

(19)



Евразийское  
патентное  
ведомство

(21) 202391055 (13) A1

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ЕВРАЗИЙСКОЙ ЗАЯВКЕ

(43) Дата публикации заявки  
2023.11.21

(51) Int. Cl. G06F 7/72 (2006.01)  
G06F 7/06 (2006.01)  
G06F 7/49 (2006.01)

(22) Дата подачи заявки  
2023.05.03

(54) УСТРОЙСТВО ВЫЧИСЛЕНИЯ РАНГА ЧИСЛА В СИСТЕМЕ ОСТАТОЧНЫХ КЛАССОВ

(96) 2023000078 (RU) 2023.05.03

(72) Изобретатель:

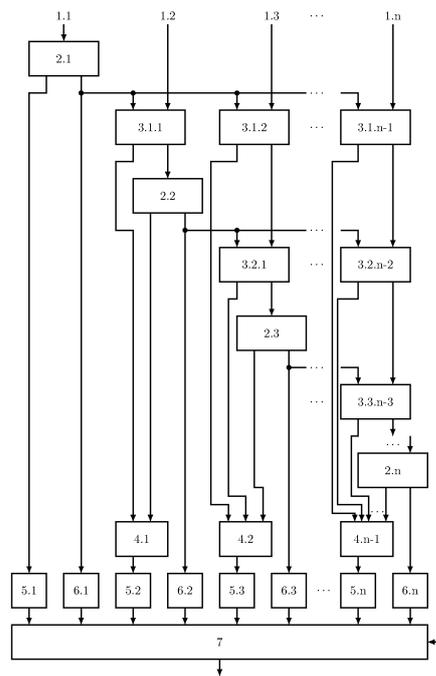
(71) Заявитель:  
ФЕДЕРАЛЬНОЕ  
ГОСУДАРСТВЕННОЕ  
АВТОНОМНОЕ  
ОБРАЗОВАТЕЛЬНОЕ  
УЧРЕЖДЕНИЕ ВЫСШЕГО  
ОБРАЗОВАНИЯ "СЕВЕРО-  
КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ  
УНИВЕРСИТЕТ" (RU)

Кучуков Виктор Андреевич, Бабенко  
Михаил Григорьевич, Кучеров  
Николай Николаевич (RU)

(74) Представитель:

Алиханов А.А. (RU)

(57) Устройство относится к вычислительной технике и может быть использовано для определения ранга числа, представленного в системе остаточных классов. Техническим результатом заявляемого изобретения является сокращение оборудования, это достигается тем, что в устройство вычисления ранга числа в системе остаточных классов, содержащее  $n$  входов остатка, где  $n$  - количество модулей  $p_i$  системы остаточных классов (СОК),  $n-1$  вычислительную ступень,  $n$  блоков вычисления ранга произведения, блок вычисления ранга суммы, при этом  $i$ -я вычислительная ступень, где  $i=1, \dots, n-1$ , содержит  $n-i$  сумматоров по модулю, в каждую вычислительную ступень введен блок вычисления кратности, введено  $n-1$  сумматоров,  $n$  умножителей,  $n$ -й блок вычисления кратности. Сущность изобретения основана на свойствах ранга числа в СОК, а именно на возможности вычисления ранга суммы чисел из рангов слагаемых и возможности получения ранга числа через ранги, кратные базисам, состоящим из  $i$  нулей и  $n-i$  единиц, чисел.



Структурная схема устройства

202391055 A1

202391055 A1

### Устройство вычисления ранга числа в системе остаточных классов

Устройство относится к вычислительной технике и может быть использовано для определения ранга числа, представленного в системе остаточных классов.

Известна нейронная сеть для вычисления позиционной характеристики ранга числа, представленного в системе остаточных классов (патент РФ №2271569, опубл. 10.03.2006), содержащая взаимосвязанные между собой входной слой нейронов и нейронную сеть конечного кольца.

Недостатком данного изобретения является использование в вычислениях выражения  $P^{pn-2}$ , вычисление которого является ресурсоемкой задачей в реальных модулярных системах. Также недостатком является некорректность метода, лежащего в основе изобретения, для наборов модулей, отличных от выбранного в качестве примера. Возьмем в качестве СОК набор модулей  $\{3,5,7\}$ , тогда для десятичного числа 17 ранг числа, вычисленный по данному устройству равен 6, в то время как истинное значение ранга равно 2.

Известно устройство сравнения и определения знака чисел, представленных в системе остаточных классов (евразийский патент №038389, опубл. 20.08.2021), содержащее входы первого и второго числа, вход знака, регистры хранения, блоки умножения, сумматоры, блоки определения знака по первому и второму числу, решающий блок, а также выходы рангов, знаков чисел, а также результата сравнения.

Недостатком данного устройство является использование в алгоритме умножения на  $C(B_i)$ , что значительно увеличивает размерность обрабатываемых чисел.

Наиболее близким к заявленному изобретению является устройство для вычисления ранга модулярного числа (патент РФ №2780400, опубл. 22.09.2022), содержащее  $n$  входов остатка, где  $n$  – количество модулей  $p_i$  системы остаточных классов,  $n$  регистров хранения разрядов исходного числа,  $n-1$  вычислительную ступень прямого хода, при этом  $i$ -я вычислительная ступень прямого хода, где  $i=1, \dots, n-1$ , содержит  $n-i$  сумматоров по модулю  $p_j$  и  $n-i$  блоков умножения на  $|p_i^{-1}|_{p_j}$  по модулю  $p_j$ , где  $j=i+1, \dots, n$  и  $|p_i^{-1}|_{p_j}$  – мультипликативная инверсия модуля  $p_i$  по модулю  $p_j$ ,  $n$  выходов прямого хода,  $n$  блоков перевода в СОК,  $n$  блоков хранения предвычисленных рангов,  $n$  выходов исходного числа, выход ранга, а также содержит  $n-1$  вычислительную ступень обратного хода, каждая из которых содержит  $n$  умножителей по модулю  $p_j$ ,  $n$  сумматоров по модулю  $p_j$ , где  $j=1, \dots, n$ , вычислитель ранга суммы, вычислитель ранга произведения.

Недостатком данного изобретения является избыточный объем оборудования и необходимость выполнять нахождение ранга в два этапа.

Техническим результатом заявляемого изобретения является сокращение оборудования.

Технический результат достигается тем, что в устройство вычисления ранга числа в системе остаточных классов, содержащее  $n$  входов остатка, где  $n$  – количество модулей  $p_i$  системы остаточных классов (СОК),  $n-1$  вычислительную ступень,  $n$  блоков вычисления ранга произведения, блок вычисления ранга суммы, при этом  $i$ -я вычислительная ступень, где  $i=1, \dots, n-1$ , содержит  $n-i$  сумматоров по модулю, в каждую вычислительную ступень введен блок вычисления кратности, введено  $n-1$  сумматоров,  $n$  умножителей,  $n$ -й блок вычисления кратности, при этом вход первого остатка соединен со входом блока

вычисления кратности первой вычислительной ступени, первый выход блока вычисления кратности первой вычислительной ступени соединен входом первого умножителя, второй выход блока вычисления кратности первой вычислительной ступени соединен входом первого блока вычисления ранга произведения и первыми входами  $n-1$  сумматоров по модулю первой вычислительной ступени, вторые входы которых соединены с входами остатка со второго по  $n$ -й соответственно, первые выходы  $n-1$  сумматоров по модулю первой вычислительной ступени соединены с первыми входами  $n-1$  сумматоров соответственно, в  $i$ -й вычислительной ступени,  $i=2, \dots, n-1$ , вход блока вычисления кратности  $i$ -й вычислительной ступени соединен со вторым выходом первого сумматора по модулю  $(i-1)$ -й вычислительной ступени, первый выход блока вычисления кратности  $i$ -й вычислительной ступени соединен с  $i$ -м входом  $(i-1)$ -го сумматора, второй выход блока вычисления кратности  $i$ -й вычислительной ступени соединен с входом  $i$ -го блока вычисления ранга произведения и первыми входами  $(n-i)$  сумматоров по модулю  $i$ -й вычислительной ступени, вторые входы которых соединены с выходами соответствующих  $(n-i)$  сумматоров по модулю  $(i-1)$ -й вычислительной ступени, со второго по  $(n-i+1)$ -й, первый выход  $j$ -го сумматора по модулю,  $j=1, \dots, n-i$ ,  $i$ -й вычислительной ступени соединен с  $i$ -м входом  $(i+j-1)$ -го сумматора, вход  $n$ -го блока вычисления кратности соединен с вторым выходом сумматора по модулю  $(n-1)$ -й вычислительной ступени, первый выход  $n$ -го блока вычисления кратности соединен с  $n$ -м входом  $(n-1)$ -го сумматора, второй выход  $n$ -го блока вычисления кратности соединен с входом  $n$ -го блока вычисления ранга произведения, выход  $i$ -го сумматора,  $i=1, \dots, n-1$ , соединен с входом  $(i+1)$ -го умножителя, выход  $i$ -го умножителя,  $i=1, \dots, n$ , соединен с  $(2i-1)$ -м входом блока вычисления ранга суммы, выход  $i$ -го блока вычисления ранга произведения,  $i=1, \dots, n$ , соединен с  $(2i)$ -м входом блока вычисления ранга суммы, на  $(2n+1)$ -й выход подается значение «-1», выход блока вычисления ранга суммы является выходом ранга устройства.

Сущность изобретения основана на следующем математическом аппарате. В системе остаточных классов (СОК) любое число  $X < P$  однозначно представляется набором остатков  $x_i$  от деления числа  $X$  на взаимно простые модули СОК  $p_i$ , где  $x_i \equiv X \pmod{p_i}$ ,  $P = \prod_{i=1}^n p_i$  - рабочий диапазон СОК,  $i=1, \dots, n$ .

Одним из самых распространенных методов перевода из СОК в позиционную систему является Китайская теорема об остатках, которая задается выражением:

$$X = \left| \sum_{i=1}^n B_i \cdot x_i \right|_P = \sum_{i=1}^n B_i \cdot x_i - r \cdot P \quad (1)$$

где  $B_i = P_i \cdot \left| P_i^{-1} \right|_{p_i}$  - ортогональные базисы СОК,  $P_i = \frac{P}{p_i}$ ,  $\left| P_i^{-1} \right|_{p_i}$  - мультипликативная инверсия  $P_i$  по модулю  $p_i$ , а оператором  $|X|_{p_i}$  обозначен остаток от деления  $X$  на  $p_i$ , т.е.  $X \pmod{p_i}$ . При этом ранг числа  $r$  показывает, во сколько раз сумма произведений остатков на ортогональные базисы превосходит динамический диапазон СОК.

Если в системе остаточных классов с модулями  $\{p_1, p_2, \dots, p_n\}$  и диапазоном  $P$  заданы два числа  $X = (x_1, x_2, \dots, x_n)$  и  $Y = (y_1, y_2, \dots, y_n)$  с рангами  $r_X$  и  $r_Y$  соответственно, то ранг  $r_{X+Y}$  суммы этих чисел равен

$$r_{X+Y} = r_X + r_Y - \sum_{i=1}^n \left\lfloor \frac{x_i + y_i}{p_i} \right\rfloor \cdot \left| P_i^{-1} \right|_{p_i}. \quad (2)$$

Чтобы упростить вычисление ранга, возьмем в качестве базисов ранга  $E_i$  числа, состоящие из  $i$  нулей и  $n-i$  единиц, т.е.  $E_0 = (1, 1, \dots, 1)$ ,  $E_1 = (0, 1, \dots, 1)$ , ...,  $E_{n-1} = (0, 0, \dots, 1)$ . Тогда любое число представляется с использованием данных базисов.

Для СОК с модулями  $\{p_1, p_2, \dots, p_n\}$  и базисов ранга  $E_i$ ,  $i = 0, \dots, n-1$ , где  $E_i = \underbrace{(0, \dots, 0}_i, \underbrace{1, \dots, 1}_{n-i})$ , для любого  $a \in N$ , удовлетворяющего условию  $0 \leq a < p_{k+1}$ , выполняется выражение

$$r(a \cdot E_k) = a \cdot r_{E_k} + \left\lfloor \frac{a}{M_k} \cdot \left\lfloor \frac{1}{\prod_{i=1}^k p_i} \right\rfloor_{M_k} \right\rfloor, \quad (3)$$

где для  $k = 0$ :  $\prod_{i=1}^0 p_i = 1$ ,  $M_0 = P$ , для  $k = 1, \dots, n-1$ :  $M_k = \frac{P}{\prod_{i=1}^k p_i}$ .

Значение рангов  $r_{E_i}$  вычисляются заранее. При этом при вычислении суммы исходного числа и масштабированного базиса  $a_i E_i$  переход через модуль  $\left\lfloor \frac{x_i + y_i}{p_i} \right\rfloor$  из формулы (2) фиксируется в переменной  $w_i$  и итоговая формула для вычисления ранга примет вид:

$$r(X) = \sum_{i=1}^n w_i \lfloor p_i^{-1} \rfloor_{p_i} - \sum_{i=1}^n r(a_i E_i) - 1, \quad (4)$$

где кратность  $a_i = p_i - x_i$ .

Рассмотрим пример для СОК  $\{2, 3, 5\}$  и числа  $X = 15 = (1, 0, 0)$ .

Остаток по модулю  $p_1$  равен 1. Вычислим кратность  $a_1 = p_1 - x_1 = 1$ . Поэтому возьмем  $E_0 = (1, 1, 1)$  с рангом  $r_{E_0} = 1$ .

При этом  $X + E_0 = (0, 1, 1)$  в котором был переход по модулю  $p_1$ ,  $w_1 = 1$ .

Так как остаток по модулю  $p_2$  числа  $X + E_0$  равен 1, то кратность  $a_2 = 3 - 1 = 2$  и для  $E_1 = (0, 1, 1)$  с рангом  $r_{E_1} = 0$  и  $M_1 = \frac{P}{p_1} = 15$ ,  $\left\lfloor \frac{1}{\prod_{i=1}^1 p_i} \right\rfloor_{M_1} = 8$  по формуле (3) ранг произведения равен

$$r_{2E_1} = 2 \cdot r_{E_1} + \left\lfloor \frac{2}{M_1} \cdot \left\lfloor \frac{1}{p_1} \right\rfloor_{M_1} \right\rfloor = 2 \cdot 0 + \left\lfloor \frac{2 \cdot 8}{15} \right\rfloor = 1.$$

Тогда  $X + E_0 + 2E_1 = (0, 1, 1) + (0, 2, 2) = (0, 0, 3)$ , при этом был переход по модулю  $p_2$ ,  $w_2 = 1$ .

Так как остаток по модулю  $p_3$  числа  $X + E_0 + 2E_1$  равен 3, то кратность  $a_3 = 5 - 3 = 2$  и для  $E_2 = (0, 0, 1)$  с рангом  $r_{E_2} = 0$  и  $M_2 = \frac{P}{p_1 p_2} = 5$ ,  $\left\lfloor \frac{1}{\prod_{i=1}^2 p_i} \right\rfloor_{M_2} = 1$  по формуле (3) ранг произведения равен

$$r_{2E_2} = 2 \cdot r_{E_2} + \left\lfloor \frac{2}{M_2} \cdot \left\lfloor \frac{1}{p_1 \cdot p_2} \right\rfloor_{M_2} \right\rfloor = 2 \cdot 0 + \left\lfloor \frac{2 \cdot 1}{5} \right\rfloor = 0.$$

Тогда  $X + E_0 + 2E_1 + 2E_2 = (0, 0, 3) + (0, 0, 2) = (0, 0, 0)$ , при этом был переход по модулю  $p_3$ ,  $w_3 = 1$ .

По формуле (4) получим

$$\begin{aligned} r(X) &= w_1 \lfloor p_1^{-1} \rfloor_{p_1} + w_2 \lfloor p_2^{-1} \rfloor_{p_2} + w_3 \lfloor p_3^{-1} \rfloor_{p_3} - r(E_0) - r(2E_1) - r(2E_2) - 1 = \\ &= 1 + 1 + 1 - 1 - 1 - 0 - 1 = 0. \end{aligned}$$

На фигуре 1 изображена структурная схема устройства, содержащая  $n$  входов остатка 1.1-1.n, где  $n$  – количество модулей системы остаточных классов,  $n-1$  вычислительную ступень, где  $i$ -я вычислительная ступень содержит блок вычисления кратности 2.i,  $n-i$  сумматор по модулю  $p_{i+j}$  3.i.j,  $j=1, \dots, n-i$ ;  $n$ -й блок вычисления кратности 2.n,  $n-1$  сумматор 4.1-4.n-1,  $n$  умножителей 5.1-5.n,  $n$  блоков вычисления ранга произведения 6.1-6.n, блок вычисления ранга суммы 7.

Блоки вычисления кратности  $2.i$  выполняют вычитание по модулю  $p_i$  значение входа из модуля  $p_i$ . Если значение входа не равно 0, то на первый выход блока вычисления кратности  $2.i$  подается значение 1, иначе 0. На второй выход блока вычисления кратности  $2.i$  подается значение разности модуля  $p_i$  и входа, т.е. число от 0 до  $p_i - 1$ . Таким образом, на первый вход подается слагаемое суммы  $w_i$ , а на второй – значение кратности  $a_i$ .

Сумматоры по модулю  $3.i.j$  вычисляет сумму входов по модулю  $p_{i+j}$ , при этом, если сумма больше модуля, на первый вход подается  $w_j = 1$ , иначе  $w_j = 0$ , на второй вход подается остаток от деления.

Сумматоры  $4.i$  выполняют подсчитывают количество сигналов на своих входах и на выход подают сумму значений  $w_i$  с первых выходов блоков вычисления кратности  $2.i$  и сумматоров по модулю  $3.i.j$ .

Умножители  $5.i$  выполняют умножение суммы  $w_i$  с выхода сумматора  $4.i$  с предвычисленным значением  $|P_i^{-1}|_{p_i}$ .

Блоки вычисления ранга произведения  $6.i$  выполняют вычисления по формуле (3) для кратности  $a_i$  с выхода блока вычисления кратности  $2.i$  и базиса  $E_{i-1}$ . При этом реализация данного блока возможна как в виде памяти, так и прямого вычисления по формуле (3).

Блок вычисления ранга суммы  $7$  выполняет вычисления по формуле (4), где на  $n$  нечетных входов подаются значения  $w_i |P_i^{-1}|_{p_i}$  с выходов умножителей  $5.i$ , на  $n$  четных входов подаются значения  $r(a_i E_i)$  с блоков вычисления ранга произведения  $6.i$ , на  $(2n+1)$ -й вход подается значение «-1».

Вход остатка  $1.1$  соединен с входом блока вычисления кратности  $2.1$  первой вычислительной ступени. Первый выход блока вычисления кратности  $2.1$  соединен с входом первого умножителя  $5.1$ , второй выход блока вычисления кратности  $2.1$  соединен с входом первого блока вычисления ранга произведения  $6.1$  и первым входам сумматоров по модулю  $3.1.1-3.1.n-1$  первой вычислительной ступени, вторые входы которых соединены с соответствующими входами остатков  $1.2-1.n$  со второго по  $n$ -й. Первые выходы сумматоров по модулю  $3.1.1-3.1.n-1$  первой вычислительной ступени соединены с первыми входами сумматоров  $4.1-4.n-1$ , второй выход первого сумматора по модулю  $3.1.1$  первой вычислительной ступени соединен с входом блока вычисления кратности  $2.2$  второй вычислительной ступени. Первый выход блока вычисления кратности  $2.2$  второй ступени соединен со вторым входом первого сумматора  $4.1$ , выход которого соединен с входом второго умножителя  $5.2$ , второй выход блока вычисления кратности  $2.2$  соединен с входом второго блока вычисления ранга произведения  $6.2$  и первым входам сумматоров по модулю  $3.2.1-3.2.n-2$  второй вычислительной ступени, вторые входы которых соединены с соответствующими выходами сумматоров по модулю  $3.1.2-3.1.n-1$  первой вычислительной ступени со второго по  $(n-1)$ -й. Первые выходы сумматоров по модулю  $3.2.1-3.1.n-2$  второй вычислительной ступени соединены со вторыми входами сумматоров  $4.2-4.n-1$ , второй выход первого сумматора по модулю  $3.2.1$  второй вычислительной ступени соединен с входом блока вычисления кратности  $2.3$  третьей вычислительной ступени. Аналогично по оставшимся вычислительным ступеням. Первый выход  $n$ -го блока вычисления кратности  $2.n$  соединен с  $n$ -м входом  $(n-1)$ -го сумматора  $4.n-1$ , выход

которого соединен с входом  $n$ -го умножителя  $5.n$ , второй выход  $n$ -го блока вычисления кратности  $2.n$  соединен с входом  $n$ -го блока вычисления ранга произведения  $6.n$ .

Значения с выходов умножителей  $5.i$  подаются на  $n$  нечетных входов блока вычисления ранга суммы  $7$ , с блоков вычисления ранга произведения  $6.i$  значения подаются на  $n$  четных входов блока вычисления ранга суммы  $7$ , на  $(2n+1)$ -й вход блока вычисления ранга суммы  $7$  подается значение «-1», выход блока вычисления ранга суммы  $7$  является выходом ранга устройства.

Рассмотрим пример устройства вычисления ранга числа в системе остаточных классов для  $n=3$  и набора модулей  $\{3,5,7\}$ , динамический диапазон которого равен  $P = 105$ .

Пусть на входы остатка 1.1-1.3 подаются числа 2, 2 и 3, что соответствует  $X = (2,2,3) = 17$ .

Тогда на вход первого блока вычисления кратности 2.1 первой вычислительной ступени поступает значение 2, в блоке вычисления кратности 2.1 происходит вычитание по модулю  $p_1 = 3$  значения входа из модуля, т.е.  $(3-2) \bmod 3$ , так как вход не равен 0, то на первый выход блока вычисления кратности 2.1 подается 1. На второй выход блока вычисления кратности 2.1 подается результат вычитания, т.е. 1.

На первый вход первого сумматора по модулю  $p_2$  3.1.1 первой вычислительной ступени поступает значение 1 со второго выхода блока вычисления кратности 2.1, на второй вход первого сумматора по модулю  $p_2$  3.1.1 первой вычислительной ступени поступает значение 2 со второго входа остатка 1.2. В первом сумматоре по модулю  $p_2$  3.1.1 первой вычислительной ступени происходит сложение по модулю 5, а именно  $1+2$ , таким образом на первый выход подается 0, поскольку перехода через модуль не было, на второй выход подается 3.

На первый вход второго сумматора по модулю  $p_3$  3.1.2 первой вычислительной ступени поступает значение 1 со второго выхода блока вычисления кратности 2.1, на второй вход второго сумматора по модулю  $p_3$  3.1.2 первой вычислительной ступени поступает значение 3 с третьего входа остатка 1.3. Во втором сумматоре по модулю  $p_3$  3.1.2 первой вычислительной ступени происходит сложение по модулю 7, а именно  $1+3$ , таким образом на первый выход подается 0, поскольку перехода через модуль не было, на второй выход подается 4.

На вход второго блока вычисления кратности 2.2 второй вычислительной ступени со второго выхода первого сумматора по модулю  $p_2$  3.1.1 первой вычислительной ступени поступает значение 3, в блоке вычисления кратности 2.2 происходит вычитание по модулю  $p_2 = 5$  значения входа из модуля, т.е.  $(5-3) \bmod 5$ , так как вход не равен 0, то на первый выход блока вычисления кратности 2.2 подается 1. На второй выход блока вычисления кратности 2.2 подается результат вычитания, т.е. 2.

На первый вход первого сумматора по модулю  $p_3$  3.2.1 второй вычислительной ступени поступает значение 2 со второго выхода блока вычисления кратности 2.2, на второй вход первого сумматора по модулю  $p_3$  3.2.1 второй вычислительной ступени поступает значение 4 со второго выхода сумматора по модулю  $p_3$  3.1.2 первой вычислительной ступени. В первом сумматоре по модулю  $p_3$  3.2.1 второй вычислительной ступени происходит сложение по модулю 7, а именно  $2+4$ , таким образом на первый выход подается 0, поскольку перехода через модуль не было, на второй выход подается 6.

На вход третьего блока вычисления кратности 2.3 со второго выхода первого сумматора по модулю  $p_2$  3.2.1 второй вычислительной ступени поступает значение 6, в блоке вычисления кратности 2.3 происходит вычитание по модулю  $p_3 = 7$  значения входа из модуля, т.е.  $(7-6) \bmod 7$ , так как вход не равен 0, то на первый выход блока вычисления кратности 2.3 подается 1. На второй выход блока вычисления кратности 2.3 подается результат вычитания, т.е. 1.

В первом сумматоре 4.1 происходит сложение 0 с первого выхода первого сумматора по модулю  $p_2$  3.1.1 первой вычислительной ступени и 1 с второго блока вычисления кратности 2.2 и на выход подается 1.

Во втором сумматоре 4.2 происходит сложение 0 с первого выхода второго сумматора по модулю  $p_3$  3.1.2 первой вычислительной ступени, 0 с первого выхода первого сумматора по модулю  $p_3$  3.2.1 второй вычислительной ступени и 1 с третьего блока вычисления кратности 2.3 и на выход подается 1.

В первом умножителе 5.1 происходит умножение сигнала с выхода первого блока вычисления кратности 2.1, т.е. 1, на  $|P_1^{-1}|_{p_1} = 2$ , и на выход подается 2.

Во втором умножителе 5.2 происходит умножение сигнала с выхода первого сумматора 4.1, т.е. 1, на  $|P_2^{-1}|_{p_2} = 1$ , и на выход подается 1.

В третьем умножителе 5.3 происходит умножение сигнала с выхода второго сумматора 4.2, т.е. 1, на  $|P_3^{-1}|_{p_3} = 1$ , и на выход подается 1.

В первом блоке вычисления ранга произведения 6.1 происходит по формуле (3), где  $E_0 = (1,1,1)$ ,  $r_{E_0} = 1$ ,  $M_0 = 105$ ,  $\left| \frac{1}{\prod_{i=1}^0 p_i} \right|_p = 1$ . Поскольку на вход блока вычисления ранга произведения 6.1 поступает  $a = 1$  со второго выхода первого блока вычисления кратности 2.1, то в блоке происходит вычисление

$$r(a \cdot E_0) = a \cdot r_{E_0} + \left[ \frac{a}{M_0} \cdot \left| \frac{1}{\prod_{i=1}^0 p_i} \right|_{M_0} \right] = 1 \cdot 1 + \left[ \frac{1}{105} \cdot 1 \right] = 1.$$

Во втором блоке вычисления ранга произведения 6.2 происходит по формуле (3), где  $E_1 = (0,1,1)$ ,  $r_{E_1} = 0$ ,  $M_1 = 35$ ,  $\left| \frac{1}{\prod_{i=1}^1 p_i} \right|_{M_1} = 12$ . Поскольку на вход блока вычисления ранга произведения 6.2 поступает  $a = 2$  со второго выхода второго блока вычисления кратности 2.2, то в блоке происходит вычисление

$$r(a \cdot E_1) = a \cdot r_{E_1} + \left[ \frac{a}{M_1} \cdot \left| \frac{1}{\prod_{i=1}^1 p_i} \right|_{M_1} \right] = 2 \cdot 0 + \left[ \frac{2}{25} \cdot \left| \frac{1}{3} \right|_{35} \right] = 2 \cdot 0 + \left[ \frac{2}{25} \cdot 12 \right] = 0.$$

Во третьем блоке вычисления ранга произведения 6.3 происходит по формуле (3), где  $E_2 = (0,0,1)$ ,  $r_{E_2} = 0$ ,  $M_2 = 7$ ,  $\left| \frac{1}{\prod_{i=1}^2 p_i} \right|_{M_2} = 1$ . Поскольку на вход блока вычисления ранга произведения 6.3 поступает  $a = 1$  со второго выхода третьего блока вычисления кратности 2.3, то в блоке происходит вычисление

$$r(a \cdot E_2) = a \cdot r_{E_2} + \left[ \frac{a}{M_2} \cdot \left| \frac{1}{\prod_{i=1}^2 p_i} \right|_{M_2} \right] = 1 \cdot 0 + \left[ \frac{1}{7} \cdot \left| \frac{1}{3 \cdot 5} \right|_7 \right] = 1 \cdot 0 + \left[ \frac{1}{7} \cdot 1 \right] = 0.$$

Блок вычисления ранга суммы 7 выполняет вычисления по формуле (4). В соответствии с формулой (4) складываются значения с выходов умножителей 5.1-5.3, а именно 2, 1 и 1 соответственно, складываются значения с выходов блоков вычисления

ранга произведения 6.1-6.3, а именно 1, 0 и 0. Далее из суммы значений умножителей 5.1-5.3 вычитается сумма значений блоков вычисления ранга произведения 6.1-6.3 и дополнительно вычитается 1, получаем

$$r(X) = \sum_{i=1}^n w_i |P_i^{-1}|_{p_i} - \sum_{i=1}^n r(a_i E_i) - 1 = (2 + 1 + 1) - (1 + 0 + 0) - 1 = 2.$$

На выход блока вычисления ранга суммы 7 подается значение 2, что соответствует рангу числа 17.

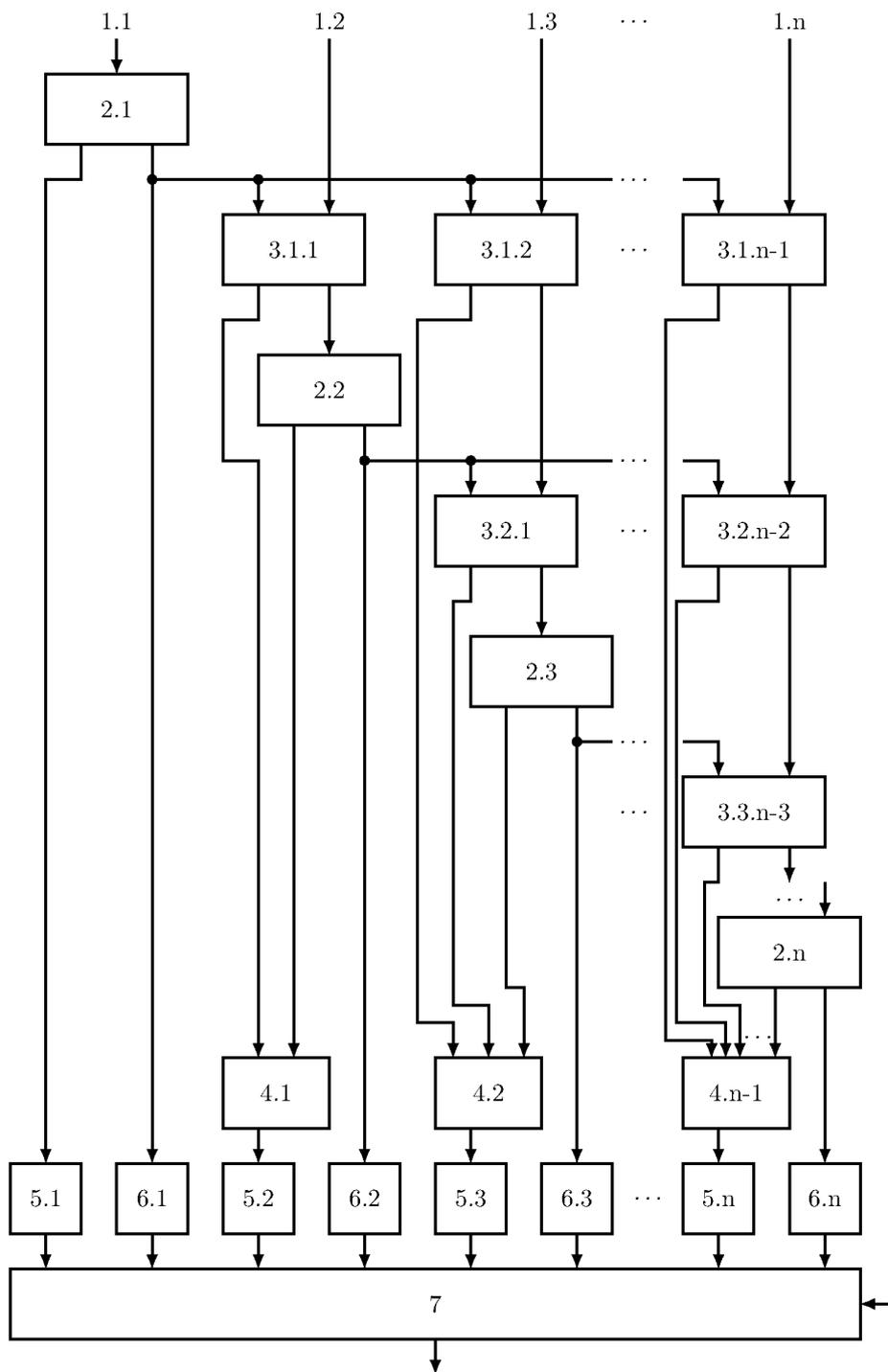
Реализация всего устройства возможна с использованием программируемых логических интегральных схем (ПЛИС), специализированных интегральных схем, а также в виде алгоритма работы ЭВМ и может использоваться как отдельное устройство, так и как сопроцессор для выполнения арифметических операций с рациональными числами в системе остаточных классов.

## Устройство вычисления ранга числа в системе остаточных классов

### Формула изобретения

Устройство вычисления ранга числа в системе остаточных классов, содержащее  $n$  входов остатка, где  $n$  – количество модулей  $p_i$  системы остаточных классов (СОК),  $n-1$  вычислительную ступень,  $n$  блоков вычисления ранга произведения, блок вычисления ранга суммы, при этом  $i$ -я вычислительная ступень, где  $i=1, \dots, n-1$ , содержит  $n-i$  сумматоров по модулю, отличающееся тем, что в каждую вычислительную ступень введен блок вычисления кратности, введено  $n-1$  сумматоров,  $n$  умножителей,  $n$ -й блок вычисления кратности, при этом вход первого остатка соединен со входом блока вычисления кратности первой вычислительной ступени, первый выход блока вычисления кратности первой вычислительной ступени соединен входом первого умножителя, второй выход блока вычисления кратности первой вычислительной ступени соединен входом первого блока вычисления ранга произведения и первыми входами  $n-1$  сумматоров по модулю первой вычислительной ступени, вторые входы которых соединены с входами остатка со второго по  $n$ -й соответственно, первые выходы  $n-1$  сумматоров по модулю первой вычислительной ступени соединены с первыми входами  $n-1$  сумматоров соответственно, в  $i$ -й вычислительной ступени,  $i=2, \dots, n-1$ , вход блока вычисления кратности  $i$ -й вычислительной ступени соединен со вторым выходом первого сумматора по модулю  $(i-1)$ -й вычислительной ступени, первый выход блока вычисления кратности  $i$ -й вычислительной ступени соединен с  $i$ -м входом  $(i-1)$ -го сумматора, второй выход блока вычисления кратности  $i$ -й вычислительной ступени соединен с входом  $i$ -го блока вычисления ранга произведения и первыми входами  $(n-i)$  сумматоров по модулю  $i$ -й вычислительной ступени, вторые входы которых соединены с выходами соответствующих  $(n-i)$  сумматоров по модулю  $(i-1)$ -й вычислительной ступени, со второго по  $(n-i+1)$ -й, первый выход  $j$ -го сумматора по модулю,  $j=1, \dots, n-i$ ,  $i$ -й вычислительной ступени соединен с  $i$ -м входом  $(i+j-1)$ -го сумматора, вход  $n$ -го блока вычисления кратности соединен с вторым выходом сумматора по модулю  $(n-1)$ -й вычислительной ступени, первый выход  $n$ -го блока вычисления кратности соединен с  $n$ -м входом  $(n-1)$ -го сумматора, второй выход  $n$ -го блока вычисления кратности соединен с входом  $n$ -го блока вычисления ранга произведения, выход  $i$ -го сумматора,  $i=1, \dots, n-1$ , соединен с входом  $(i+1)$ -го умножителя, выход  $i$ -го умножителя,  $i=1, \dots, n$ , соединен с  $(2i-1)$ -м входом блока вычисления ранга суммы, выход  $i$ -го блока вычисления ранга произведения,  $i=1, \dots, n$ , соединен с  $(2i)$ -м входом блока вычисления ранга суммы, на  $(2n+1)$ -й выход подается значение «-1», выход блока вычисления ранга суммы является выходом ранга устройства.

# Устройство вычисления ранга числа в системе остаточных классов



Фиг. 1. Структурная схема устройства

**ОТЧЕТ О ПАТЕНТНОМ ПОИСКЕ**  
(статья 15(3) ЕАПК и правило 42 Патентной инструкции к ЕАПК)

Номер евразийской заявки:

**202391055**

**А. КЛАССИФИКАЦИЯ ПРЕДМЕТА ИЗОБРЕТЕНИЯ:**

**G06F 7/72 (2006.01)**  
**G06F 7/06 (2006.01)**  
**G06F 7/49 (2006.01)**  
**G06F 13/00 (2006.01)**

Согласно Международной патентной классификации (МПК)

**Б. ОБЛАСТЬ ПОИСКА:**

Просмотренная документация (система классификации и индексы МПК)  
G06F 7/00-7/72; 13/00

Электронная база данных, использовавшаяся при поиске (название базы и, если, возможно, используемые поисковые термины)  
ЕАРАТIS, GOOGLE PATENTS, YANDEX, ESPACENET

**В. ДОКУМЕНТЫ, СЧИТАЮЩИЕСЯ РЕЛЕВАНТНЫМИ**

Категория*	Ссылки на документы с указанием, где это возможно, релевантных частей	Относится к пункту №
A	SU800989 (БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ) 30-01-1981 весь документ	1
A	EA202090736A1 (СЕВЕРО-КАВКАЗСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ) 19-08-2021 весь документ	1
A	BY3703 C1 (БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ) 30-12-2000 весь документ	1
A	SU951305 (ЧЕРВЯКОВ Н. И.) 15-08-1982 весь документ	1
A	US4704701A (RAYTHEON CO) 03-11-1987 весь документ	1
A	US5018093A (INTERNATIONAL BUSINESS MACHINES CORP) 21-05-1991 весь документ	1

последующие документы указаны в продолжении графы В

\* Особые категории ссылочных документов:

«А» - документ, определяющий общий уровень техники

«D» - документ, приведенный в евразийской заявке

«E» - более ранний документ, но опубликованный на дату подачи евразийской заявки или после нее

«O» - документ, относящийся к устному раскрытию, экспонированию и т.д.

"P" - документ, опубликованный до даты подачи евразийской заявки, но после даты испрашиваемого приоритета"

«Т» - более поздний документ, опубликованный после даты приоритета и приведенный для понимания изобретения

«X» - документ, имеющий наиболее близкое отношение к предмету поиска, порочащий новизну или изобретательский уровень, взятый в отдельности

«Y» - документ, имеющий наиболее близкое отношение к предмету поиска, порочащий изобретательский уровень в сочетании с другими документами той же категории

«&» - документ, являющийся патентом-аналогом

«L» - документ, приведенный в других целях

Дата проведения патентного поиска: **06/09/2023**

Уполномоченное лицо:  
Начальник отдела механики,  
физики и электротехники

 Д.Ф. Крылов