(2)}] \bmod m_{n-3} \,\|\| [a_{n-2}^{(2)} - t_{n-2}^{(2)}] \bmod m_{n-2} \,\|\|$
	$\|\| \, 0 \,\|\| \, 0 \,\|\| [a_{n+1}^{(2)} - t_{n+1}^{(2)}] \bmod m_{n+1} \} = [0 \,\|\| \, 0 \,\|\| \, 0 \,\|\| \, a_4^{(3)} \,\|\| \, a_5^{(2)} \,\|\| \dots \,\|\| \, a_{i-1}^{(3)} \,\|\| \, a_i^{(3)} \,\|\| \, a_{i+1}^{(3)} \,\|\| \dots$
	$\dots \,\|\| \, a_{n-4}^{(3)} \,\|\| \, a_{n-3}^{(3)} \,\|\| \, 0 \,\|\| \, 0 \,\|\| \, 0 \,\|\| \, a_{n+1}^{(3)}] .$
...	...

Fig. 4. (continuation)

For a value of $A^{(i)}$	Referencing residue values $a_i^{(i-1)}$ and $a_{n-i+1}^{(i-1)}$ of number $A^{(i-1)} = [0 \parallel \parallel 0 \parallel \ldots \parallel 0 \parallel a_i^{(i-1)} \parallel a_{i+1}^{(i-1)} \parallel a_{i+2}^{(i-1)} \parallel \ldots \parallel a_{n-i-3}^{(i-1)} \parallel a_{n-i}^{(i-1)} \parallel a_{n-i+1}^{(i-1)} \parallel 0 \parallel 0 \parallel \ldots \parallel 0 \parallel a_{n+1}^{(i-1)}]$ in NCB_{i-1} via nullification constant $NC^{(i-1)} = [0 \parallel 0 \parallel \ldots \parallel 0 \parallel \parallel t_i^{(i-1)} \parallel t_{i+1}^{(i-1)} \parallel t_{i+2}^{(i-1)} \parallel \ldots \parallel t_{n-i-1}^{(i-1)} \parallel t_{n-i}^{(i-1)} \parallel t_{n-i+1}^{(i-1)} \parallel 0 \parallel 0 \parallel \ldots \parallel 0 \parallel t_{n+1}^{(i-1)}]$; $t_i^{(i-1)} = a_i^{(i-1)}$, $t_{n-i+1}^{(i-1)} = a_{n-i+1}^{(i-1)}$; $t_i^{(i-1)} = \overline{0, m_i - 1}$, $t_{n-i+1}^{(i-1)} = \overline{0, m_{n-i+1} - 1}$.
	Executing subtraction operation $A^{(i)} = A^{(i-1)} - NC^{(i-1)} = [0 \parallel 0 \parallel 0 \parallel \ldots \ldots \parallel 0 \parallel a_i^{(i-1)} \parallel a_{i+1}^{(i-1)} \parallel \ldots \parallel 0 \parallel 0 \parallel a_{n+1}^{(i-1)}] - [0 \parallel 0 \parallel 0 \parallel \ldots \parallel 0 \parallel t_i^{(i-1)} \parallel t_{i+1}^{(i-1)} \parallel \ldots \parallel 0 \parallel \parallel 0 \parallel t_{n+1}^{(i-1)}] = \{0 \parallel 0 \parallel \ldots \parallel 0 \parallel [a_i^{(i-1)} - t_i^{(i-1)}] \bmod m_i \parallel [a_{i+1}^{(i-1)} - t_{i+1}^{(i-1)}] \bmod m_{i+1} \parallel \parallel [a_{i+2}^{(i-1)} - t_{i+2}^{(i-1)}] \bmod m_{i+2} \parallel \ldots \parallel [a_{n-i-1}^{(i-1)} - t_{n-i-1}^{(i-1)}] \bmod m_{n-i-1} \parallel \parallel [a_{n-i}^{(i-1)} - t_{n-i}^{(i-1)}] \bmod m_{n-i} \parallel [a_{n-i+1}^{(i-1)} - t_{n-i+1}^{(i-1)}] \bmod m_{n-i+1} \parallel 0 \parallel 0 \parallel \ldots \parallel 0 \parallel \parallel [a_{n+1}^{(i-1)} - t_{n+1}^{(i-1)}] \bmod m_{n+1}\} = [0 \parallel 0 \parallel \ldots \parallel 0 \parallel 0 \parallel a_{i+1}^{(i)} \parallel a_{i+2}^{(i)} \parallel a_{i+3}^{(i)} \parallel \ldots \ldots \parallel a_{n-i-1}^{(i)} \parallel a_{n-i}^{(i)} \parallel 0 \parallel 0 \parallel \ldots \parallel 0 \parallel a_{n+1}^{(i)}]$.

Fig. 4. (continuation)

	Referencing residue values $a_{i+1}^{(i)}$ and $a_{n-i}^{(i)}$ of number $A^{(i)} = [0 \,\|\| \, 0 \,\|\| \, 0 \,\|\| \ldots$ $\ldots \,\|\| \, 0 \,\|\| \, 0 \,\|\| \, a_{i+1}^{(i)} \,\|\| \ldots \,\|\| \, a_{n-i-1}^{(i)} \,\|\| \, a_{n-i}^{(i)} \,\|\| \, 0 \,\|\| \, 0 \,\|\| \, a_{n+1}^{(i)}]$ in NCB_i via nullification constant $NC^{(i)} = [0 \,\|\| \, 0 \,\|\| \, 0 \,\|\| \ldots \,\|\| \, 0 \,\|\| \, 0 \,\|\| \, t_{i+1}^{(i)} \,\|\| \ldots \,\|\| \, t_{n-i-1}^{(i)} \,\|\| \, t_{n-i}^{(i)} \,\|\| \, 0 \,\|\| \, 0 \,\|\| \, t_{n+1}^{(i)}]$; $t_{i+1}^{(i)} = a_{i+1}^{(i)}$, $t_{n-i}^{(i)} = a_{n-i}^{(i)}$; $t_{i+1}^{(i)} = \overline{0,\, m_{i+1} - 1}$, $t_{n-i}^{(i)} = \overline{0,\, m_{n-i} - 1}$.
For a value of $A^{(i+1)}$	Executing subtraction operation $A^{(i+1)} = A^{(i)} - NC^{(i)} = [0 \,\|\| \, 0 \,\|\| \ldots$ $\ldots \,\|\| \, 0 \,\|\| \, a_{i+1}^{(i)} \,\|\| \, a_{i+2}^{(i)} \,\|\| \, a_{i+3}^{(i)} \,\|\| \ldots \,\|\| \, a_{n-i-2}^{(i)} \,\|\| \, a_{n-i-1}^{(i)} \,\|\| \, a_{n-i}^{(i)} \,\|\| \, 0 \,\|\| \ldots \,\|\| \, 0 \,\|\| \, a_{n+1}^{(i)}] -$ $-[0 \,\|\| \, 0 \,\|\| \ldots \,\|\| \, 0 \,\|\| \, t_{i+1}^{(i)} \,\|\| \, t_{i+2}^{(i)} \,\|\| \, t_{i+3}^{(i)} \,\|\| \ldots \,\|\| \, t_{n-i-2}^{(i)} \,\|\| \, t_{n-i-1}^{(i)} \,\|\| \, 0 \,\|\| \ldots \,\|\| \, 0 \,\|\| \, t_{n+1}^{(i)}] =$ $= \{0 \,\|\| \, 0 \,\|\| \ldots \,\|\| \, 0 \,\|\| \, [a_{i+1}^{(i)} - t_{i+1}^{(i)}] \bmod m_{i+1} \,\|\| \, [a_{i+2}^{(i)} - t_{i+2}^{(i)}] \bmod m_{i+2} \,\|$ $\|\| \, [a_{i+3}^{(i)} - t_{i+3}^{(i)}] \bmod m_{i+3} \,\|\| \ldots \,\|\| \, [a_{n-i-2}^{(i)} - t_{n-i-2}^{(i)}] \bmod m_{n-i-2} \,\|$ $\|\| \, [a_{n-i-1}^{(i)} - t_{n-i-1}^{(i)}] \bmod m_{n-i-1} \,\|\| \, [a_{n-i}^{(i)} - t_{n-i}^{(i)}] \bmod m_{n-i} \,\|\| \, 0 \,\|\| \ldots \,\|\| \, 0 \,\|$ $\|\| \, [a_{n+1}^{(i)} - t_{n+1}^{(i)}] \bmod m_{n+1} \Big\} = [0 \,\|\| \, 0 \,\|\| \ldots \,\|\| \, 0 \,\|\| \, 0 \,\|\| \, a_{i+2}^{(i+1)} \,\|\| \, a_{i+3}^{(i+1)} \,\|\| \ldots \,\|\| \, a_{n-i-2}^{(i+1)} \,\|\| \, a_{n-i-1}^{(i+1)} \,\|$ $\|\| \, 0 \,\|\| \, 0 \,\|\| \ldots \,\|\| \, 0 \,\|\| \, 0 \,\|\| \, a_{n+1}^{(i+1)}]$.
…	…

Fig. 4. (continuation)

$n-1$	Subsequently for even *n* and odd *n* we'll get. For even number *n*: Referencing residue values $a_{n/2}^{(n/2-1)}$ and $a_{n/2+1}^{(n/2-1)}$ of number $A^{(n/2-1)} = [0 \,\|\|\, 0 \,\|\|\, \ldots \,\|\|\, 0 \,\|\|\, a_{n/2}^{(n/2-1)} \,\|\|\, a_{n/2+1}^{(n/2-1)} \,\|\|\, 0 \,\|\|\, \ldots \,\|\|\, 0 \,\|\|\, 0 \,\|\|\, a_{n+1}^{(n/2-1)}]$ in $NCB_{n/2-1}$ via nullification constant $NC^{(n/2-1)} = [0 \,\|\|\, 0 \,\|\|\, \ldots \,\|\|\, 0 \,\|\|\, t_{n/2}^{(n/2-1)} \,\|\|\, \|\| t_{n/2+1}^{(n/2-1)} \,\|\|\, 0 \,\|\|\, \ldots \,\|\|\, 0 \,\|\|\, 0 \,\|\|\, t_{n+1}^{(n/2-1)}]$; $t_{n/2}^{(n/2-1)} = a_{n/2}^{(n/2-1)}$, $t_{n/2+1}^{(n/2-1)} = a_{n/2+1}^{(n/2-1)}$; $t_{n/2}^{(n/2-1)} = \overline{0, m_{n/2}-1}$, $t_{n/2+1}^{(n/2-1)} = \overline{0, m_{n/2+1}-1}$. For odd number n: Referencing residue values $a_{(n+1)/2}^{((n+1)/2-1)}$ of number $A^{((n+1)/2-1)} = [0 \,\|\|\, 0 \,\|\|\, \ldots \,\|\|\, 0 \,\|\|\, a_{(n+1)/2}^{((n+1)/2-1)} \,\|\|\, 0 \,\|\|\, \ldots \,\|\|\, 0 \,\|\|\, a_{n+1}^{((n+1)/2-1)}]$ in $NCB_{(n+1)/2-1}$ via nullification constant $NC^{((n+1)/2-1)} = [0 \,\|\|\, 0 \,\|\|\, \ldots \,\|\|\, 0 \,\|\|\, t_{(n+1)/2}^{((n+1)/2-1)} \,\|\|\, 0 \,\|\|\, \ldots \,\|\|\, 0 \,\|\|\, t_{n+1}^{((n+1)/2-1)}]$, $t_{(n+1)/2}^{((n+1)/2-1)} = a_{(n+1)/2}^{((n+1)/2-1)}$; $t_{(n+1)/2}^{((n+1)/2-1)} = \overline{0, m_{(n+1)/2}-1}$.

Fig. 4. (continuation)

n	For both even n and odd n numbers we'll get following values of nullified number $A^{(N)}$: For even number n: getting nullified number $A^{(N)}$: $A^{(N)} = A^{(n/2)} = A^{(n/2-1)} -$ $-NC^{(n/2-1)} = [0 \,\|\| \, 0 \,\|\| \ldots \|\| \, 0 \,\|\| \, a_{n/2}^{(n/2-1)} \,\|\| \, a_{n/2+1}^{(n/2-1)} \,\|\| \, 0 \,\|\| \ldots \|\| \, 0 \,\|\| \, 0 \,\|\| \, a_{n+1}^{(n/2-1)}] -$ $-[0 \,\|\| \, 0 \,\|\| \ldots \|\| \, 0 \,\|\| \, t_{n/2}^{(n/2-1)} \,\|\| \, t_{n/2+1}^{(n/2-1)} \,\|\| \, 0 \,\|\| \ldots \|\| \, 0 \,\|\| \, 0 \,\|\| \, t_{n+1}^{(n/2-1)}] = \{0 \,\|\| \, 0 \,\|\| \ldots \|\| \, 0 \,\|\|$ $\|\| [a_{n/2}^{(n/2-1)} - t_{n/2}^{(n/2-1)}] \bmod m_{n/2} \,\|\| [a_{n/2+1}^{(n/2-1)} - t_{n/2+1}^{(n/2-1)}] \bmod m_{n/2+1} \,\|\| \, 0 \,\|\| \ldots \|\| \, 0 \,\|\| \, 0 \,\|\|$ $\|\| [a_{n+1}^{(n/2-1)} - t_{n+1}^{(n/2-1)}] \bmod m_{n+1}\} = \left[0 \,\|\| \, 0 \,\|\| \ldots \|\| \, 0 \,\|\| \, 0 \,\|\| \, 0 \,\|\| \ldots \|\| \, 0 \,\|\| \, 0 \,\|\| \, a_{n+1}^{(n/2)}\right]$, where $\gamma_{n+1} = a_{n+1}^{(n/2)}$. For odd number n: getting nullified number $A^{(N)}$: $A^{(N)} = A^{(n+1/2)} = A^{((n+1/2-1)} -$ $NC^{((n+1)/2-1)} = [0 \,\|\| \, 0 \,\|\| \ldots \|\| \, 0 \,\|\| \, a_{(n+1)/2}^{((n+1)/2-1)} \,\|\| \, 0 \,\|\| \ldots \|\| \, 0 \,\|\| \, a_{n+1}^{((n+1)/2-1)}] - [0 \,\|\| \, 0 \,\|\| \ldots$ $\ldots \|\| \, 0 \,\|\| \, t_{(n+1)/2}^{((n+1)/2-1)} \,\|\| \, 0 \,\|\| \ldots \|\| \, 0 \,\|\| \, t_{n+1}^{((n+1)/2-1)}] = \{0 \,\|\| \, 0 \,\|\| \ldots \|\| \, 0 \,\|\|$ $\|\| [a_{(n+1)/2}^{((n+1)/2-1)} - t_{(n+1)/2}^{((n+1)/2-1)}] \bmod m_{(n+1)/2} \,\|\| \, 0 \,\|\| \ldots \|\| \, 0 \,\|\|$ $\|\| [a_{n+1}^{((n+1)/2-1)} - t_{n+1}^{((n+1)/2-1)}] \bmod m_{n+1}\} = [0 \,\|\| \, 0 \,\|\| \ldots \|\| \, 0 \,\|\| \ldots \|\| \, 0 \,\|\| \, 0 \,\|\| \, a_{n+1}^{((n+1)/2)}]$, where $\gamma_{n+1} = a_{n+1}^{((n+1)/2)}$.
$T_{H3} = n \cdot \tau$	

Fig. 4. (continuation)

The time T_{N3} for the execution of the nullification procedure for the given parallel subtraction method is defined as [3-4]:

$$T_{N3} = n \cdot \tau_{subtr}. \quad (4)$$

While implementing the nullification procedure for the described ($N3$) method in nullification block (NB) of computer in RNS it's essential to have

$$K_{N3} = \sum_{i=1}^{\left\lceil \frac{n}{2} \right\rceil} (m_i \cdot m_{n-i+1} - 1)$$

nullification constants. At the same time the amount of binary bits NN_3 of NB is defined by the expression

$$N_{N3} = \sum_{i=1}^{\left\lceil \frac{n}{2} \right\rceil} (m_i \cdot m_{n-i+1} - 1) \cdot (n - 2i + 1).$$

3 The parallel subtraction method with a preliminary analysis of the sequent residue of the non-positional code structure in RNS

Let's take a closer look at the nullification procedure (N2), which is a sequential nullification procedure of the subsequent residues determination (NP SRD), which in turn helps to eliminate the problem described while performing procedure (N1). Implementation of this procedure reduces the verification time of RNS data in comparison to procedure (N1). The main idea of the procedure is to extract the nullification constant $NC^{(i)} = [0 \| 0 \| 0 \| \ldots \| 0 \| t_{i+1}^{(i)} \| t_{i+2}^{(i)} \| \ldots \| t_{n-3}^{(i)} \| t_{n-2}^{(i)} \| t_{n-1}^{(i)} \| t_n^{(i)} \| t_{n+1}^{(i)}]$ for a number $A^{(i)} = [0 \| \ \| 0 \| 0 \| \ldots \| a_{i+1}^{(i)} \| a_{i+2}^{(i)} \| \ldots \| a_{n-3}^{(i)} \| a_{n-2}^{(i)} \| a_{n-1}^{(i)} \| a_n^{(i)} \| a_{n+1}^{(i)}]$ via the value if the residue $a_{i+1}^{(i)}$ based m_{i+1}, in a computing lane (CL) of

CSCIDC, that operate using base m_{i+2}, the value of the residue can be obtained $a_{i+2}^{(i+1)}$, that will be used in the next nullification stage to extract sequent nullification constant $NC^{(i+1)} = [0 \| 0 \| 0 \| \ldots \| 0 \| t_{i+2}^{(i+1)} \| t_{i+3}^{(i+1)} \| \ldots$ $\ldots \| t_{n-3}^{(i+1)} \| t_{n-2}^{(i+1)} \| t_{n-1}^{(i+1)} \| t_n^{(i+1)} \| t_{n+1}^{(i+1)}]$.

The value of the Δa_{i+2}, that will be deducted from the value of $a_{i+2}^{(i)}$, in order to obtain the value of the residue $a_{i+2}^{(i+1)}$, is defined by a value of the single residue $a_{i+1}^{(i)}$. Analytically it's defined using following expression

$$a_{i+2}^{(i+1)} = \left[a_{i+2}^{(i)} - \Delta a_{i+2} \right] \bmod m_{i+2} . \tag{5}$$

In the process of $CN^{(i)}$ extraction using the value of the residue $a_{i+1}^{(i)}$ of the number $A^{(i)}$, the same residue will be simultaneously passed to the CL of CSCIC based m_{i+2}. In this case, with a use of according up-front generated bi-code tables $F\left\{a_{i+2}^{(i+1)}\right\} = \left[a_{i+1}^{(i)};\ a_{i+2}^{(i)} \right]$, by the values of $a_{i+1}^{(i)}$ and $a_{i+2}^{(i)}$ the value is for $a_{i+2}^{(i+1)}$ is selected. The algorithm example of NP SRD is illustrated in Table 3. The number of additions for the NP SRD is equal to *n*, since the nullification is performed by all *n* informational RNS bases. However, after each two additions an extra cycle is needed to create the sequent address and applying to NB. With this in mind there's one extra cycle for each two cycles, being free from the subtraction operation from the number of operations of the sequent nullification constant extraction. Thus, the general amount of cycles, free from subtraction operations, used to apply for NCB CSCIDC and the sequent address generation, is defined by the value [*n*/2]. The NP SRD is shown in the illustration 5.

The time T_{N2} of nullification procedure execution NP SDR is defined by the value (6)

$$T_{N2} = \left(\left[\frac{n-1}{2} \right] + n \right) \cdot \tau_{subtr} \tag{6}$$

In order to perform the overviewed nullification procedure NCB have to contain $K_{N2} = \sum_{i=1}^{n-1}(m_i - 1)$ of nullification constants. In this case the amount of N_{N2} binary bits of NCB, processing system is defined by the expression

$$N_{N2} = \sum_{i=1}^{n-1}(m_i - 1)\cdot(n-i).$$

Table 3 – Sequential nullification procedure of the subsequent residues determination algorithm

Operation №	Operation content	
1	Referencing residue value $a_1^{(0)}$ of the number $A^{(0)}$ in NCB_0 via $NC^{(0)}$	Forming residue value $a_2^{(1)}$ of number $A^{(1)}$ in the form of $a_2^{(1)} = t_2^{(1)} = \left[a_2^{(0)} - a_1^{(0)}\right] \bmod m_2$.
2	Executing subtraction operation $A^{(1)} = A^{(0)} - NC^{(0)}$.	Referencing residue value $a_2^{(1)}$ of number $A^{(1)}$ in NCB_1 via $NC^{(1)}$.
3	Executing subtraction operation $A^{(2)} = A^{(1)} - NC^{(1)}$.	Forming residue value $A^{(2)}$ in the form of $a_3^{(2)} = t_3^{(2)} = \left[a_3^{(1)} - a_2^{(1)}\right] \bmod m_3$.
4	Referencing residue value $a_3^{(2)}$ of number $A^{(2)}$ in NCB_2 via .	Forming residue value $a_4^{(3)}$ of number $A^{(3)}$ in the form of $a_4^{(3)} = t_4^{(3)} = \left[a_4^{(2)} - a_3^{(2)}\right] \bmod m_4$.
5	Executing subtraction operation $A^{(3)} = A^{(2)} - NC^{(2)}$.	Referencing residue value $a_4^{(3)}$ of number $A^{(3)}$ in NCB_3 via $NC^{(3)}$.

6	Executing subtraction operation $A^{(4)} = A^{(3)} - NC^{(3)}$.	Forming residue value $a_5^{(4)}$ of number $A^{(4)}$ in the form of $a_5^{(4)} = t_5^{(4)} = \left[a_5^{(3)} - a_4^{(3)} \right] \bmod m_5$
⋮	…	…
i	Executing subtraction operation $A^{(i)} = A^{(i-1)} - NC^{(i-1)}$.	Referencing residue value $a_{i+1}^{(i)}$ of number $A^{(i)}$ in NCB_i via $NC^{(i)}$.
$i+1$	Executing subtraction operation $A^{(i+1)} = A^{(i)} - NC^{(i)}$.	Forming residue value $a_{i+2}^{(i+1)}$ of number $A^{(i+1)}$ in the form of $a_{i+2}^{(i+1)} = t_{i+2}^{(i+1)} = \left[a_{i+2}^{(i)} - a_{i+1}^{(i)} \right] \bmod m_{i+2}$
$i+2$	Referencing residue value $a_{i+2}^{(i+1)}$ of number $A^{(i+1)}$ in NCB_{i+1} via $NC^{(i+1)}$.	Forming residue value $a_{i+3}^{(i+2)}$ of number $A^{(i+2)}$ in the form of $a_{i+3}^{(i+2)} = t_{i+3}^{(i+2)} = \left[a_{i+3}^{(i+1)} - a_{i+2}^{(i+1)} \right] \bmod m_{i+3}$
⋮	…	…
$K-2$	Referencing residue value $a_{n-1}^{(n-2)}$ of number $A^{(n-2)}$ in NCB_{n-2} via $NC^{(n-2)}$.	Forming residue value $a_n^{(n-1)}$ of number $A^{(n-1)}$ in the form of $a_n^{(n-1)} = t_n^{(n-1)} = \left[a_n^{(n-2)} - a_{n-1}^{(n-2)} \right] \bmod m_n$
$K-1$	Executing subtraction operation $A^{(n-1)} = A^{(n-2)} - NC^{(n-2)}$	Referencing residue value $a_n^{(n-1)}$ of number $A^{(n-1)}$ in NCB_{n-1} via $NC^{(n-1)}$.
K	Executing subtraction operation $A^{(n)} = A^{(n-1)} - NC^{(n-1)}$. Obtaining nullified $A^{(N)}$ number $A^{(N)} = A^{(n)} = [0 \,\|\| \, 0 \,\|\| \ldots \|\| \, 0 \,\|\| \ldots \|\| \, 0 \,\|\| \, 0 \,\|\| \, (\gamma_{n+1} = a_{n+1}^{(n)})]$	

Operation № (cycle)	Operation conetent	
1	Referencing residue value $a_1^{(0)}$ of number $A = A^{(0)} = [a_1^{(0)} \parallel a_2^{(0)} \parallel$ $\parallel a_3^{(0)} \parallel \ldots \parallel a_{i-1}^{(0)} \parallel a_i^{(0)} \parallel a_{i+1}^{(0)} \parallel \ldots \parallel a_{n-3}^{(0)} \parallel$ $\parallel a_{n-2}^{(0)} \parallel a_{n-1}^{(0)} \parallel a_n^{(0)} \parallel a_{n+1}^{(0)}]$ in NCB_0 via nullification constant $NC^{(0)} =$ $= [t_1^{(0)} \parallel t_2^{(0)} \parallel t_3^{(0)} \parallel \ldots \parallel t_{i-1}^{(0)} \parallel t_i^{(0)} \parallel t_{i+1}^{(0)} \parallel \ldots$ $\ldots \parallel t_{n-3}^{(0)} \parallel t_{n-2}^{(0)} \parallel t_{n-1}^{(0)} \parallel t_n^{(0)} \parallel t_{n+1}^{(0)}]$.	Forming residue value $a_2^{(1)}$ числа $A^{(1)} = [0 \parallel a_2^{(1)} \parallel$ $\parallel a_3^{(1)} \parallel \ldots \parallel a_{i-1}^{(1)} \parallel a_i^{(1)} \parallel a_{i+1}^{(1)} \parallel \ldots$ $\ldots \parallel a_{n-3}^{(1)} \parallel a_{n-2}^{(1)} \parallel a_{n-1}^{(1)} \parallel a_n^{(1)} \parallel a_{n+1}^{(1)}]$ in the form of $a_2^{(1)} = t_2^{(1)} = \left[a_2^{(0)} - a_1^{(0)}\right] \bmod m_2$.

Fig. 5.

2	Executing subtraction operation $A^{(1)} = A^{(0)} - NC^{(0)} = [a_1^{(0)} \| a_2^{(0)} \|$ $\| a_3^{(0)} \| \ldots \| a_{i-1}^{(0)} \| a_i^{(0)} \| a_{i+1}^{(0)} \| \ldots$ $\ldots \| a_{n-3}^{(0)} \| a_{n-2}^{(0)} \| a_{n-1}^{(0)} \| a_n^{(0)} \| a_{n+1}^{(0)}] -$ $-[t_1^{(0)} \| t_2^{(0)} \| t_3^{(0)} \| \ldots \| t_{i-1}^{(0)} \| t_i^{(0)} \| t_{i+1}^{(0)} \| \ldots$ $\ldots \| t_{n-3}^{(0)} \| t_{n-2}^{(0)} \| t_{n-1}^{(0)} \| t_n^{(0)} \| t_{n+1}^{(0)}] =$ $= \{[a_1^{(0)} - t_1^{(0)}] \bmod m_1 \| [a_2^{(0)} - t_2^{(0)}] \bmod m_2 \|$ $\| [a_3^{(0)} - t_3^{(0)}] \bmod m_3 \| \ldots \| [a_{i-1}^{(0)} - t_{i-1}^{(0)}] \bmod m_{i-1} \|$ $\| [a_i^{(0)} - t_i^{(0)}] \bmod m_i \| [a_{i+1}^{(0)} - t_{i+1}^{(0)}] \bmod m_{i+1} \| \ldots$ $\ldots \| [a_{n-3}^{(0)} - t_{n-3}^{(0)}] \bmod m_{n-3} \| [a_{n-2}^{(0)} - t_{n-2}^{(0)}] \bmod m_{n-2} \|$ $\| [a_{n-1}^{(0)} - t_{n-1}^{(0)}] \bmod m_{n-1} \| [a_n^{(0)} - t_n^{(0)}] \bmod m_n \|$ $\| [a_{n+1}^{(0)} - t_{n+1}^{(0)}] \bmod m_{n+1} \} = [0 \| a_2^{(1)} \|$ $\| a_3^{(1)} \| \ldots \| a_{i-1}^{(1)} \| a_i^{(1)} \| a_{i+1}^{(1)} \| \ldots \| a_{n-3}^{(1)} \|$ $\| a_{n-2}^{(1)} \| a_{n-1}^{(1)} \| a_n^{(1)} \| a_{n+1}^{(1)}]$.	Referencing residue value $a_2^{(1)}$ of number $A^{(1)} = [0 \| \| a_2^{(1)} \| a_3^{(1)} \| \ldots \| a_{i-1}^{(1)} \| a_i^{(1)} \|$ $\| a_{i+1}^{(1)} \| \ldots \| a_{n-3}^{(1)} \| a_{n-2}^{(1)} \| a_{n-1}^{(1)} \| \| a_n^{(1)} \| a_{n+1}^{(1)}]$ in NCB_1 via nullification constant $NC^{(1)} = [0 \| t_2^{(1)} \| t_3^{(1)} \| \ldots \| t_{i-1}^{(1)} \|$ $\| t_i^{(1)} \| t_{i+1}^{(1)} \| \ldots \| t_{n-3}^{(1)} \| t_{n-2}^{(1)} \| t_{n-1}^{(1)} \| \| t_n^{(1)} \| t_{n+1}^{(1)}]$.

Fig. 5. (continuation)

3	Executing subtraction operation $A^{(2)} = A^{(1)} - NC^{(1)} = [0 \,\|\| \, a_2^{(1)} \,\|\| \, a_3^{(1)} \,\|\| \ldots$ $\ldots \,\|\| \, a_{i-1}^{(1)} \,\|\| \, a_i^{(1)} \,\|\| \, a_{i+1}^{(1)} \,\|\| \ldots \,\|\| \, a_{n-3}^{(1)} \,\|\| \, a_{n-2}^{(1)} \,\|\|$ $\|\| \, a_{n-1}^{(1)} \,\|\| \, a_n^{(1)} \,\|\| \, a_{n+1}^{(1)}] - [0 \,\|\| \, t_2^{(1)} \,\|\| \, t_3^{(1)} \,\|\| \ldots$ $\ldots \,\|\| \, t_{i-1}^{(1)} \,\|\| \, t_i^{(1)} \,\|\| \, t_{i+1}^{(1)} \,\|\| \ldots \,\|\| \, t_{n-3}^{(1)} \,\|\| \, t_{n-2}^{(1)} \,\|\| \, t_{n-1}^{(1)} \,\|\|$ $\|\| \, t_n^{(1)} \,\|\| \, t_{n+1}^{(1)}] = \{0 \,\|\| \, [a_2^{(1)} - t_2^{(1)}] \bmod m_2 \,\|\|$ $\|\| [a_3^{(1)} - t_3^{(1)}] \bmod m_3 \,\|\| \ldots$ $\ldots \,\|\| [a_{i-1}^{(1)} - t_{i-1}^{(1)}] \bmod m_{i-1} \,\|\|$ $\|\| [a_i^{(1)} - t_i^{(1)}] \bmod m_i \,\|\| [a_{i+1}^{(1)} - t_{i+1}^{(1)}] \bmod m_{i+1} \,\|\| \ldots$ $\ldots \,\|\| [a_{n-3}^{(1)} - t_{n-3}^{(1)}] \bmod m_{n-3} \,\|\|$ $\|\| [a_{n-2}^{(1)} - t_{n-2}^{(1)}] \bmod m_{n-2} \,\|\|$ $\|\| [a_{n-1}^{(1)} - t_{n-1}^{(1)}] \bmod m_{n-1} \,\|\|$ $\|\| [a_n^{(1)} - t_n^{(1)}] \bmod m_n \,\|\|$ $\|\| [a_{n+1}^{(1)} - t_{n+1}^{(1)}] \bmod m_{n+1}\} = [0 \,\|\| \, 0 \,\|\| \, a_3^{(2)} \,\|\| \ldots$ $\ldots \,\|\| \, a_{i-1}^{(2)} \,\|\| \, a_i^{(2)} \,\|\| \, a_{i+1}^{(2)} \,\|\| \ldots \,\|\| \, a_{n-3}^{(2)} \,\|\| \, a_{n-2}^{(2)} \,\|\|$ $\|\| \, a_{n-1}^{(2)} \,\|\| \, a_n^{(2)} \,\|\| \, a_{n+1}^{(2)}]$.	Forming residue value $a_3^{(2)}$ of number $A^{(2)} = [0 \,\|\| \, 0 \,\|\| \, a_3^{(2)} \,\|\| \ldots$ $\ldots \,\|\| \, a_{i-1}^{(2)} \,\|\| \, a_i^{(2)} \,\|\| \, a_{i+1}^{(2)} \,\|\| \ldots \,\|\| \, a_{n-3}^{(2)} \,\|\|$ $\|\| \, a_{n-2}^{(2)} \,\|\| \, a_{n-1}^{(2)} \,\|\| \, a_n^{(2)} \,\|\| \, a_{n+1}^{(2)}]$ in the form of $a_3^{(2)} = t_3^{(2)} = \left[a_3^{(1)} - a_2^{(1)}\right] \bmod m_3$.

Fig. 5. (continuation)

4	Referencing residue value $a_3^{(2)}$ of number $A^{(2)} = [0 \,\|\|\, 0 \,\|\|\, a_3^{(2)} \,\|\| \ldots \,\|\| \, a_{i-1}^{(2)} \,\|\| \, a_i^{(2)} \,\|\| \, a_{i+1}^{(2)} \,\|\| \ldots$ $\ldots \,\|\| \, a_{n-3}^{(2)} \,\|\| \, a_{n-2}^{(2)} \,\|\| \, a_{n-1}^{(2)} \,\|\| \, a_n^{(2)} \,\|\| \, a_{n+1}^{(2)}]$ in NCB_2 via nullification constant $NC^{(2)}$.	Forming residue value $a_4^{(3)}$ of number $A^{(3)} = [0 \,\|\|\, 0 \,\|\|\, 0 \,\|\| \ldots$ $\ldots \,\|\| \, a_{i-1}^{(3)} \,\|\| \, a_i^{(3)} \,\|\| \, a_{i+1}^{(3)} \,\|\| \ldots \,\|\| \, a_{n-3}^{(3)} \,\|\|$ $\|\| \, a_{n-2}^{(3)} \,\|\| \, a_{n-1}^{(3)} \,\|\| \, a_n^{(3)} \,\|\| \, a_{n+1}^{(3)}]$ in the form of $a_4^{(3)} = t_4^{(3)} = \left[a_4^{(2)} - a_3^{(2)} \right] \bmod m_4 .$

Fig. 5. (continuation)

5	Executing subtraction operation $A^{(3)} = A^{(2)} - NC^{(2)} = [0 \,\|\| \, 0 \,\|\| \, a_3^{(2)} \,\|\| \ldots$ $\ldots \,\|\| \, a_{i-1}^{(2)} \,\|\| \, a_i^{(2)} \,\|\| \, a_{i+1}^{(2)} \,\|\| \ldots \,\|\| \, a_{n-3}^{(2)} \,\|\| \, a_{n-2}^{(2)} \,\|\|$ $\|\| \, a_{n-1}^{(2)} \,\|\| \, a_n^{(2)} \,\|\| \, a_{n+1}^{(2)}] - [0 \,\|\| \, 0 \,\|\| \, t_3^{(2)} \,\|\| \ldots$ $\ldots \,\|\| \, t_{i-1}^{(2)} \,\|\| \, t_i^{(2)} \,\|\| \, t_{i+1}^{(2)} \,\|\| \ldots \,\|\| \, t_{n-3}^{(2)} \,\|\| \, t_{n-2}^{(2)} \,\|\| \, t_{n-1}^{(2)} \,\|\|$ $\|\| \, t_n^{(2)} \,\|\| \, t_{n+1}^{(2)}] = \{0 \,\|\| \, 0 \,\|\| [a_3^{(2)} - t_3^{(2)}] \bmod m_3 \,\|\| \ldots$ $\ldots \,\|\| [a_{i-1}^{(2)} - t_{i-1}^{(2)}] \bmod m_{i-1} \,\|\|$ $\|\| [a_i^{(2)} - t_i^{(2)}] \bmod m_i \,\|\| [a_{i+1}^{(2)} - t_{i+1}^{(2)}] \bmod m_{i+1} \,\|\| \ldots$ $\ldots \,\|\| [a_{n-3}^{(2)} - t_{n-3}^{(2)}] \bmod m_{n-3} \,\|\| [a_{n-2}^{(2)} - t_{n-2}^{(2)}] \bmod m_{n-2} \,\|\|$ $\|\| [a_{n-1}^{(2)} - t_{n-1}^{(2)}] \bmod m_{n-1} \,\|\| [a_n^{(2)} - t_n^{(2)}] \bmod m_n \,\|\|$ $\|\| [a_{n+1}^{(2)} - t_{n+1}^{(2)}] \bmod m_{n+1}\} = [0 \,\|\| \, 0 \,\|\| \, 0 \,\|\|$ $\|\| \, a_4^{(3)} \,\|\| \, a_5^{(3)} \,\|\| \ldots \,\|\| \, a_{i-1}^{(3)} \,\|\| \, a_i^{(3)} \,\|\| \, a_{i+1}^{(3)} \,\|\| \ldots$ $\|\| \, t_2^{(0)} \,\|\| \, t_3^{(0)} \,\|\| \ldots \,\|\| \, t_{i-1}^{(0)} \,\|\| \, t_i^{(0)} \,\|\| \, t_{i+1}^{(0)} \,\|\| \ldots \,\|\| \, t_{n-3}^{(0)} \,\|\|$.	Referencing residue value $a_4^{(3)}$ of number $A^{(3)} = [0 \,\|\| \, \|\| \, 0 \,\|\| \, 0 \,\|\| \ldots \,\|\| \, a_{i-1}^{(3)} \,\|\| \, a_i^{(3)} \,\|\| \, a_{i+1}^{(3)} \,\|\| \ldots$ $\ldots \,\|\| \, a_{n-3}^{(3)} \,\|\| \, a_{n-2}^{(3)} \,\|\| \, a_{n-1}^{(3)} \,\|\| \, a_n^{(3)} \,\|\| \, a_{n+1}^{(3)}]$ in NCB_3 via nullification constant $NC^{(3)} = [0 \,\|\| \, 0 \,\|\|$ $\|\| \, 0 \,\|\| \ldots \,\|\| \, t_{i-1}^{(3)} \,\|\| \, t_i^{(3)} \,\|\| \, t_{i+1}^{(3)} \,\|\| \ldots \,\|\| \, t_{n-3}^{(3)} \,\|\|$ $\|\| \, t_{n-2}^{(3)} \,\|\| \, t_{n-1}^{(3)} \,\|\| \, t_n^{(3)} \,\|\| \, t_{n+1}^{(3)}]$.

Fig. 5. (continuation)

6	Executing subtraction operation $A^{(4)} = A^{(3)} - NC^{(3)} = [0 \,\|\|\, 0 \,\|\, 0 \,\|\| \ldots$ $\ldots \|\| a_{i-1}^{(3)} \,\|\| a_i^{(3)} \,\|\| a_{i+1}^{(3)} \,\|\| \cdots \,\|\| a_{n-3}^{(3)} \,\|\| a_{n-2}^{(3)} \,\|\|$ $\|\| a_{n-1}^{(3)} \,\|\| a_n^{(3)} \,\|\| a_{n+1}^{(3)}] - [0 \,\|\, 0 \,\|\, 0 \,\|\| \ldots \|\| t_{i-1}^{(3)} \,\|\|$ $\|\| t_i^{(3)} \,\|\| t_{i+1}^{(3)} \,\|\| \ldots \,\|\| t_{n-3}^{(3)} \,\|\| t_{n-2}^{(3)} \,\|\| t_{n-1}^{(3)} \,\|\| t_n^{(3)} \,\|\|$ $\|\| t_{n+1}^{(3)}] = \{0 \,\|\, 0 \,\|\, 0 \,\|\| [a_4^{(3)} - t_4^{(3)}] \bmod m_4 \,\|\|$ $\|\| [a_5^{(3)} - t_5^{(3)}] \bmod m_5 \,\|\| \ldots \,\|\| [a_{i-1}^{(3)} - t_{i-1}^{(3)}] \bmod m_{i-1} \,\|\|$ $\|\| [a_i^{(3)} - t_i^{(3)}] \bmod m_i \,\|\| [a_{i+1}^{(3)} - t_{i+1}^{(3)}] \bmod m_{i+1} \,\|\| \ldots$ $\ldots \|\| [a_{n-3}^{(3)} - t_{n-3}^{(3)}] \bmod m_{n-3} \,\|\| [a_{n-2}^{(3)} - t_{n-2}^{(3)}] \bmod m_{n-2} \,\|\|$ $\|\| [a_{n-1}^{(3)} - t_{n-1}^{(3)}] \bmod m_{n-1} \,\|\| [a_n^{(3)} - t_n^{(3)}] \bmod m_n \,\|\|$ $\|\| [a_{n+1}^{(3)} - t_{n+1}^{(3)}] \bmod m_{n+1}\} = [0 \,\|\, 0 \,\|\, 0 \,\|\| 0 \,\|\|$ $\|\| a_5^{(4)} \,\|\| \ldots \,\|\| a_{i-1}^{(4)} \,\|\| a_i^{(4)} \,\|\| a_{i+1}^{(4)} \,\|\| \ldots \,\|\| a_{n-3}^{(4)} \,\|\|$ $\|\| a_{n-2}^{(4)} \,\|\| a_{n-1}^{(4)} \,\|\| a_n^{(4)} \,\|\| a_{n+1}^{(4)}]$.	Forming residue value $a_5^{(4)}$ of number $A^{(4)} = [0 \,\|\, 0 \,\|\, 0 \,\|\| \ldots$ $\ldots \|\| a_{i-1}^{(4)} \,\|\| a_i^{(4)} \,\|\| a_{i+1}^{(4)} \,\|\| \ldots \,\|\| a_{n-3}^{(4)} \,\|\|$ $\|\| a_{n-2}^{(4)} \,\|\| a_{n-1}^{(4)} \,\|\| a_n^{(4)} \,\|\| a_{n+1}^{(4)}]$ in the form of $a_5^{(4)} = t_5^{(4)} = \left[a_5^{(3)} - a_4^{(3)} \right] \bmod m_5$.
…	…	…

Fig. 5. (continuation)

For a value of $A^{(i)}$

Executing subtraction operation

$$A^{(i)} = A^{(i-1)} - NC^{(i-1)} = [0 \,\|\, 0 \,\|\, 0 \,\|\, \ldots$$
$$\ldots \|\, 0 \,\|\, a_i^{(i-1)} \,\|\, a_{i+1}^{(i-1)} \,\|\, \ldots \,\|\, a_{n-3}^{(i-1)} \,\|\, a_{n-2}^{(i-1)} \,\|$$
$$\|\, a_{n-1}^{(i-1)} \,\|\, a_n^{(i-1)} \,\|\, a_{n+1}^{(i-1)}] - [0 \,\|\, 0 \,\|\, 0 \,\|\, 0 \,\|\, \ldots$$
$$\ldots \|\, 0 \,\|\, t_i^{(i-1)} \,\|\, t_{i+1}^{(i-1)} \,\|\, \ldots \,\|\, t_{n-3}^{(i-1)} \,\|\, t_{n-2}^{(i-1)} \,\|$$
$$\|\, t_{n-1}^{(i-1)} \,\|\, t_n^{(i-1)} \,\|\, t_{n+1}^{(i-1)}] = \{0 \,\|\, 0 \,\|\, 0 \,\|\, 0 \,\|\, \ldots \| \,0 \,\|\, 0 \,\|$$
$$\|\, [a_i^{(i-1)} - t_i^{(i-1)}] \bmod m_i \,\|$$
$$\|\, [a_{i+1}^{(i-1)} - t_{i+1}^{(i-1)}] \bmod m_{i+1} \,\|\, \ldots$$
$$\ldots \|\, [a_{n-3}^{(i-1)} - t_{n-3}^{(i-1)}] \bmod m_{n-3} \,\|$$
$$\|\, [a_{n-2}^{(i-1)} - t_{n-2}^{(i-1)}] \bmod m_{n-2} \,\|$$
$$\|\, [a_{n-1}^{(i-1)} - t_{n-1}^{(i-1)}] \bmod m_{n-1} \,\|$$
$$\|\, [a_n^{(i-1)} - t_n^{(i-1)}] \bmod m_n \,\|$$
$$\|\, [a_{n+1}^{(i-1)} - t_{n+1}^{(i-1)}] \bmod m_{n+1} \} = [0 \,\|\, 0 \,\|\, 0 \,\|\, \ldots$$
$$\ldots \|\, 0 \,\|\, 0 \,\|\, a_{i+1}^{(i)} \,\|\, \ldots \,\|\, a_{n-3}^{(i)} \,\|\, a_{n-2}^{(i)} \,\|\, a_{n-1}^{(i)} \,\|$$
$$\|\, a_n^{(i)} \,\|\, a_{n+1}^{(i)}] \,.$$

Referencing residue value $a_{i+1}^{(i)}$ of number

$$A^{(i)} = [0 \,\|\, 0 \,\|$$
$$\|\, 0 \,\|\, \ldots \,\|\, 0 \,\|\, 0 \,\|\, a_{i+1}^{(i)} \,\|\, \ldots \,\|\, a_{n-3}^{(i)} \,\|$$
$$\|\, a_{n-2}^{(i)} \,\|\, a_{n-1}^{(i)} \,\|\, a_n^{(i)} \,\|\, a_{n+1}^{(i)}] \text{ in } NCB_i \text{ via nullification constant}$$
$$NC^{(i)} = [0 \,\|\, 0 \,\|\, 0 \,\|\, \ldots \,\|\, 0 \,\|\, 0 \,\|$$
$$\|\, t_{i+1}^{(i)} \,\|\, \ldots \,\|\, t_{n-3}^{(i)} \,\|\, t_{n-2}^{(i)} \,\|\, t_{n-1}^{(i)} \,\|\, t_n^{(i)} \,\|\, t_{n+1}^{(i)}] \,.$$

Fig. 5. (continuation)

For a value of $A^{(i+1)}$	Executing subtraction operation $A^{(i+1)} = A^{(i)} - NC^{(i)} = [0 \,\|\|\, 0 \,\|\|\, 0 \,\|\| \ldots \,\|\| \, 0 \,\|\|$ $\|\| \, 0 \,\|\| \, a_{i+1}^{(i)} \,\|\| \ldots \,\|\| \, a_{n-3}^{(i)} \,\|\| \, a_{n-2}^{(i)} \,\|\| \, a_{n-1}^{(i)} \,\|\| \, a_n^{(i)} \,\|\|$ $\|\| \, a_{n+1}^{(i)}] - [0 \,\|\| \, 0 \,\|\| \, 0 \,\|\| \ldots \,\|\| \, 0 \,\|\| \, 0 \,\|\| \, t_{i+1}^{(i)} \,\|\| \ldots$ $\ldots \,\|\| \, t_{n-3}^{(i)} \,\|\| \, t_{n-2}^{(i)} \,\|\| \, t_{n-1}^{(i)} \,\|\| \, t_n^{(i)} \,\|\| \, t_{n+1}^{(i)}]$. Referencing residue value $a_{i+2}^{(i+1)}$ of number $A^{(i+1)} = [0 \,\|\| \, 0 \,\|\| \, 0 \,\|\| \ldots \,\|\| \, 0 \,\|\|$ $\|\| \, 0 \,\|\| \, 0 \,\|\| \ldots \,\|\| \, a_{n-3}^{(i+1)} \,\|\| \, a_{n-2}^{(i+1)} \,\|\| \, a_{n-1}^{(i+1)} \,\|\| \, a_n^{(i+1)} \,\|\| \, a_{n+1}^{(i+1)}]$ in NCB_{i+1} via nullification constant $NC^{(i+1)} = [0 \,\|\| \, 0 \,\|\| \, 0 \,\|\| \ldots$ $\ldots \,\|\| \, 0 \,\|\| \, 0 \,\|\| \, 0 \,\|\| \ldots \,\|\| \, t_{n-3}^{(i+1)} \,\|\| \, t_{n-2}^{(i+1)} \,\|\| \, t_{n-1}^{(i+1)} \,\|\| \, t_n^{(i+1)} \,\|\| \, t_{n+1}^{(i+1)}]$.	Forming residue value $a_{i+2}^{(i+1)}$ of number $A^{(i+1)} = [0 \,\|\| \, 0 \,\|\| \, 0 \,\|\| \ldots \,\|\| \, 0 \,\|\| \, 0 \,\|\|$ $\|\| \, 0 \,\|\| \ldots \,\|\| \, a_{n-3}^{(i+1)} \,\|\| \, a_{n-2}^{(i+1)} \,\|\| \, a_{n-1}^{(i+1)} \,\|\|$ $\|\| \, a_n^{(i+1)} \,\|\| \, a_{n+1}^{(i+1)}]$ in the form of $a_{i+2}^{(i+1)} =$ $= t_{i+2}^{(i+1)} = [a_{i+2}^{(i)} - a_{i+1}^{(i)}] \bmod m_{i+2}$ Forming residue value $a_{i+3}^{(i+2)}$ of number $A^{(i+2)} = [0 \,\|\| \, 0 \,\|\| \, 0 \,\|\| \ldots$ $\ldots \,\|\| \, 0 \,\|\| \, 0 \,\|\| \, 0 \,\|\| \ldots \,\|\| \, a_{n-3}^{(i+2)} \,\|\| \, a_{n-2}^{(i+2)} \,\|\|$ $\|\| \, a_{n-1}^{(i+2)} \,\|\| \, a_n^{(i+2)} \,\|\| \, a_{n+1}^{(i+2)}]$ in the form of $a_{i+3}^{(i+2)} = t_{i+3}^{(i+2)} = = [a_{i+3}^{(i+1)} - a_{i+2}^{(i+1)}] \bmod m_{i+3}$.
⋮	…	…

Fig. 5. (continuation)

$k-2$	Referencing residue value $a_{n-1}^{(n-2)}$ of number $A^{(n-2)} = [0 \| \| 0 \| \| 0 \| \| \ldots \| \| 0 \| \| 0 \| \| 0 \| \| \ldots \| \| 0 \| \| 0 \| \| a_{n-1}^{(n-2)} \| \| a_n^{(n-2)} \| \| \| \| a_{n+1}^{(n-2)}]$ in NCB_{n-2} via nullification constant $NC^{(n-2)} = [0 \| \| 0 \| \| 0 \| \| \ldots \| \| 0 \| \| 0 \| \| 0 \| \| \ldots \| \| 0 \| \| 0 \| \| t_{n-1}^{(n-2)} \| \| \| \| t_n^{(n-2)} \| \| t_{n+1}^{(n-2)}]$.	Forming residue value $a_n^{(n-1)}$ of number $A^{(n-1)} = [0 \| \| 0 \| \| 0 \| \| \ldots \| \| 0 \| \| 0 \| \| 0 \| \| \ldots \| \| 0 \| \| 0 \| \| 0 \| \| a_n^{(n-1)} \| \| \| \| a_{n+1}^{(n-1)}]$ in the form of $a_n^{(n-1)} = t_n^{(n-1)} = \left[a_n^{(n-2)} - a_{n-1}^{(n-2)}\right] \bmod m_n$.
$k-1$	Executing subtraction operation $A^{(n-1)} = A^{(n-2)} - NC^{(n-2)} = [0 \| \| 0 \| \| 0 \| \| \ldots \| \| 0 \| \| 0 \| \| 0 \| \| \ldots \| \| 0 \| \| 0 \| \| a_{n-1}^{(n-2)} \| \| a_n^{(n-2)} \| \| \| \| a_{n+1}^{(n-2)}] - [0 \| \| 0 \| \| 0 \| \| \ldots \| \| 0 \| \| 0 \| \| 0 \| \| \ldots \| \| 0 \| \| 0 \| \| t_{n-1}^{(n-2)} \| \| t_n^{(n-2)} \| \| t_{n+1}^{(n-2)}]$.	Referencing residue value $a_n^{(n-1)}$ of number $A^{(n-1)} = [0 \| \| 0 \| \| 0 \| \| \ldots \| \| 0 \| \| 0 \| \| 0 \| \| \ldots \| \| 0 \| \| 0 \| \| 0 \| \| a_n^{(n-1)} \| \| a_{n+1}^{(n-1)}]$ in NCB_{n-1} via nullification constant $NC^{(n-1)}$.
k	Executing subtraction operation $A^{(n)} = A^{(n-1)} - NC^{(n-1)} = [0 \| \| 0 \| \| 0 \| \| \ldots = \left[a_{n-1}^{(0)} - a_n^{(0)}\right] \bmod m_{n-1}$ $\ldots \| \| 0 \| \| 0 \| \| 0 \| \| t_{n+1}^{(n-1)}]$. Obtaining nullified $A^{(N)}$ number $A^{(N)} = A^{(n)} = [0 \| \| 0 \| \| \ldots \| \| 0 \| \| \ldots \| \| 0 \| \| 0 \| \| \gamma_{n+1} = a_{n+1}^{(n)}]$.	
$T_{N2} = \left(\left[\frac{n-1}{2}\right] + n\right) \cdot \tau_{сл}$		

Fig. 5. (continuation)

4 Method of RNS data verification with a preliminary analysis of sequential symmetrical residues of the controlled number, based on the principle of parallel nullification

The main limitation of the methods, that were reviewed in the previous chapters (N1-N3) of RNS data verification is that significant time needed for verification, which in turn contributes to a lower control performance and considerably higher non-productive computational cost [4].

In order to increase efficiency of data verification by reducing time needed to perform nullification procedure, we'll take a look at data verification method in RNS, called the method of parallel nullification (PN) along the subsequent residues determination (SRD) (N4). The proposed verification method is based on the procedure of the parallel number nullification with an additional operation of the preliminary residues extraction (see method (N2)). The idea of this method is based on that preliminary extraction being performed simultaneously by two residues $a_{i+1}^{(i)}$ and $a_{n-i}^{(i)}$ of number

$$A^{(i)} = [\overbrace{0\|0\|\ldots\|0}^{i-\text{zeros}}\|a_{i+1}^{(i)}\|a_{i+2}^{(i)}\|\ldots\|a_{n-i-1}^{(i)}\|a_{n-i}^{(i)}\|\overbrace{0\|\ldots\|0\|0}^{i-\text{zeros}}\|a_{n+1}^{(i)}].$$

As a result, in the process of nullification the operations of selecting the number by residue values of $a_{i+1}^{(i)}$ and $a_{n-i}^{(i)}$ of number

$$A^{(i)} = [0\|0\|\ldots\|0\|a_{i+1}^{(i)}\|a_{i+2}^{(i)}\|a_{i+3}^{(i)}\|\ldots$$
$$\ldots\|a_{n-i-2}^{(i)}\|a_{n-i-1}^{(i)}\|a_{n-i}^{(i)}\|0\|\ldots\|0\|a_{n+1}^{(i)}],$$

of the nullification constant

$$NC^{(i)} = [0\|0\|\ldots\|0\|t_{i+1}^{(i)}\|t_{i+2}^{(i)}\|t_{i+3}^{(i)}\|\ldots\|t_{n-i-2}^{(i)}\|t_{n-i-1}^{(i)}\|t_{n-1}^{(i)}\|0\|\ldots\|0\|t_{n+1}^{(i)}]$$

and the determining operation by the residue values of $a_{i+1}^{(i)}$ and $a_{n-i}^{(i)}$, of the

subsequent residues $a_{i+2}^{(i+1)}$ and $a_{n-i-1}^{(i+1)}$ of number

$$A^{(i+1)} = [0 \,||\, 0 \,||\, ... \,||\, 0 \,||\, 0 \,||\, a_{i+2}^{(i+1)} \,||\, a_{i+3}^{(i+1)} \,||\, ...$$
$$... \,||\, a_{n-i-2}^{(i+1)} \,||\, a_{n-i-1}^{(i+1)} \,||\, 0 \,||\, 0 \,||\, ... \,||\, 0 \,||\, 0 \,||\, a_{n+1}^{(i+1)}]$$

are combined in time. The operations of subtraction $A^{(i+1)} = A^{(i)} - NC^{(i)}$ and the operation of sequent nullification constant

$$NC^{(i+1)} = [0 \,||\, 0 \,||\, 0 \,||\, \ldots \,||\, 0 \,||\, 0 \,||\, t_{i+2}^{(i+1)} \,||\, \ldots \,||\, t_{n-i-2}^{(i+1)} \,||\, t_{n-i-1}^{(i+1)} \,||\, \,||\, 0 \,||\, 0 \,||\, t_{n+1}^{(i+1)}]$$

are also combined in time. Nullification algorithm is shown in Table 4.

The values of the Δa_{i+2} Δa_{n-i-1}, that will be deducted from the corresponding values of $a_{i+2}^{(i)}$ and $a_{n-i-1}^{(i)}$, in order to obtain the values of the residues $a_{i+2}^{(i+1)}$ and $a_{n-i-1}^{(i+1)}$, are determined only be the values of the corresponding residues of the numbers $a_{i+1}^{(i)}$ and $a_{n-i}^{(i)}$. Analytically it can be pictured in the form of the following expressions

$a_{i+2}^{(i+1)} = [a_{i+2}^{(i)} - \Delta a_{i+2}] \bmod m_{i+2}$ and $a_{n-i-1}^{(i+1)} = [a_{n-i-1}^{(i)} - \Delta a_{n-i-1}] \bmod m_{n-i-1}$.

In the process of $NC^{(i)}$ extraction by the residue values $a_{i+1}^{(i)}$ and $a_{n-i}^{(i)}$ of number $A^{(i)}$, these residues will be addressed to the computer accordingly based m_{i+2} and m_{n-i-1}. Using bi-code tables $F_1\left\{a_{i+2}^{(i+1)}\right\} = \left[a_{i+1}^{(i)};\ a_{i+2}^{(i)}\right]$ and $F_2\left\{a_{n-i-1}^{(i+1)}\right\} = \left[a_{n-1}^{(i)};\ a_{n-i-1}^{(i)}\right]$ the values are selected (determined) of $a_{i+2}^{(i+1)}$ and $a_{n-i-1}^{(i+1)}$. In this case the quantity of cycles, free from addition, used to address to NB and form the subsequent address, is equal to the value [(*n*+1)/2], (where [x] is an integer, closest to x number, not exceeding it). Along with it nullification is conducted using two informational RNS bases a_1, a_n; a_2, a_{n-1} etc. After each two subtractions one extra cycle to form sequent address and to access the nullification constant storage is needed. As a result for each two addition cycles ($\tau_{add} = \tau_0$) there is one free from addition cycle.

Table 4 – Sequential nullification procedure of the subsequent residues determination algorythm

№	Operation content	
1	Referencing residue value $a_1^{(0)}$ and $a_n^{(0)}$ of number $A^{(0)}$ in NCB_0 via $NC^{(0)}$.	Forming residue value $a_2^{(1)}$ and $a_{n-1}^{(1)}$ of number $A^{(1)}$ in the form $a_2^{(1)} = t_2^{(1)} = \left[a_2^{(0)} - a_1^{(0)} \right] \bmod m_2$ and $a_{n-1}^{(1)} = t_{n-1}^{(1)} = \left[a_{n-1}^{(0)} - a_n^{(0)} \right] \bmod m_{n-1}$.
2	Executing subtraction operation $A^{(1)} = A^{(0)} - NC^{(0)}$.	Referencing residue value $a_2^{(1)}$ and $a_{n-1}^{(1)}$ of number $A^{(1)}$ in NCB_1 via $NC^{(1)}$.
3	Executing subtraction operation $A^{(2)} = A^{(1)} - NC^{(1)}$.	Forming residue value $a_3^{(2)}$ and $a_{n-2}^{(2)}$ of number $A^{(2)}$ in the form $a_3^{(2)} = t_3^{(2)} = \left[a_3^{(1)} - a_2^{(1)} \right] \bmod m_3$ and $a_{n-2}^{(2)} = t_{n-2}^{(2)} = \left[a_{n-2}^{(1)} - a_{n-1}^{(1)} \right] \bmod m_{n-2}$.
⋮	…	…
i	Executing subtraction operation $A^{(i)} = A^{(i-1)} - NC^{(i-1)}$.	Referencing residue value $a_{i+1}^{(i)}$ and $a_{n-i}^{(i)}$ of number $A^{(i)}$ in NCB_i via $NC^{(i)}$.
$i+1$	Executing subtraction operation $A^{(i+1)} = A^{(i)} - NC^{(i)}$.	Forming residue value $a_{i+2}^{(i+1)}$ and $a_{n-i-1}^{(i+1)}$ of number $A^{(i+1)}$ in the form $a_{i+2}^{(i+1)} = t_{i+2}^{(i+1)} = \left[a_{i+2}^{(i)} - a_{i+1}^{(i)} \right] \bmod m_{i+2}$ and $a_{n-i-1}^{(i+1)} = t_{n-i-1}^{(i+1)} = \left[a_{n-i-1}^{(i)} - a_{n-i-2}^{(i)} \right] \bmod m_{n-i-1}$
$i+2$	Referencing residue value $a_{i+2}^{(i+1)}$ and $a_{n-i-1}^{(i+1)}$ of number $A^{(i+1)}$ in NCB_{i+1} via $NC^{(i+1)}$.	Forming residue value $a_{i+3}^{(i+2)}$ and $a_{n-i-2}^{(i+2)}$ of number $A^{(i+2)}$ in the form $a_{i+3}^{(i+2)} = t_{i+2}^{(i+2)} = \left[a_{i+3}^{(i+1)} - a_{i+2}^{(i+1)} \right] \bmod m_{i+3}$ and $a_{n-i-2}^{(i+2)} = t_{n-i-2}^{(i+2)} = \left[a_{n-i-2}^{(i+1)} - a_{n-i-3}^{(i+1)} \right] \bmod m_{n-i-2}$

Table 4 (continuation)

№	Operation content	
⋮	…	…
$k-2$	Referencing residue value $a_{n/2-1}^{(n/2-2)}$ and $a_{n/2+2}^{(n/2-2)}$ of number $A^{(n/2-2)}$ in $NCB_{n/2-2}$ via $NC^{(n/2-2)}$.	Forming residue value $a_{n/2}^{(n/2-1)}$ and $a_{n/2+1}^{(n/2-1)}$ of number $A^{(n/2-1)}$ in the form $a_{n/2}^{(n/2-1)} = t_{n/2}^{(n/2-1)} = \left[a_{n/2}^{(n/2-2)} - a_{n/2-1}^{(n/2-2)} \right] \bmod m_{n/2}$ and $a_{n/2+1}^{(n/2-1)} = t_{n/2+1}^{(n/2-1)} = \left[a_{n/2+1}^{(n/2-2)} - a_{n/2}^{(n/2-2)} \right] \bmod m_{n/2+1}$
$k-1$	Executing subtraction operation $A^{(n/2-1)} = A^{(n/2-2)} - -NC^{(n/2-2)}$.	Referencing residue value $a_{n/2}^{(n/2-1)}$ and $a_{n/2+1}^{(n/2-1)}$ of number $A^{(n/2-1)}$ in $NCB_{n/2-1}$ via $NC^{(n/2-1)}$.
k	Executing subtraction operation $A^{(n/2)} = A^{(n/2-1)} - NC^{(n/2-1)}$. Obtaining nullified $A^{(N)}$ number $A^{(N)} = A^{(n/2)} = [0 \| \| 0 \| \| ... \| \| 0 \| \| ... \| \| 0 \| \| 0 \| \| \gamma_{n+1} = a_{n+1}^{(n/2)}]$.	

Based on above-mentioned the time for executing nullification operation for the overviewed method of operative data control (N4) is determined in the following way

$$T_{N4} = \left[\frac{n+1}{2} \right] \cdot \tau_{add} + \left[\frac{\frac{n+1}{2}+1}{2} \right] \cdot \tau_{sel} . \quad (7)$$

Considering, that $\tau_{add} = \tau_{sel}$ getting:

$$T_{N4} = \left(\left[\frac{n+1}{2} \right] + \left[\frac{\frac{n+1}{2}+1}{2} \right] \right) \cdot \tau_{add} \quad (8)$$

While n is even, expression (8) will be written as follows:

$$T'_{N4} = \left(\frac{n}{2} + \left[\frac{\frac{n}{2}+1}{2} \right] \right) \cdot \tau_{add} \tag{9}$$

If $\frac{n}{2}$ is even, than

$$T'_{N4} = \frac{3}{4} n \cdot \tau_{add} . \tag{10}$$

If $\frac{n}{2}$ is odd, than

$$T'_{N4} = \left(\frac{3n+2}{4} \right) \cdot \tau_{add} . \tag{11}$$

While n is odd:

$$T''_{N4} = \left(\frac{n+1}{2} + \left[\frac{\frac{n+1}{2}+1}{2} \right] \right) \cdot \tau_{add} . \tag{12}$$

If $\frac{n+1}{2}$ is even, than

$$T''_{N4} = \frac{3}{4} (n+1) \cdot \tau_{add} . \tag{13}$$

If $\frac{n+1}{2}$ is odd, than

$$T''_{N4} = \left(\frac{3n+5}{4}\right)\cdot\tau_{add}. \qquad (14)$$

To prove obtained expression (8) it is convenient to use the mathematical induction method using n.

First stage of proof.

For the minimal value of $n=3$ the nullification time is equal to $T_{N4}=3\cdot\tau_{add}$. This becomes obvious from the Illustration 6, diagram (N4) PN method of SRD.

The second stage.

Assuming that the expression (8) is true, while $n=K$, i.e.

$$T_{N4} = \left(\left\lceil\frac{K+1}{2}\right\rceil + \left\lceil\frac{\left\lceil\frac{K-1}{2}\right\rceil+1}{2}\right\rceil\right)\cdot\tau_{add}.$$

The third stage.

Let's prove, that expression (4.19) is also true, while $n=K+1$, i.e.

$$T_{N4} = \left(\left\lceil\frac{K+2}{2}\right\rceil + \left\lceil\frac{\left\lceil\frac{K+2}{2}+1\right\rceil}{2}\right\rceil\right)\cdot\tau_{add}.$$

While K is even (K+1 is odd) getting:

$$T'_{N4} = \left(\frac{K}{2} + 1 + \left[\frac{\frac{K}{2} + 2}{2} \right] \right) \cdot \tau_{add} .$$

If $\frac{K}{2}$ is even, than $T'_{N4} = \left(\frac{3K+8}{4} \right) \cdot \tau_{add}$.

And if $\frac{K}{2}$ is odd, than $T'_{N4} = \left(\frac{3K+6}{4} \right) \cdot \tau_{add}$.

While K is odd (K+1 is even), we get:

$$T''_{N4} = \left(\frac{K+1}{2} + \left[\frac{\left[\frac{K+1}{2} \right] + 1}{2} \right] \right) \cdot \tau_{add} .$$

If $\frac{K+1}{2}$ is even, than $T''_{N4} = \left(\frac{3K+3}{4} \right) \cdot \tau_{add}$; if $\frac{K+1}{2}$ is odd, than $T''_{N4} = \left(\frac{3K+5}{4} \right) \cdot \tau_{add}$. According to the expressions (10), (11), (12) and (14) let's write next expressions:

$$\frac{3K+3}{4} \cdot \tau_{add} = \frac{3}{4}(K+1) \cdot \tau_{add} , \quad \frac{3K+5}{4} \cdot \tau_{add} = \left\{ \frac{3(K+1)+2}{4} \right\} \cdot \tau_{add} ,$$

$$\frac{3K+6}{4} \cdot \tau_{add} = \frac{3}{4}\{(K+1)+1\} \cdot \tau_{add} , \quad \frac{3K+8}{4} \cdot \tau_{add} = \left\{ \frac{3(K+1)+5}{4} \right\} \cdot \tau_{add} .$$

As a result the expression (8) is true while $n = K+1$, which completes the proof. For a practical calculations to determine the time for RNS data verification it's advices to use expressions (10), (11), (12) and (14).

On the fig. 6 time diagrams of NB operation for SN method (diagram N1), for a SN SRD method (diagram N2), as well as for the first PN SRD (diagram (N3)) and for the second PN SRD (diagram (N4) control methods, that were previously overviewed are shown.

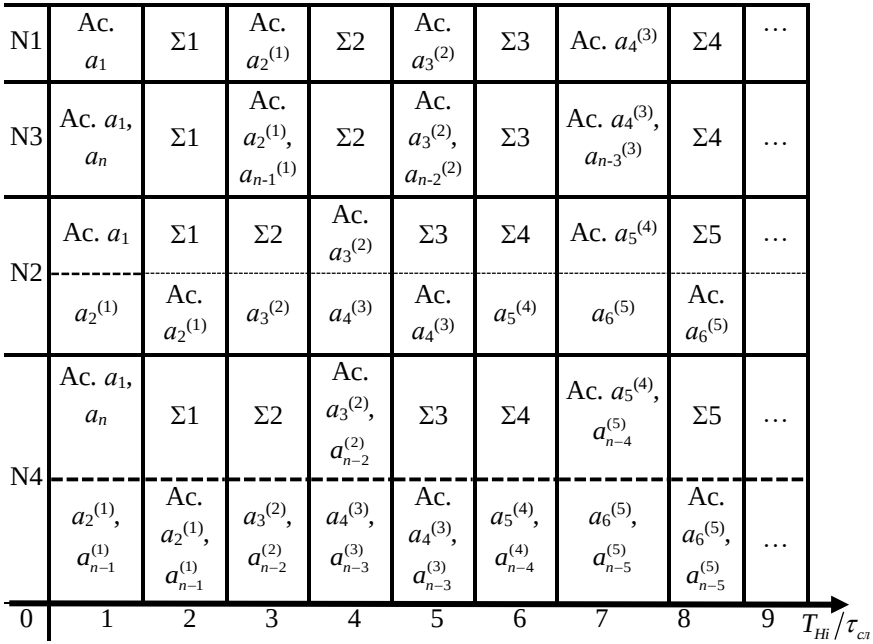

Fig 6. – Time diagrams of the NB operation, using different nullification methods

Where: Ac. $a_i^{(i-1)}$, $...\|[a_{i-1}^{(0)} - t_{i-1}^{(0)}] \bmod m_{i-1}\|$, stands for accessing using number values of $a_i^{(i-1)}$ $a_{n-i+1}^{(i-1)}$ of the number

$$A^{(i-1)} = (0\|...\|0\|a_i^{(i-1)}\|a_{i+1}^{(i-1)}\|...\|a_{n-i}^{(i-1)}\|a_{n-i+1}^{(i-1)}\|0\|...\|0\|a_{n+1}^{(i-1)})$$

in NB via nullification constant in the form of

$$NC^{(i)} = (0 \,||\, ... \,||\, 0 \,||\, t_{i,i} \,||\, t_{i+1,i} \,||\, ... \,||\, t_{n-i,i} \,||\, t_{n-i+1,i} \,||\, 0 \,||\, ... \;\; ... \,||\, 0 \,||\, t_{n+1,i}) ;$$

$a_{i+1}^{(i+1)}$, $a_{n-i}^{(i+1)}$ and generating using the values of $a_i^{(i)}$ and $a_{n-i+1}^{(i)}$ of the number $A^{(i-1)}$ of the next numbers $a_{i+1}^{(i)}$ and $||\,[a_i^{(0)} - t_i^{(0)}] \bmod m_i \,||$ for a number

$$A^{(i)} = (0 \,||\, ... \,||\, 0 \,||\, a_{i+1}^{(i)} \,||\, ... \,||\, a_{n-1}^{(i)} \,||\, 0 \,||\, ... \,||\, 0 \,||\, a_{n+1}^{(i)}) ;$$

where $\sum i$ is a deduction operation of the value of the $NC^{(i-1)}$ form the number $A^{(i-1)}$, i.e. performing the operation $A^{(i-1)} - NC^{(i-1)}$.

While implementing nullification procedure for N4 method NB must contain $K_{N4} = \sum_{i=1}^{\left\lceil \frac{n}{2} \right\rceil} (m_i \cdot m_{n-i+1} - 2)$ nullification constants. In this case the amount of N_{H3} binary bits of nullification constants determines by the expression $K_{N4} = \sum_{i=1}^{\left\lceil \frac{n}{2} \right\rceil} (m_i \cdot m_{n-i+1} - 2) \cdot (n - 2i + 1)$.

PN SRD data verification method is shown in the Fig. 7.

Let's benchmark and analyze basic characteristics of the methods for RNS data verification. When picking the method for RNS data verification it's required to take into the account characteristics value, describing the method [5-6]. Obtained expressions are functional formulas capable to evaluate the performance of nullification procedure implementation, depending on the values of n and τ_{add}.

Generalized characteristics for all four data control methods are shown in the Table 5. Based on the data in the Table 6, Table 7 contains calculation results of the characteristics of the reviewed methods for controlling l-byte ($l = \overline{1 \div 8}$) RNS computer bit grids.

Operation № (cycle)	Operation content	
1	Referencing residue values $a_1^{(0)}$ and $a_n^{(0)}$ of number $A = A^{(0)} = [a_1^{(0)} \,\|\| \, a_2^{(0)} \,\|\|$ $\|\| \, a_3^{(0)} \,\|\| \cdots \|\| \, a_{i-1}^{(0)} \,\|\| \, a_i^{(0)} \,\|\| \, a_{i+1}^{(0)} \,\|\| \cdots \|\| \, a_{n-3}^{(0)} \,\|\|$ $\|\| \, a_{n-2}^{(0)} \,\|\| \, a_{n-1}^{(0)} \,\|\| \, a_n^{(0)} \,\|\| \, a_{n+1}^{(0)}]$ in NCB_0 via nullification constant $NC^{(0)} = [t_1^{(0)} \,\|\|$ $\|\| \, t_2^{(0)} \,\|\| \, t_3^{(0)} \,\|\| \cdots \|\| \, t_{i-1}^{(0)} \,\|\| \, t_i^{(0)} \,\|\| \, t_{i+1}^{(0)} \,\|\| \cdots \|\| \, t_{n-3}^{(0)} \,\|\|$ $\|\| \, t_{n-2}^{(0)} \,\|\| \, t_{n-1}^{(0)} \,\|\| \, t_n^{(0)} \,\|\| \, t_{n+1}^{(0)}]$; $t_1^{(0)} = a_1^{(0)}$, $t_n^{(0)} = a_n^{(0)}$; $t_1^{(0)} = \overline{0, m_1 - 1}$, $t_n^{(0)} = \overline{0, m_n - 1}$.	Forming residue values $a_2^{(1)}$ and $a_{n-1}^{(1)}$ of number $A^{(1)} = [0 \,\|\| \, a_2^{(1)} \,\|\| \, a_3^{(1)} \,\|\| \cdots \|\| \, a_{i-1}^{(1)} \,\|\|$ $\|\| \, a_i^{(1)} \,\|\| \, a_{i+1}^{(1)} \,\|\| \cdots \|\| \, a_{n-3}^{(1)} \,\|\| \, a_{n-2}^{(1)} \,\|\|$ $\|\| \, a_{n-1}^{(1)} \,\|\| \, 0 \,\|\| \, a_{n+1}^{(1)}]$ in the form of $a_2^{(1)} = t_2^{(1)} = \left[a_2^{(0)} - a_1^{(0)}\right] \bmod m_2$ and $a_{n-1}^{(1)} = t_{n-1}^{(1)} = = \left[a_{n-1}^{(0)} - a_n^{(0)}\right] \bmod m_{n-1}$.

Fig. 7. – PN SRD data control method

2	Executing subtraction operation $A^{(1)} = A^{(0)} - NC^{(0)} = [a_1^{(0)} \,\|\|\, a_2^{(0)} \,\|\, a_3^{(0)} \,\|\| \cdots$ $\cdots \,\|\| a_{i-1}^{(0)} \,\|\| a_i^{(0)} \,\|\| a_{i+1}^{(0)} \,\|\| \cdots \,\|\| a_{n-3}^{(0)} \,\|\| a_{n-2}^{(0)} \,\|\| a_{n-1}^{(0)} \,\|\|$ $\|\| a_n^{(0)} \,\|\| a_{n+1}^{(0)}] - [t_1^{(0)} \,\|\| t_2^{(0)} \,\|\| t_3^{(0)} \,\|\| \cdots \,\|\| t_{i-1}^{(0)} \,\|\|$ $\|\| t_i^{(0)} \,\|\| t_{i+1}^{(0)} \,\|\| \cdots \,\|\| t_{n-3}^{(0)} \,\|\| t_{n-2}^{(0)} \,\|\| t_{n-1}^{(0)} \,\|\| t_n^{(0)} \,\|\| t_{n+1}^{(0)}] =$ $= \{[a_1^{(0)} - t_1^{(0)}] \bmod m_1 \,\|\| [a_2^{(0)} - t_2^{(0)}] \bmod m_2 \,\|\|$ $\|\| [a_3^{(0)} - t_3^{(0)}] \bmod m_3 \,\|\| \cdots \|\| [a_{i-1}^{(0)} - t_{i-1}^{(0)}] \bmod m_{i-1} \,\|\|$ $\|\| [a_i^{(0)} - t_i^{(0)}] \bmod m_i \,\|\| \,\|\| [a_{i+1}^{(0)} - t_{i+1}^{(0)}] \bmod m_{i+1} \,\|\| \cdots$ $\cdots \,\|\| [a_{n-3}^{(0)} - t_{n-3}^{(0)}] \bmod m_{n-3} \,\|\| [a_{n-2}^{(0)} - t_{n-2}^{(0)}] \bmod m_{n-2} \,\|\|$ $\|\| [a_{n-1}^{(0)} - t_{n-1}^{(0)}] \bmod m_{n-1} \,\|\| \,\|\| [a_n^{(0)} - t_n^{(0)}] \bmod m_n \,\|\|$ $\|\| [a_{n+1}^{(0)} - t_{n+1}^{(0)}] \bmod m_{n+1}\} = [0 \,\|\| a_2^{(1)} \,\|\| a_3^{(1)} \,\|\| \cdots$ $\cdots \,\|\| a_{i-1}^{(1)} \,\|\| a_i^{(1)} \,\|\| a_{i+1}^{(1)} \,\|\| \cdots \,\|\| a_{n-3}^{(1)} \,\|\| a_{n-2}^{(1)} \,\|\| a_{n-1}^{(1)} \,\|\| 0 \,\|\| a_{n+1}^{(1)}]$.	Referencing residue values $a_2^{(1)}$ and $a_{n-1}^{(1)}$ of number $A^{(1)} = [0 \,\|\| a_2^{(1)} \,\|\| a_3^{(1)} \,\|\| \ldots \,\|\| a_{i-1}^{(1)} \,\|\|$ $\|\| a_i^{(1)} \,\|\| a_{i+1}^{(1)} \,\|\| \ldots \,\|\| a_{n-3}^{(1)} \,\|\| a_{n-2}^{(1)} \,\|\|$ $\|\| a_{n-1}^{(1)} \,\|\| 0 \,\|\| a_{n+1}^{(1)}]$ in NCB_1 via nullification constant $NC^{(1)} = [0 \,\|\| t_2^{(1)} \,\|\| t_3^{(1)} \,\|\| \ldots \,\|\| t_{i-1}^{(1)} \,\|\|$ $\|\| t_i^{(1)} \,\|\| t_{i+1}^{(1)} \,\|\| \ldots \,\|\| t_{n-3}^{(1)} \,\|\| t_{n-2}^{(1)} \,\|\| t_{n-1}^{(1)} \,\|\|$ $0 \,\|\| t_{n+1}^{(1)}]$; $t_2^{(1)} = a_2^{(1)}$, $t_{n-1}^{(1)} = a_{n-1}^{(1)}$; $t_2^{(1)} = \overline{0, m_2 - 1}$, $t_{n-1}^{(1)} = \overline{0, m_{n-1} - 1}$.

Fig. 7. (continuation)

	Executing subtraction operation	Forming residue values $a_3^{(2)}$ and $a_{n-2}^{(2)}$ of
	$A^{(2)} = A^{(1)} - NC^{(1)} = = \{0 \Vert [a_2^{(1)} - t_2^{(1)}] \bmod m_2 \Vert$	number $A^{(2)} = [0 \Vert 0 \Vert a_3^{(2)} \Vert \ldots \Vert a_{i-1}^{(2)} \Vert$
	$\Vert [a_3^{(1)} - t_3^{(1)}] \bmod m_3 \Vert \Vert [a_4^{(1)} - t_4^{(1)}] \bmod m_4 \Vert \ldots$	$\Vert a_i^{(2)} \Vert a_{i+1}^{(2)} \Vert \ldots \Vert a_{n-3}^{(2)} \Vert a_{n-2}^{(2)} \Vert$
	$\ldots \Vert [a_{i-1}^{(1)} - t_{i-1}^{(1)}] \bmod m_{i-1} \Vert \Vert [a_i^{(1)} - t_i^{(1)}] \bmod m_i \Vert$	$\Vert 0 \Vert 0 \Vert a_{n+1}^{(2)}]$ in the form of
3	$\Vert [a_{i+1}^{(1)} - t_{i+1}^{(1)}] \bmod m_{i+1} \Vert \ldots \Vert [a_{n-3}^{(1)} - t_{n-3}^{(1)}] \bmod m_{n-3} \Vert$	$a_3^{(2)} = t_3^{(2)} = \left[a_3^{(1)} - a_2^{(1)} \right] \bmod m_3$ and
	$\Vert [a_{n-2}^{(1)} - t_{n-2}^{(1)}] \bmod m_{n-2} \Vert$	$a_{n-2}^{(2)} = t_{n-2}^{(2)} = = \left[a_{n-2}^{(1)} - a_{n-1}^{(1)} \right] \bmod m_{n-2}$.
	$\Vert [a_{n+1}^{(1)} - t_{n+1}^{(1)}] \bmod m_{n+1} \} = [0 \Vert 0 \Vert a_3^{(2)} \Vert$	
	$\Vert a_4^{(2)} \Vert \ldots \Vert a_{i-1}^{(2)} \Vert a_i^{(2)} \Vert a_{i+1}^{(2)} \Vert \ldots \Vert a_{n-3}^{(2)} \Vert$	
	$\Vert a_{n-2}^{(2)} \Vert 0 \Vert 0 \Vert a_{n+1}^{(2)}]$.	
⋮	…	…

Fig. 7. (continuation)

For values $A^{(i)}$

Executing subtraction operation

$$A^{(i)} = A^{(i-1)} - NC^{(i-1)} = [0 \| 0 \| 0 \| 0 \| \| \| 0 \| 0 \| a_i^{(i-1)} \| \| a_{i+1}^{(i-1)} \| \dots \| 0 \| 0 \| a_{n+1}^{(i-1)}] - [0 \| 0 \| 0 \| 0 \| \dots \| 0 \| 0 \| t_i^{(i-1)} \| \| t_{i+1}^{(i-1)} \| \dots \| 0 \| 0 \| t_{n+1}^{(i-1)}] =$$

$$= 0 \| 0 \| 0 \| \dots \| 0 \| 0 \| [a_i^{(i-1)} - t_i^{(i-1)}] \bmod m_i \| \| [a_{i+1}^{(i-1)} - t_{i+1}^{(i-1)}] \bmod m_{i+1} \| \| [a_{i+2}^{(i-1)} - t_{i+2}^{(i-1)}] \bmod m_{i+2} \| \dots \| [a_{n-i-1}^{(i-1)} - t_{n-i-1}^{(i-1)}] \bmod m_{n-i-1} \| \| [a_{n-i}^{(i-1)} - t_{n-i}^{(i-1)}] \bmod m_{n-i} \| \| [a_{n-i+1}^{(i-1)} - t_{n-i+1}^{(i-1)}] \bmod m_{n-i+1} \| 0 \| 0 \| 0 \| \dots \| 0 \| 0 \| [a_{n+1}^{(i-1)} - t_{n+1}^{(i-1)}] \bmod m_{n+1} \} = [0 \| 0 \| 0 \| \dots \| 0 \| 0 \| 0 \| a_{i+1}^{(i)} \| a_{i+2}^{(i)} \| a_{i+3}^{(i)} \| \dots \| a_{n-i-1}^{(i)} \| \| a_{n-i}^{(i)} \| 0 \| 0 \| 0 \| \dots \| 0 \| 0 \| a_{n+1}^{(i)}] .$$

Referencing residue values and $a_{n-i}^{(i)}$ of number $A^{(i)} = [0 \| 0 \| 0 \| \dots \| 0 \| 0 \| a_{i+1}^{(i)} \| \| a_{i+2}^{(i)} \| \dots \| a_{n-i-1}^{(i)} \| \| a_{n-i}^{(i)} \| 0 \| 0 \| \dots \| 0 \| 0 \| 0 \| a_{n+1}^{(i)}]$ in NCB_i via nullification constant

$$NC^{(i)} = [0 \| 0 \| 0 \| \dots \| 0 \| 0 \| t_{i+1}^{(i)} \| \| t_{i+2}^{(i)} \| \dots \| t_{n-i-1}^{(i)} \| \| t_{n-i}^{(i)} \| 0 \| 0 \| \dots \| 0 \| 0 \| 0 \| t_{n+1}^{(i)}] ; \; t_{i+1}^{(i)} = a_{i+1}^{(i)}, \; t_{n-i}^{(i)} = a_{n-i}^{(i)} ; \; t_{i+1}^{(i)} = \overline{0, m_{i+1} - 1} ; \; t_{n-i}^{(i)} = \overline{0, m_{n-i} - 1} .$$

Fig. 7. (continuation)

For a value $A^{(i+1)}$	Executing subtraction operation	Forming residue values $a_{i+2}^{(i+1)}$ and $a_{n-i-1}^{(i+1)}$ of number $A^{(i+1)} = [0 \,\|\|\, 0 \,\|\| \ldots \|\| \, 0 \,\|\| \, 0 \,\|\|$ $\|\| \, a_{i+2}^{(i+1)} \,\|\| \, a_{i+3}^{(i)} \,\|\| \ldots \|\| \, a_{n-i-2}^{(i+1)} \,\|\| \, a_{n-i-1}^{(i+1)} \,\|\|$ $\|\| \, 0 \,\|\| \, 0 \,\|\| \ldots \|\| \, 0 \,\|\| \, 0 \,\|\| \, a_{n+1}^{(i+1)}]$ in the form of $a_{i+2}^{(i+1)} = r_{i+2}^{(i+1)} = = \left[a_{i+2}^{(i)} - a_{i+1}^{(i)} \right] \bmod m_{i+2}$ and $a_{n-i-1}^{(i+1)} = r_{n-i-1}^{(i+1)} =$ $= \left[a_{n-i-1}^{(i)} - a_{n-i-2}^{(i)} \right] \bmod m_{n-i-1}$.
	$A^{(i+1)} = A^{(i)} - NC^{(i)} = [0 \,\|\|\, 0 \,\|\| \ldots \|\| \, 0 \,\|\| \, a_{i+1}^{(i)} \,\|\|$ $\|\| \, a_{i+2}^{(i)} \,\|\| \, a_{i+3}^{(i)} \,\|\| \ldots \|\| \, a_{n-i-2}^{(i)} \,\|\| \, a_{n-i-1}^{(i)} \,\|\| \, a_{n-i}^{(i)} \,\|\| \, 0 \,\|\| \ldots$ $\ldots \|\| \, 0 \,\|\| \, a_{n+1}^{(i)}] - [0 \,\|\|\, 0 \,\|\| \ldots \|\| \, 0 \,\|\| \, r_{i+1}^{(i)} \,\|\| \, r_{i+2}^{(i)} \,\|\|$ $\|\| \, r_{i+3}^{(i)} \,\|\| \ldots \|\| \, r_{n-i-2}^{(i)} \,\|\| \, r_{n-i-1}^{(i)} \,\|\| \, 0 \,\|\| \ldots \|\| \, 0 \,\|\|$ $\|\| \, r_{n+1}^{(i)}] = \{0 \,\|\|\, 0 \,\|\| \ldots \|\| \, 0 \,\|\| \;\; \|\| [a_{i+1}^{(i)} - r_{i+1}^{(i)}] \bmod m_{i+1} \,\|\|$ $\|\| [a_{i+2}^{(i)} - r_{i+2}^{(i)}] \bmod m_{i+2} \,\|\| [a_{i+3}^{(i)} - r_{i+3}^{(i)}] \bmod m_{i+3} \,\|\| \ldots$ $\ldots \|\| [a_{n-i-2}^{(i)} - r_{n-i-2}^{(i)}] \bmod m_{n-i-2} \,\|\| [a_{n-i-1}^{(i)} - r_{n-i-1}^{(i)}] \bmod m_{n-i-1}$ $\|\| [a_{n-i}^{(i)} - r_{n-i}^{(i)}] \bmod m_{n-i} \,\|\| \, 0 \,\|\| \ldots \|\| \, 0 \,\|\|$ $\|\| [a_{n+1}^{(i)} - r_{n+1}^{(i)}] \bmod m_{n+1}\} =$ $= [0 \,\|\| \, 0 \,\|\| \ldots \|\| \, 0 \,\|\| \, 0 \,\|\| \, a_{i+2}^{(i+1)} \,\|\| \, a_{i+3}^{(i+1)} \,\|\| \ldots$ $\ldots \|\| \, a_{n-i-2}^{(i+1)} \,\|\| \, a_{n-i-1}^{(i+1)} \,\|\| \, 0 \,\|\| \, 0 \,\|\| \ldots \|\| \, 0 \,\|\| \, 0 \,\|\| \, a_{n+1}^{(i+1)}]$.	

Fig. 7. (continuation)

$i+2$	Referencing residue values $a_{i+2}^{(i+1)}$ and $a_{n-i-1}^{(i+1)}$ of number $A^{(i+1)}$ in NCB_{i+1} via nullification constant $NC^{(i+1)} = [0 \,\|\|\, 0 \,\|\| \ldots \|\| \, 0 \,\|\| \, 0 \,\|\| \, t_{i+2}^{(i+1)} \,\|\|$ $\|\| \, t_{i+3}^{(i+1)} \,\|\| \ldots \|\| \, t_{n-i-2}^{(i+1)} \,\|\| \, t_{n-i-1}^{(i+1)} \,\|\| \, 0 \,\|\| \, 0 \,\|\| \ldots \|\| \, 0 \,\|\| \, 0 \,\|\| \, t_{n+1}^{(i+1)}]$; $t_{i+2}^{(i+1)} = a_{i+2}^{(i+1)}$, $t_{n-i-1}^{(i+1)} = a_{n-i-1}^{(i+1)}$; $t_{i+2}^{(i+1)} = 0, \overline{m_{i+2} - 1}$, $t_{n-i-1}^{(i+1)} = 0, \overline{m_{n-i-1} - 1}$.	Forming residue values $a_{i+3}^{(i+2)}$ and $a_{n-i-2}^{(i+2)}$ of number $A^{(i+2)}$ in the form of $a_{i+3}^{(i+2)} = t_{i+2}^{(i+2)} =$ $= \left[a_{i+3}^{(i+1)} - a_{i+2}^{(i+1)} \right] \bmod m_{i+3}$ and $a_{n-i-2}^{(i+2)} =$ $= t_{n-i-2}^{(i+2)} = \left[a_{n-i-2}^{(i+1)} - a_{n-i-3}^{(i+1)} \right] \bmod m_{n-i-2}$.
$\vdots$	…	…
$k-2$	Referencing residue values $a_{n/2-1}^{(n/2-2)}$ and $a_{n/2+2}^{(n/2-2)}$ of number $A^{(n/2-2)}$ in $\mathrm{NCB}_{n/2-2}$ via nullification constant $NC^{(n/2-2)} = [0 \,\|\, 0 \,\|\| \ldots \|\| \, 0 \,\|\| \, 0 \,\|\| \, t_{n/2-1}^{(n/2-2)} \,\|\|$ $\|\| \, t_{n/2-2}^{(n/2-2)} \,\|\| \ldots \|\| \, t_{n/2+1}^{(n/2-2)} \,\|\| \, t_{n/2+2}^{(n/2-2)} \,\|\| \, 0 \,\|\| \, 0 \,\|\| \ldots \|\| \, 0 \,\|\| \, 0 \,\|\|$ $\|\| \, t_{n+1}^{(n/2-2)}]$; $t_{n/2-1}^{(n/2-1)} = a_{n/2-1}^{(n/2-2)}$, $t_{n/2+2}^{(n/2-2)} = a_{n/2+2}^{(n/2-2)}$; $t_{n/2-1}^{(n/2-2)} = 0, \overline{m_{n/2-1} - 1}$, $t_{n/2+2}^{(n/2-2)} = 0, \overline{m_{n/2+2} - 1}$.	Forming residue values $a_{n/2}^{(n/2-1)}$ and $a_{n/2+1}^{(n/2-1)}$ of number $A^{(n/2-1)}$ in the form of $a_{n/2}^{(n/2-1)} = t_{n/2}^{(n/2-1)} =$ $= \left[a_{n/2}^{(n/2-2)} - a_{n/2-1}^{(n/2-2)} \right] \bmod m_{n/2}$ and $a_{n/2+1}^{(n/2-1)} = t_{n/2+1}^{(n/2-1)} =$ $= \left[a_{n/2+1}^{(n/2-2)} - a_{n/2}^{(n/2-2)} \right] \bmod m_{n/2+1}$.

Fig. 7. (continuation)

	Executing subtraction operation	Referencing residue values $a_{n/2}^{(n/2-1)}$ and
$k-1$	$A^{(n/2-1)} = A^{(n/2-2)} - NC^{(n/2-2)} = [0 \,\|\|\, 0 \,\|\| \ldots \|\| \, 0 \,\|\| \, 0 \,\|\|$	$a_{n/2+1}^{(n/2-1)}$ of number
	$\|\| \, a_{n/2-1}^{(n/2-2)} \,\|\| \, a_{n/2}^{(n/2-2)} \,\|\| \, a_{n/2+1}^{(n/2-2)} \,\|\| \, a_{n/2+2}^{(n/2-2)} \,\|\| \, 0 \,\|\| \, 0 \,\|\| \ldots \|\| \, 0 \,\|\|$	$A^{(n/2-1)} = [0 \,\|\| \, 0 \,\|\| \ldots \|\| \, 0 \,\|\| \, 0 \,\|\|$
	$\|\| \, 0 \,\|\| \, a_{n+1}^{(n/2-2)}] - [0 \,\|\| \, 0 \,\|\| \ldots \|\| \, 0 \,\|\| \, 0 \,\|\| \, t_{n/2-1}^{(n/2-2)} \,\|\| \, t_{n/2}^{(n/2-2)} \,\|\|$	$\|\| \, a_{n/2}^{(n/2-1)} \,\|\| \, a_{n/2+1}^{(n/2-1)} \,\|\| \, 0 \,\|\| \, 0 \,\|\| \ldots \|\| \, 0 \,\|\|$
	$\|\| \, t_{n/2+1}^{(n/2-2)} \,\|\| \, t_{n/2+2}^{(n/2-2)} \,\|\| \, 0 \,\|\| \, 0 \,\|\| \ldots \|\| \, t_{n+1}^{(n/2-2)}] = \{0 \,\|\| \, 0 \,\|\| \cdots$	$\|\| \, 0 \,\|\| \, a_{n+1}^{(n/2-1)}]$; in $NCB_{n/2-1}$ via
	$\cdots \|\| \, 0 \,\|\| \, 0 \,\|\| [a_{n/2-1}^{(n/2-2)} - t_{n/2-1}^{(n/2-2)}] \bmod m_{n/2-1} \,\|\|$	nullification constant
	$\|\| [a_{n/2}^{(n/2-2)} - t_{n/2}^{(n/2-2)}] \bmod m_{n/2} \,\|\| \cdots$	$NC^{(n/2-1)} = [0 \,\|\| \, 0 \,\|\| \ldots \|\| \, 0 \,\|\| \, 0 \,\|\|$
	$\cdots \|\| [a_{n/2+1}^{(n/2-2)} - t_{n/2+1}^{(n/2-2)}] \bmod m_{n/2+1} \,\|\|$	$\|\| \, t_{n/2}^{(n/2-1)} \,\|\| \, t_{n/2+1}^{(n/2-1)} \,\|\| \, 0 \,\|\| \, 0 \,\|\| \ldots \|\| \, 0 \,\|\|$
	$\|\| [a_{n/2+2}^{(n/2-2)} - t_{n/2+2}^{(n/2-2)}] \bmod m_{n/2+2} \,\|\| \, 0 \,\|\| \, 0 \,\|\| \ldots \|\| \, 0 \,\|\| \, 0 \,\|\|$	$\|\| \, 0 \,\|\| \, t_{n+1}^{(n/2-1)}]$; $t_{n/2}^{(n/2-1)} = a_{n/2}^{(n/2-1)}$,
	$\|\| [a_{n+1}^{(n/2-2)} - t_{n+1}^{(n/2-2)}] \bmod m_{n+1}\} = [0 \,\|\| \, 0 \,\|\| \ldots \|\| \, 0 \,\|\| \, 0 \,\|\|$	$t_{n/2+1}^{(n/2-1)} = a_{n/2+1}^{(n/2-1)}$; $t_{n/2}^{(n/2-1)} = \overline{0, m_{n/2}-1}$,
	$\|\| \, 0 \,\|\| \, a_{n/2}^{(n/2-1)} \,\|\| \, a_{n/2+1}^{(n/2-1)} \,\|\| \, 0 \,\|\| \, 0 \,\|\| \ldots \|\| \, 0 \,\|\| \, a_{n+1}^{(n/2-1)}]$.	$t_{n/2+1}^{(n/2-1)} = \overline{0, m_{n/2+1}-1}$.

Fig. 7. (continuation)

k	Obtaining nullified $A^{(N)}$ number. Executing operation $A^{(n/2-1)} = A^{(n/2-2)} - NC^{(n/2-2)} = [0 \,\|\|\, 0 \,\|\| \ldots \|\| \, 0 \,\|\| \, a_{n/2}^{(n/2-1)} \,\|\| \, a_{n/2+1}^{(n/2-1)} \,\|\| \, 0 \,\|\| \ldots \|\| \, 0 \,\|\| \, a_{n+1}^{(n/2-1)}] - [0 \,\|\|$ $\|\| \, 0 \,\|\| \ldots \|\| \, 0 \,\|\| \, t_{n/2}^{(n/2-1)} \,\|\| \, t_{n/2+1}^{(n/2-1)} \,\|\| \, 0 \,\|\| \ldots \|\| \, 0 \,\|\| \, t_{n+1}^{(n/2-1)}] = [0 \,\|\| \, 0 \,\|\| \ldots \|\| \, 0 \,\|\| \, [a_{n/2}^{(n/2-1)} - t_{n/2}^{(n/2-1)}] \bmod m_{n/2} \,\|\|$ $\|\| \, [a_{n/2+1}^{(n/2-1)} - t_{n/2+1}^{(n/2-1)}] \bmod m_{n/2+1} \,\|\| \, 0 \,\|\| \ldots \|\| \, 0 \,\|\| \, [a_{n+1}^{(n/2-1)} - t_{n+1}^{(n/2-1)}] \bmod m_{n+1} = [0 \,\|\| \, 0 \,\|\| \ldots \|\| \, 0 \,\|\| \ldots$ $\ldots \|\| \, 0 \,\|\| \, 0 \,\|\| \, (\gamma_{n+1} = a_{n+1}^{(n/2)})]$.
	$T_{N4} = \left(\left\lfloor \frac{n+1}{2} \right\rfloor + \left\lceil \frac{\frac{n+1}{2}+1}{2} \right\rceil \right) \cdot \tau_{add}$

Fig. 7. (continuation)

Table 5 – Basic characteristics of RNS data verification methods

Data verification methods N_i		Nullification time T_{Ni}	Amount of nullification constants K_{Ni}	Amount of binary bit constants N_{Ni}
N1	Successive nullification method	$T_{N1} = 2 \cdot n \cdot \tau_{add}$	$K_{N1} = \sum_{i=1}^{n} (m_i - 1)$	$N_{N1} = \sum_{i=1}^{n} (m_i - 1) \cdot (n - i + 1)$
N2	Successive nullification method with a sequent residues determination	$T_{N2} = \left(\left[\frac{n-1}{2} \right] + n \right) \cdot \tau_{add}$	$K_{N2} = \sum_{i=1}^{n-1} (m_i - 1)$	$N_{N2} = \sum_{i=1}^{n-1} (m_i - 1) \cdot (n - i)$
N3	Parallel nullification method	$T_{N3} = n \cdot \tau_{add}$	$K_{N3} = \sum_{i=1}^{\left[\frac{n}{2}\right]} (m_i \cdot m_{n-i+1} - 1)$	$N_{N3} = \sum_{i=1}^{\left[\frac{n}{2}\right]} (m_i \cdot m_{n-i+1} - 1) \cdot \cdot (n - 2 \cdot i + 1)$
N4	Parallel nullification method with a sequent residues determination	$T_{N4} = \left(\left[\frac{n+1}{2} \right] + \left[\frac{\left[\frac{n+1}{2} \right]}{2} \right] \right) \tau$	$K_{N4} = \sum_{i=1}^{\left[\frac{n}{2}\right]} (m_i \cdot m_{n-i+1} - 1)$	$N_{N4} = \sum_{i=1}^{\left[\frac{n}{2}\right]} (m_i \cdot m_{n-i+1} - 2) \cdot \cdot (n - 2 \cdot i + 1)$

Table 6 – RNS base aggregate for l-byte ($l = \overline{1 \div 8}$) computer bit grids

Bit grid size $l(n)$	RNS informational bases $\{m_i\}$, $i = \overline{1, n}$	RNS check base m_{n+1}
1(4)	$m_1 = 3$, $m_2 = 4$, $m_3 = 5$, $m_4 = 7$	$m_5 = 11$
2(6)	$m_1 = 2$, $m_2 = 5$, $m_3 = 7$, $m_4 = 9$, $m_5 = 11$, $m_6 = 13$	$m_7 = 17$
3(8)	$m_1 = 3$, $m_2 = 4$, $m_3 = 5$, $m_4 = 7$, $m_5 = 11$, $m_6 = 13$, $m_7 = 17$, $m_8 = 19$	$m_9 = 23$
4(10)	$m_1 = 2$, $m_2 = 3$, $m_3 = 5$, $m_4 = 7$, $m_5 = 11$, $m_6 = 13$, $m_7 = 17$, $m_8 = 19$, $m_9 = 23$, $m_{10} = 29$	$m_{11} = 31$
8(16)	$m_1 = 3$, $m_2 = 4$, $m_3 = 5$, $m_4 = 7$, $m_5 = 11$, $m_6 = 13$, $m_7 = 17$, $m_8 = 19$, $m_9 = 23$, $m_{10} = 29$, $m_{11} = 31$, $m_{12} = 37$, $m_{13} = 41$, $m_{14} = 43$, $m_{15} = 47$, $m_{16} = 53$	$m_{17} = 59$

Table 7 – Characteristics calculated data of RNS data verification methods for l-byte ($l = \overline{1 \div 8}$) bit grids

l (n)	N1			N2			N3			N4		
	$\frac{T_{N1}}{\tau_{cl}}$	K_{N1}	N_{N1}	$\frac{T_{N2}}{\tau_{add}}$	K_{N2}	N_{N2}	$\frac{T_{N3}}{\tau_{add}}$	K_{N3}	N_{N3}	$\frac{T_{N4}}{\tau_{add}}$	K_{N4}	N_{N4}
1 (4)	8	15	31	5	9	16	4	39	79	3	37	75
2 (6)	12	41	106	8	29	65	6	141	349	4	138	340
3 (8)	16	71	217	11	53	146	8	263	995	6	259	979
4 (10)	20	119	412	14	91	293	10	479	1955	7	474	1930
8 (16)	32	367	1947	23	315	1580	16	2581	16493	12	2573	16429

Table 8 – Time characteristics of control methods

$l\ (n)$	T_{N_i}/τ_{add}			
	$N1$	$N2$	$N3$	$N4$
1 (4)	8	5	4	**3**
2 (6)	12	8	6	**4**
3 (8)	16	11	8	**6**
4 (10)	20	14	10	**7**
8 (16)	32	23	16	**12**

Table 9 – Control methods characteristics

$l\ (n)$	K_{N_i}			
	*N*1	***N*2**	*N*3	*N*4
1 (4)	15	**9**	39	37
2 (6)	41	**29**	141	138
3 (8)	71	**53**	263	259
4 (10)	119	**91**	479	474
8 (16)	367	**315**	2581	2573

Table 10 – Control methods characteristics

$l\ (n)$	N_{H_i}			
	*H*1	***H*2**	*H*3	*H*4
1 (4)	31	**16**	79	75
2 (6)	106	**65**	349	340
3 (8)	217	**146**	995	979
4 (10)	412	**293**	1955	1930
8 (16)	1947	**1580**	16493	16429

Table 11 – Comparative time analysis data of RNS data verification

n	$T_{Ni} = T/\tau$				Gain [%]		
	T_{N1}	T_{N2}	T_{N3}	T_{N4}	K_{N1}	K_{N2}	K_{N3}
4	8	5	4	**3**	62	40	25
6	12	8	6	**4**	66	55	33
8	16	11	8	**6**	62	45	25
10	20	14	10	**7**	65	53	30
16	32	23	16	**12**	62	47	25

For the sake of convenience of comparative analysis of the efficiency of the introduced verification methods, generalized data from Table 7 will be appropriate to divide into three (based on the amount of characteristics) separate tables (Table 8-10).

Based on the Table 10 the Table 11 of comparative data analysis was composed for the effectiveness of the operative PN SRD method implementation with a reference to the existing methods of RNS data verification by the processing speed of nullification procedure.

Efficiency coefficient K_{Ni} of implementing data verification PN SRD method, with a reference to existing nullification methods, is determined by the expression $K_{Ni} = \frac{T_{N1} - T_{Ni}}{T_{N1}} \cdot 100\% \quad (i = \overline{1, 3})$. Analyzing Table 11 high effectiveness of the operative data verification method (N4), based on the implementing of the parallel nullification procedure with a simultaneous subsequent residues determination is noticeable.

3 Conclusion

Thus, the developed method of data control, based on the implementing of the parallel nullification procedure with a simultaneous subsequent residues of the controlled number, as compared with existing methods based on the principle of nullification, allows, depending on the length of the machine word, to increase the efficiency of data control by 25-30%. Based on the developed data control method, based on the implementing of the parallel nullification procedure with a simultaneous subsequent residues determination is noticeable of the controlled number, an error control algorithm was synthesized based on which devices were obtained for its implementation [6, 7].

References

[1] I. Ya. Akushskii and D. I. Yuditskii, Machine Arithmetic in Residual Classes [in Russian]: Sov. Radio, Moscow, 1968.

[2] V. A. Krasnobayev, S. A. Koshman, and M. A. Mavrina, "A method for increasing the reliability of verification of data represented in a residue number system," Cybernetics and Systems Analysis, vol. 50, Issue 6, pp. 969-976, November 2014.

[3] V. A. Krasnobayev, A. S. Yanko, and S. A. Koshman, "A Method for arithmetic comparison of data represented in a residue number system, "Cybernetics and Systems Analysis, vol. 52, Issue 1, pp. 145-150, January 2016.

[4] S. A. Moroz and V. A. Krasnobayev, "A data verification method in a non-positional residue number system," Control, Navigation, and Communication Systems, No. 2 (18), pp. 134–138, 2011.

[5] V. A. Krasnobayev and S. A. Koshman, "A method for operational diagnosis of data represented in a residue number system, "Cybernetics and Systems Analysis, vol. 54, Issue 2, pp. 336-344, March 2018.

[6] A. Yanko, S. Koshman, V. Krasnobayev, "Algorithms of data processing in the residual classes system," 4th International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T), Kharkiv, 2017, pp. 117-121.

[7] V. Krasnobayev, A. Kuznetsov, S. Koshman, S. Moroz "Improved method of determining the alternative set of numbers in residue number system," Advances in Intelligent Systems and Computing, Vol. 836, pp. 319-328, 2019.