

(19)



**Евразийское
патентное
ведомство**

(11) **043517**(13) **B1**

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ЕВРАЗИЙСКОМУ ПАТЕНТУ

(45) Дата публикации и выдачи патента
2023.05.30

(21) Номер заявки
202291069

(22) Дата подачи заявки
2022.05.04

(51) Int. Cl. **G06F 7/57 (2006.01)**
G06F 7/52 (2006.01)
G06F 7/72 (2006.01)

(54) ВЫЧИСЛИТЕЛЬНОЕ УСТРОЙСТВО ДЛЯ РАБОТЫ С РАЦИОНАЛЬНЫМИ ЧИСЛАМИ В СИСТЕМЕ ОСТАТОЧНЫХ КЛАССОВ

(43) **2023.05.29**

(96) **2022000034 (RU) 2022.05.04**

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

(72) Изобретатель:

**Кучуков Виктор Андреевич, Бабенко
Михаил Григорьевич, Кучеров
Николай Николаевич, Гладков
Андрей Владимирович, Валуев
Георгий Вячеславович (RU)**

(74) Представитель:
Алиханов А.А. (RU)

(56) **US-A1-2013262549
KR-B1-100858559
DE-A1-102021119396
US-B2-7991812**

(57) Изобретение относится к вычислительной технике и предназначено для выполнения операций сложения, вычитания и умножения рациональных чисел, представленных в модулярно-позиционном формате. Техническим результатом предлагаемого изобретения является расширение функциональных возможностей, а именно выполнение вычислительным устройством операций сложения, умножения и вычитания чисел, представленных в беззнаковом модулярно-позиционном формате. Технический результат достигается тем, что в вычислительном устройстве для работы с рациональными числами в системе остаточных классов (СОК), в котором числа представлены в беззнаковом модулярно-позиционном формате $\{[m_1, m_2, \dots, m_n], \lambda, | m_i \in [0, p_i - 1], \lambda \in [\lambda'_{min}, \lambda'_{max}]\}$ с модулями СОК $p_i, i=1, \dots, n$, где m_i - остаток от деления целочисленной мантииссы на модуль p_i , а λ - перемещенный порядок числа, умножение выполняется параллельно по каждому модулю мантииссы в вычислительном блоке, а степень произведения получается сложением степеней в блоке вычисления степеней, отличающееся тем, что устройство содержит входы мантииссы первого и второго числа, входы степени первого и второго числа, вход операции, выходы степени результата, выход мантииссы результата, первый и второй мультиплексор, блок вычисления степеней, блок масштабирования, вычислительный блок, при этом вход мантииссы первого числа подключен к первым входам первого и второго мультиплексоров, вход мантииссы второго числа подключен к вторым входам первого и второго мультиплексоров, входы степеней первого и второго чисел подключены к первому и второму входам блока вычисления степеней, вход операции подключен к управляющим входам блока вычисления степеней и вычислительного блока, первый выход блока вычисления степеней подключен к управляющему входу второго мультиплексора и через инвертор к управляющему входу первого мультиплексора, второй выход блока вычисления степеней подключен к второму входу блока масштабирования, первый вход которого подключен к выходу второго мультиплексора, а выход подключен ко второму входу вычислительного блока, первый вход которого соединен с выходом первого мультиплексора, а выход является выходом мантииссы результата, третий выход блока вычисления степеней является выходом степеней результата.

043517 B1

043517 B1

Изобретение относится к вычислительной технике и предназначено для выполнения операций сложения, вычитания и умножения рациональных чисел, представленных в модулярно-позиционном формате.

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 $x_i \equiv X \bmod p_i = |X|_{p_i}$, $P = \prod_{i=1}^n p_i$ - рабочий диапазон СОК, $i = \overline{1, n}$.

При этом в общем случае СОК работает только с целыми числами.

Известно арифметико-логическое устройство, работающее в системе остаточных классов (патент US 2013311532, опубл. 21.11.2013). Дробное представление с фиксированной точкой для чисел СОК, раскрытое в данном изобретении, представлено следующим образом:

$$I_1, I_2, I_3, \dots, I_M \cdot F_1, F_2, F_3, \dots, F_N \quad (1)$$

где $I_1, I_2, I_3, \dots, I_M$ - модули для представления целой части, $F_1, F_2, F_3, \dots, F_N$ - для представления дробной части.

В данном случае диапазон дробных чисел равен $RF = F_1 \cdot F_2 \cdot F_3 \cdot \dots \cdot F_N$, тогда наименьшая представимая дробь равна

$$LF = \frac{1}{RF},$$

наибольшая представимая дробь

$$HF = \frac{RF - 1}{RF}.$$

Для перевода дроби в масштабированный вид её умножают на RF , округляют и переводят в СОК. Точное представление в данной СОК имеют только кратные LF . Для перевода из масштабированного режима в десятичную дробь делят на RF .

Сложение в данном случае выполняется аналогично обычному сложению в СОК. В случае дробного умножения имеем

$$\frac{Y_1}{RF} \cdot \frac{Y_2}{RF} = \frac{Y_1 \cdot Y_2}{RF \cdot RF}$$

Для получения корректного результата надо масштабировать на RF :

$$\frac{Y_1}{RF} \cdot \frac{Y_2}{RF} = \frac{Y_1 \cdot Y_2}{RF}$$

Недостатком данного устройства является необходимость выполнения деления для получения немасштабированного значения в СОК. Деление в СОК является немодульной операцией, которая является вычислительно сложной.

В стандарте IEEE-754 любое $(w+t+1)$ -разрядное вещественное число представляется трехэлементным набором

$$[M, e, S \mid M \in [0, 2), e \in [e_{\min}, e_{\max}], S \in \{0, 1\}]. \quad (2)$$

где M - рациональная мантисса, e - порядок числа, $e_{\min} = 2 - 2^{w-1}$ и $e_{\max} = 2^{w-1} - 1$, s - знак числа.

Величина $(w+t+1)$ -разрядного числа выражается формулой - $1^s \cdot M \cdot 2^e$, где t бит отводится под двоичную мантиссу, w бит под степень. Степень записывается в форме с избытком $E = e + e_{\max}$.

Известен способ организации выполнения операции умножения двух чисел в модулярно-позиционном формате представления с плавающей точкой на универсальных многоядерных процессорах (патент РФ № 2509345, опубл. 10.03.2014), выбранный в качестве прототипа. В данном патенте целочисленная мантисса M' определена так что $M = M' \cdot 2^{1-t}$ и её преобразуют в модулярную мантиссу

$$\overline{M} = \{m_1, m_2, \dots, m_n\} = \{|M'|_{p_1}, |M'|_{p_2}, \dots, |M'|_{p_n}\}$$

Перемещенный порядок числа $\lambda = e - t + 1$. Таким образом, в прототипе используют числа в модулярно-позиционном формате

$$\{m_1, m_2, \dots, m_n, \lambda, S \mid m_i \in [0, p_i - 1), \lambda \in [\lambda'_{\min}, \lambda'_{\max}], S \in \{0, 1\}\}. \quad (3)$$

Данный способ предполагает только операцию умножения, для которой множитель

$$A = \{m_1^A, m_2^A, \dots, m_n^A, \lambda_A, S_A\}$$

и множимое

$$B = \{m_1^B, m_2^B, \dots, m_n^B, \lambda_B, S_B\},$$

представленные в модулярно-позиционном формате с плавающей точкой, загружаются в память компьютера, в котором параллельно вычисляют умножения по модулям

$$\text{СОК } m_i^C = |m_i^A \cdot m_i^B|_{p_i}$$

для

получения мантиссы итогового числа, выполняют сложение двоичных порядков λ_A и λ_B , а также сложение по модулю два $s_C = |s_A + s_B|_2$ знаков s_A и s_B чисел A и B соответственно.

Недостатком данного способа является невозможность выполнения сложения и вычитания чисел, представленных в модулярно-позиционном формате.

Техническим результатом предлагаемого изобретения является расширение функциональных возможностей, а именно выполнение вычислительным устройством операций сложения, умножения и вычитания чисел, представленных в беззнаковом модулярно-позиционном формате.

Технический результат достигается тем, что в вычислительном устройстве для работы с рациональными числами в системе остаточных классов (СОК), в котором числа представлены в беззнаковом модулярно-позиционном формате $\{m_1, m_2, \dots, m_n, \lambda, | m_i \in [0, p_i - 1], \lambda \in [\lambda'_{min}, \lambda'_{max}]\}$ с модулями СОК $p_i, i=1, \dots, n$, где m_i остаток от деления целочисленной мантииссы на модуль p_i , а λ перемещенный порядок числа, умножение выполняется параллельно по каждому модулю мантииссы в вычислительном блоке, а степень произведения получается сложением степеней в блоке вычисления степеней, отличающееся тем что, устройство содержит входы мантииссы первого и второго числа, входы степени первого и второго числа, вход операции, выходы степени результата, выход мантииссы результата, первый и второй мультиплексор, блок вычисления степеней, блок масштабирования, вычислительный блок, при этом вход мантииссы первого числа подключен к первым входам первого и второго мультиплексоров, вход мантииссы второго числа подключен к вторым входам первого и второго мультиплексоров, входы степеней первого и второго чисел подключены к первому и второму входам блока вычисления степеней, вход операции подключен к управляющим входам блока вычисления степеней и вычислительного блока, первый выход блока вычисления степеней подключен к управляющему входу второго мультиплексора и через инвертор к управляющему входу первого мультиплексора, второй выход блока вычисления степеней подключен к второму входу блока масштабирования, первый вход которого подключен к выходу второго мультиплексора, а выход подключен ко второму входу вычислительного блока, первый вход которого соединен с выходом первого мультиплексора, а выход является выходом мантииссы результата, третий выход блока вычисления степеней является выходом степеней результата.

Сущность изобретения основана на следующем математическом аппарате. Величина $(w+t)$ -разрядного числа выражается формой $M \cdot 2^e$, где t бит выделено под двоичную мантииссу $M \in [0, 2)$, w бит под степень. Тогда минимальная и максимальные степени $e_{min} = 2 - 2^{w-1}$ и $e_{max} = 2^{w-1} - 1$ соответственно.

Значение t влияет на минимальное и максимальное представимые в данном случае числа. Например, поскольку $M \in [0, 2)$, то минимально представимая мантиисса равна $1/2^{t-1}$, максимально представимая мантиисса $2^t - 1/2^{t-1}$.

Таким образом, минимально представимое положительное число $\frac{1}{2^{t-1}} \cdot (2 - 2^{w-1})$, максимально представимое положительное число $\frac{2^t - 1}{2^{t-1}} \cdot (2^{w-1} - 1)$.

На основе значения размерности мантииссы t и значения степени e определяют смещенный порядок для данного числа $\lambda = e - t + 1$.

Поскольку система остаточных классов оперирует только целыми числами, для получения целочисленной мантииссы M' дробную мантииссу M умножают на 2^{t-1} . При двоичном умножении диапазон удваивается, поэтому в случае системы остаточных классов модули $p_1, p_2, \dots, p_n$ необходимо подбирать таким образом чтобы покрывать диапазон 2^{2t} . Тогда беззнаковое модулярно-позиционное представление

$$\{m_1, m_2, \dots, m_n, \lambda, | m_i \in [0, p_i - 1], \lambda \in [\lambda'_{min}, \lambda'_{max}]\}. \quad (4)$$

Степень результата для операции умножения λ_c равна сумме степеней сомножителей λ_A и λ_B , для сложения и вычитания степенью результата является наименьшая степень λ_A и λ_B , т.е.

$$\lambda_c = \begin{cases} \lambda_A + \lambda_B, & \text{для умножения} \\ \min(\lambda_A, \lambda_B), & \text{для сложения и вычитания} \end{cases}$$

При этом для умножения мантииссы первого и второго числа перемножаются по каждому модулю, для сложения и вычитания число с наивысшей степенью масштабируется на 2 в степени абсолютного значения разности λ_A и λ_B .

Рассмотрим пример.

Возьмем в качестве примера 8-битное число с $w=3$ и $t=5$. Для данной системы минимальная степень равно $e_{min} = 2 - 2^{3-1} = 2 - 4 = -2$, максимальная степень равно $e_{max} = 2^{3-1} - 1 = 4 - 1 = 3$

Тогда смещенный диапазон $\lambda = e - t + 1$, $\lambda \in [\lambda'_{min}, \lambda'_{max}] = [-2 - 5 + 1, 3 - 5 + 1] = [-6, -1]$.

Поскольку при умножении диапазон удваивается, для обеспечения корректности умножения подбирается набор модулей, произведение которых больше 2^{2t} . В частности, можно взять набор модулей специального вида $\{2^n - 1, 2^n, 2^n + 1\}$ при $n=4$, получим $\{15, 16, 17\}$ чей динамический диапазон равен 4080, который больше 2^{10} .

Рассмотрим пример для чисел $A=4.0$ и $B=2.5$. Тогда $A=1.0 \cdot 2^2$, $B=1.25 \cdot 2^1$.

Получим целочисленную мантииссу для данных чисел, для чего умножим мантииссу на $2^{t-1}=16$.

$$M'_A = 1.0 \cdot 16 = 16, M'_B = 1.25 \cdot 16 = 20.$$

Переведем целочисленные мантииссы в СОК

$$M_A^{RNS} = \{16|_{15}, 16|_{16}, 16|_{17}\} = \{1, 0, 16\}, M_B^{RNS} = \{20|_{15}, 20|_{16}, 20|_{17}\} = \{5, 4, 3\}.$$

Смещенный диапазон для этих чисел $\lambda_A = 2 - 5 + 1 = -2$, $\lambda_B = 1 - 5 + 1 = -3$.

Получили модулярно-позиционное представление $A_{RNS} = \{1, 0, 16\}, -2$, $B_{RNS} = \{5, 4, 3\}, -3$.

Рассмотрим операцию умножения $C = A \cdot B$. В данном случае числа в СОК перемножаются по стандартным правилам, а степени складываются.

$$M_C^{RNS} = M_A^{RNS} \cdot M_B^{RNS} = \{1 \cdot 5|_{15}, 0 \cdot 4|_{16}, 16 \cdot 3|_{17}\} = \{5, 0, 14\}.$$

Смещенный диапазон равен $\lambda_C = \lambda_A + \lambda_B = -2 - 3 = -5$.

Получим $C_{RNS} = \{5, 0, 14\}, -5$. По Китайской теореме об остатках (КТО) восстановим целочисленную мантииссу $\{5, 0, 14\} = 320$.

$$320 \cdot 2^{-5} = 10 = 2.5 \cdot 4.$$

Рассмотрим операцию сложения. Проблема в случае сложения заключается в выравнивании степени 2, для этого наибольшая степень складывается с разницей степеней, а число в СОК умножается на 2 в соответствующей степени, представленное в СОК.

Рассмотрим пример сложения для тех же чисел.

$$\begin{aligned} D_{RNS} &= A_{RNS} + B_{RNS} = \{1, 0, 16\} \cdot 2^{-2} + \{5, 4, 3\} \cdot 2^{-3} = \\ &= \{1, 0, 16\} \cdot \{2, 2, 2\} \cdot 2^{-2} \cdot 2^{-1} + \{5, 4, 3\} \cdot 2^{-3} = \\ &= (\{1, 0, 16\} \cdot \{2, 2, 2\} + \{5, 4, 3\}) \cdot 2^{-3} = \\ &= \{1 \cdot 2 + 5|_{15}, 0 \cdot 2 + 4|_{16}, 16 \cdot 2 + 3|_{17}\} \cdot 2^{-3} = \{7, 4, 1\} \cdot 2^{-3} \end{aligned}$$

$$\text{Получили } D = [\{7, 4, 1\}, -3] = 52 \cdot 2^{-3} = 6.5.$$

Рассмотрим пример вычитания для тех же чисел.

$$\begin{aligned} E_{RNS} &= A_{RNS} - B_{RNS} = \{1, 0, 16\} \cdot 2^{-2} - \{5, 4, 3\} \cdot 2^{-3} = \\ &= \{1, 0, 16\} \cdot \{2, 2, 2\} \cdot 2^{-2} \cdot 2^{-1} - \{5, 4, 3\} \cdot 2^{-3} = \\ &= (\{1, 0, 16\} \cdot \{2, 2, 2\} - \{5, 4, 3\}) \cdot 2^{-3} = \\ &= \{1 \cdot 2 - 5|_{15}, 0 \cdot 2 - 4|_{16}, 16 \cdot 2 - 3|_{17}\} \cdot 2^{-3} = \{12, 12, 12\} \cdot 2^{-3} \end{aligned}$$

$$\text{Получили } E = [\{12, 12, 12\}, -3] = 12 \cdot 2^{-3} = 1.5.$$

Изобретение поясняется фиг. 1, на которой изображена блок-схема устройства.

Мантииссы обрабатываемых чисел поступают на входы мантииссы первого числа 1 и второго числа 2, которые подключены к первым и вторым соответственно входам первого 6 и второго 7 мультиплексоров. При этом мантииссы представлены в системе остаточных классов и содержат набор остатков от деления целочисленной мантииссы на p взаимно простых модулей системы остаточных классов. Степени обрабатываемых чисел поступают на входы степени первого числа 3 и второго числа 4, которые подключены к первому и второму входам блока вычисления степеней 8 соответственно. Выполняемая операция (сложение, вычитание или умножение) с входа операции 5 поступает на управляющие входы блока вычисления степеней 8 и вычислительного блока 10. Блок вычисления степеней 8 для операции умножения, значение которой поступает на управляющий вход, на первый выход подает значение 0, которое поступая на управляющий вход второго мультиплексора 7 подает на выход через второй вход значение со входа мантииссы второго числа 2, также значение 0 с первого выхода блока вычисления степеней 8 через инвертор поступает на управляющий вход первого мультиплексора 6, подавая на выход через первый вход значение со входа мантииссы первого числа 1. Для операций сложения и вычитания на первый выход блока вычисления степеней 8 поступает значение логического выражения "степень первого числа больше либо равна степени второго числа", т.е. $\lambda_A \geq \lambda_B$. Таким образом когда степень первого числа больше, на первый выход блока вычисления степеней 8 поступает 1 и тогда на выходы первого 6 и второго 7 мультиплексоров поступают соответственно мантииссы второго и первого числа со входов мантииссы второго 2 и первого 1 чисел. На второй выход блока вычисления степеней 8 поступает значение, на которое необходимо масштабировать одно из чисел. Так для операции умножения масштабирование не требуется, поэтому на второй выход блока вычисления степеней 8 подается 2^0 , представленное в системе остаточных классов, т.е. $\{1, 1, \dots, 1\}$. Для операций сложения и вычитания на второй выход блока вычисления степеней 8 подается значение 2^k , представленное в СОК, где k - абсолютное значение разности степеней, поступающих на первый и второй входы блока вычисления степеней 8. Значение со второго выхода блока степеней 8 поступает на второй вход блока масштабирования 9, на первый вход которого поступает мантиисса с выхода второго мультиплексора 7. В блоке масштабирования 9 происходит параллельное умножение остатков мантииссы на остатки степени 2 по соответствующему модулю. Результат масштабирования поступает с выхода блока масштабирования 9 на второй вход вычислительного блока 10, на первый вход которого поступает мантиисса с выхода первого мультиплексора 6, и в зависимости от операции, подаваемой на

управляющий вход на выход, который является выходом мантиссы результата 12, подается результат умножения, сложения или вычитания по модулю. На третий вход блока вычисления степеней 8, который является выходом степени результата 11, для умножения поступает сумма степеней первого и второго чисел, для сложения и вычитания - наименьшая из степеней.

Рассмотрим приведенный выше пример сложения чисел $A_{RNS}=\{1,0,16\}$, -2 и $B_{RNS}=\{5,4,3\}$, -3 с помощью устройства.

На вход мантиссы первого числа 1 поступает мантисса $\{1,0,16\}$, на вход мантиссы второго числа 2 поступает мантисса $\{5,4,3\}$, на вход степени первого числа 3 поступает -2 , на вход степени второго числа 4 поступает -3 , на вход операции 5 поступает сигнал "сложение".

В блоке вычисления степеней 8 под действием управляющего сигнала "сложение" с управляющего входа происходит сравнение степеней первого и второго числа и поскольку логическое выражение "степень первого числа больше либо равна степени второго числа", т.е. $\lambda_A \geq \lambda_B$ выполняется, то на первый выход подается 1, тем самым на выходе первого мультиплексора 6 будет значение $\{5,4,3\}$ с входа мантиссы второго числа 2, а на выходе второго мультиплексора 7 будет значение $\{1,0,16\}$ с входа мантиссы первого числа 1.

На второй выход блока вычисления степеней 8 поступает значение $2^{\lfloor -2(-3) \rfloor} = 2 = \{2,2,2\}$.

На третий выход блока вычисления степеней 8 поступает наименьшее из степеней, т.е. $\min(-2, -3) = -3$.

В блоке масштабирования 9 происходит параллельное умножения по модулям значений $\{1,0,16\}$ с выхода второго мультиплексора 7 и $\{2,2,2\}$ со второго выхода блока вычисления степеней 8, т.е. выполняется $|1 \cdot 2|_{15}$, $|0 \cdot 2|_{16}$, $|16 \cdot 2|_{17}$.

Результат $\{2,0,15\}$ с выхода блока масштабирования 9 поступает на второй вход вычислительного блока 10, на первый вход которого поступает значение $\{5,4,3\}$ с выхода первого мультиплексора 6 и под действием сигнала "сложение" с управляющего входа происходит параллельное сложение по модулям, т.е. $|2+5|_{15}$, $|0+4|_{16}$, $|15+3|_{17}$. Результат $\{7,4,1\}$ поступает на выход вычислительного блока 10.

Таким образом на выходе мантиссы результата 12 будет значение $\{7,4,1\}$, на выходе степени результата 11 будет значение -3 , что соответствует вычисленному выше значению.

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.

ФОРМУЛА ИЗОБРЕТЕНИЯ

Вычислительное устройство для работы с рациональными числами в системе остаточных классов (СОК), в котором числа представлены в беззнаковом модулярно-позиционном формате $\{m_1, m_2, \dots, m_n\}, \lambda, | m_i \in [0, p_i - 1], \lambda \in [\lambda'_{min}, \lambda'_{max}]$ с модулями СОК $p_i, i=1, \dots, n$, где m_i - остаток от деления целочисленной мантиссы на модуль p_i , а λ - перемещенный порядок числа, умножение мантиссы выполняется параллельно по каждому модулю в вычислительном блоке, а степень произведения получается сложением степеней в блоке вычисления степеней, отличающееся тем, что устройство содержит входы мантиссы первого и второго числа, входы степени первого и второго числа, вход операции, выходы степени результата, выход мантиссы результата, первый и второй мультиплексор, блок вычисления степеней, блок масштабирования, вычислительный блок, при этом вход мантиссы первого числа подключен к первым входам первого и второго мультиплексоров, вход мантиссы второго числа подключен к вторым входам первого и второго мультиплексоров, входы степеней первого и второго чисел подключены к первому и второму входам блока вычисления степеней, вход операции подключен к управляющим входам блока вычисления степеней и вычислительного блока, первый выход блока вычисления степеней подключен к управляющему входу второго мультиплексора и через инвертор к управляющему входу первого мультиплексора, второй выход блока вычисления степеней подключен к второму входу блока масштабирования, первый вход которого подключен к выходу второго мультиплексора, а выход подключен ко второму входу вычислительного блока, первый вход которого соединен с выходом первого мультиплексора, а выход является выходом мантиссы результата, третий выход блока вычисления степеней является выходом степеней результата.

