УДК 004.052

МЕТОД ВЫПОЛНЕНИЯ НЕМОДУЛЬНЫХ ОПЕРАЦИЙ В СИСТЕМЕ ОСТАТОЧНЫХ КЛАССОВ НА ОСНОВЕ ИНТЕРВАЛЬНЫХ ПОЗИЦИОННЫХ ХАРАКТЕРИСТИК

Исупов К.С.

ФГБОУ ВПО «Вятский государственный университет», Киров, e-mail: isupov.k@gmail.com

Высокая трудоемкость немодульных операций в системе остаточных классов (сравнение по величине, вычитание с получением отрицательного результата, определение переполнения и т.д.) не позволяет в полной мере использовать все достоинства данной системы, заключающиеся в возможности параллельной обработки отдельных разрядов чисел. Точные методы выполнения немодульных операций (преобразование к обобщенной позиционной системе, использование функции ядра, SQT-метод и т.д.) требуют больших временных либо аппаратурных затрат на реализацию, а приближенный метод не всегда позволяет получить корректный результат. В статье предлагается новый метод выполнения немодульных операций в СОК, основанный на концепциях интервальных (доказательных, достоверных) вычислений. Метод обладает низкой вычислительной и аппаратурной сложностью, но при этом обеспечивает получение достоверного результата операции.

Ключевые слова: система остаточных классов, немодульная операция, достоверные вычисления, интервальная позиционная характеристика

METHOD FOR IMPLEMENTATION NON-MODULAR OPERATIONS IN RNS BASED ON INTERVAL POSITIONAL CHARACTERISTIC

Isupov K.S.

Vyatka State University, Kirov, e-mail: isupov.k@gmail.com

The high complexity of non-modular operations in the residue number system (magnitude comparison, subtraction with a negative result, overflow detection etc.) does not allow the full use of all the advantages of this system, which consist of parallel processing of individual digits of numbers. Accurate methods for implementation non-modular operations in RNS (Mixed-Radix Conversion, Core-Function, Sum of Quotients Technique etc.) require high computational or hardware expenses, and approximate method does not always produce the correct result of operation. In this article we propose a new method for implementation non-modular operations in RNS which based on interval (verified) computation. This method has low computational and hardware complexity, and provides verified non-modular operation result.

Keywords: residue number system, non-modular operation, verified computing, interval positional characteristic

Если задан ряд положительных целых чисел $p_1, p_2, \ldots, p_n$, называемых основаниями (модулями) системы, то под *системой счисления в остаточных классах* (СОК) понимают такую систему, в которой целое число $X \in [0, P-1]$, где $P = p_1 \cdot p_2 \cdot \ldots \cdot p_n$, представляется в виде остатков по выбранным основаниям [1, 7]:

$$\tilde{X} = \langle x_1, x_2, \ldots, x_n \rangle; \quad x_i \equiv X \ (\mathrm{mod}) p_i \ , \tag{1}$$

т.е. цифра i-го разряда x_i числа $\tilde{X}$, называемого *модулярным числом*, есть наименьший неотрицательный остаток от деления позиционного числа X на p_i. Если все p_i попарно взаимно простые, то между множеством $\{X \mid X \in [0, P-1]\}$ и множеством кортежей $\{\langle x_1, x_2, \ldots, x_n \rangle\}$ однозначным образом определяется биекция $\{X\} \leftrightarrow \{\langle x_1, x_2, \ldots, x_n \rangle\}$, причем прямое преобразование задается в соответствии с (1), а обратное определяется формулой

$$X = \left| \sum_{i=1}^{n} x_i B_i \right|_P . \tag{2}$$

Здесь числа B_i представляют собой *ортогональные базисы* СОК [1].

Определенная таким образом система обладает рядом важных достоинств. Отдельные разряды модулярных чисел малоразрядные и могут обрабатываться без учета переносов между ними, поэтому СОК отвечает многоядерной архитектуре современных вычислительных устройств. На основе СОК могут быть построены эффективные параллельные алгоритмы для решения задач из самых разнообразных областей знаний. Базовые арифметические операции в СОК делятся на следующие две группы [1, 7].

1. *Модульные операции*, которые могут быть выполнены параллельно и независимо над отдельными цифрами чисел (1), например, сложение, умножение, вычитание без знака и т.д.

2. *Немодульные операции*, которые требуют знания величины модулярных чисел в целом. К данной группе относятся: сравнение, вычитание с получением отрицательного результата, контроль переполнения модулярного числа и т.д.

Основным фактором, сдерживающим широкое применение СОК на практике,

является неочевидность выполнения *немодульных операций* [1, 3, 5–7].

1. Выполнение немодульных операций в системе остаточных классов

Для выполнения немодульных операций в СОК применяются, как правило, точные методы, основанные на вычислении *точных позиционных характеристик* модулярных чисел. Всякая позиционная характеристика представляет собой выраженную тем или иным способом информацию о позиционном значении модулярного числа (1). К наиболее известным точным позиционным характеристикам относятся коэффициенты обобщенной позиционной системы счисления (ОПСС), ранг, след, функция ядра и т.д. [1, 3, 7]. Недостатком методов, основанных на вычислении точных позиционных характеристик, является их высокая временная либо аппаратная сложность реализации [7].

Альтернативой точных является приближенный метод выполнения немодульных операций [5, 6]. Он основан на вычислении *приближенной позиционной характеристики*, которая представляет собой округленное до машинного представления значение отношения анализируемого модулярного числа к произведению модулей СОК. Вычисление приближенной характеристики осуществляется за малое время и при этом не требует хранения больших подстановочных таблиц. При знании приближенных характеристик чисел в СОК операции определения знака, сравнения, обнаружения ошибки и переполнения выполняются простым образом [5, 6]. Однако погрешности округления, возникающие в ходе вычисления приближенной характеристики, могут приводить к некорректному выполнению немодульных операций. Оценить эти погрешности и определить, что операция выполнена некорректно, весьма сложно без знания позиционного значения соответствующего модулярного числа. Это затрудняет использование приближенного метода на практике.

2. Метод выполнения немодульных операций на основе интервальных позиционных характеристик

Определение. Всякую немодульную операцию над модулярными числами будем называть *достоверной* тогда и только тогда, когда ее результат либо является корректным, либо за время, сопоставимое со временем выполнения данной операции, может быть доказательно определена невозможность получения корректного результата.

Решить проблему достоверности приближенного метода выполнения немодульных операций, сохранив при этом его преимущества, заключающиеся в низкой вычислительной и аппаратурной сложности, позволяет метод, основанный на применении *интервальных позиционных характеристик*. Предлагаемый метод опирается на базовые концепции интервальных (достоверных, доказательных) вычислений [2, 4] и состоит в следующем.

Пусть в СОК с модулями $P = p_1, p_2, ..., p_n$ задано модулярное число $\tilde{X} = \langle x_1, x_2, ..., x_n \rangle$. Пусть $C_{\tilde{X}}$ – точное значение отношения $\tilde{X}/\mathrm{P}$, где $\mathrm{P} = p_1 \cdot p_2 \cdot ... \cdot p_n$. $C_{\tilde{X}}$ по определению представляет собой рациональное число, разрядность которого определяется разрядностью P и может быть в общем случае много больше разрядности вычислительного устройства.

Определение. Вещественный интервал $I_{\tilde{X}/\mathrm{P}} = \left[\downarrow \frac{\tilde{X}}{\mathrm{P}}, \uparrow \frac{\tilde{X}}{\mathrm{P}} \right]$ с рациональными границами $\downarrow \frac{\tilde{X}}{\mathrm{P}} = \inf I_{\tilde{X}/\mathrm{P}}$ и $\uparrow \frac{\tilde{X}}{\mathrm{P}} = \sup I_{\tilde{X}/\mathrm{P}}$, направленно округленными до размера разрядной сетки вычислительного устройства и отвечающими условию $\downarrow \frac{\tilde{X}}{\mathrm{P}} \le C_{\tilde{X}} \le \uparrow \frac{\tilde{X}}{\mathrm{P}}$, называется *интервальной позиционной характеристикой* модулярного числа $\tilde{X}$. Стоит различать интервальную позиционную характеристику и интервальный номер модулярного числа [1].

Границы, задающие интервальную позиционную характеристику, определяются с помощью направленных округлений: нижняя граница округляется до ближайшего машинного числа с недостатком, а верхняя – с избытком:

$$\downarrow \frac{\tilde{X}}{\mathrm{P}} \approx \left| \sum_{i=1}^{n} \downarrow \left(\frac{N_i}{p_i} \right) \right|_1, \uparrow \frac{\tilde{X}}{\mathrm{P}} \approx \left| \sum_{i=1}^{n} \uparrow \left(\frac{N_i}{p_i} \right) \right|_1, \quad (3)$$

где $N_i = \left| \left| \mathrm{P}_i^{-1} \right|_{p_i} x_i \right|_{p_i}$. Здесь операторы $\downarrow$ и $\uparrow$ отвечают округлениям с недостатком и избытком соответственно. Техника выполнения этих округлений для различных способов представления чисел неоднократно освещалась в литературе (см., например, работы [3, 8]).

Интервальная позиционная характеристика $I_{\tilde{X}/\mathrm{P}}$ модулярного числа $\tilde{X}$ позволяет единообразным способом учесть погрешности округлений, неизбежно возникающие при сопоставлении точному значению

$C_{\tilde{X}} = \tilde{X}/\mathrm{P}$ представления с ограниченной разрядностью: $C_{\tilde{X}}$ заключается в гарантированно содержащие это значение границы, направленно округленные до разрядности машинного представления. При этом погрешности округлений лишь несколько расширяют границы, оставляя включение $C_{\tilde{X}} \in I_{\tilde{X}/\mathrm{P}}$ истинным.

Пример. Пусть $p_1 = 7, p_2 = 9, p_3 = 11, p_4 = 13$ – модули СОК, $\mathrm{P} = 9009$ – их произведение,

$$\left|\mathrm{P}_1^{-1}\right|_{p_1} = 6, \quad \left|\mathrm{P}_2^{-1}\right|_{p_2} = 5, \quad \left|\mathrm{P}_3^{-1}\right|_{p_3} = 9,$$

$\left|\mathrm{P}_4^{-1}\right|_{p_4} = 10$ – соответствующие мультипликативные инверсии [1, 7]. Тогда интервальная позиционная характеристика модулярного числа $\tilde{X} = \langle 6,1,0,8 \rangle$ определится в соответствии с (3) следующим образом:

$$\downarrow \frac{\tilde{X}}{\mathrm{P}} = \left| \downarrow \frac{|6\cdot 6|_7}{7} + \downarrow \frac{|5\cdot 1|_9}{9} + \downarrow \frac{|9\cdot 0|_{11}}{11} + \downarrow \frac{|10\cdot 8|_{13}}{13} \right|_1 \approx 0{,}84;$$

$$\uparrow \frac{\tilde{X}}{\mathrm{P}} = \left| \uparrow \frac{|6\cdot 6|_7}{7} + \uparrow \frac{|5\cdot 1|_9}{9} + \uparrow \frac{|9\cdot 0|_{11}}{11} + \uparrow \frac{|10\cdot 8|_{13}}{13} \right|_1 \approx 0{,}87.$$

Таким образом, $I_{\tilde{X}/\mathrm{P}} = [0{,}84;\ 0{,}87]$, причем гарантируется, что точное значение $\tilde{X}/\mathrm{P}$ лежит в указанном интервале. В соответствии с (2), $\tilde{X} = \langle 6,1,0,8 \rangle \mapsto 7678_{10}$, поэтому $C_{\tilde{X}} \approx 0{,}852$.

Определение. Для любого модулярного числа $\tilde{X}$ его интервальная позиционная характеристика $I_{\tilde{X}/\mathrm{P}}$ является *корректной* тогда и только тогда, когда $\downarrow \frac{\tilde{X}}{\mathrm{P}} \le \uparrow \frac{\tilde{X}}{\mathrm{P}}$.

Необходимым условием правильного выполнения немодульных операций над модулярными числами $\tilde{X}$ и $\tilde{Y}$ с помощью их интервальных позиционных характеристик $I_{\tilde{X}/\mathrm{P}}$ и $I_{\tilde{Y}/\mathrm{P}}$ соответственно является корректность как $I_{\tilde{X}/\mathrm{P}}$, так и $I_{\tilde{Y}/\mathrm{P}}$.

Определение. *Диаметром* интервальной позиционной характеристики называется разность ее верхней и нижней границ:

$$d\left(I_{\tilde{X}/\mathrm{P}}\right) = \uparrow \frac{\tilde{X}}{\mathrm{P}} - \downarrow \frac{\tilde{X}}{\mathrm{P}}. \qquad (4)$$

Погрешности округления границ при вычислении интервальной позиционной характеристики прямым образом отражаются в ее диаметре [4]. Если для машинного представления границ отведено k двоичных разрядов, а модулярное число задается n k-разрядными модулями СОК, то $d\left(I_{\tilde{X}/\mathrm{P}}\right) < 2^{2-k} n$.

Определение. Пусть $I_{\tilde{X}/\mathrm{P}}$ и $I_{\tilde{Y}/\mathrm{P}}$ – интервальные позиционные характеристики модулярных чисел $\tilde{X}$ и $\tilde{Y}$ соответственно. Тогда отношение

$$I_{\tilde{X}/\mathrm{P}} \cap I_{\tilde{Y}/\mathrm{P}} = \left\{ a \mid a \in I_{\tilde{X}/\mathrm{P}} \wedge a \in I_{\tilde{Y}/\mathrm{P}} \right\}$$

суть теоретико-множественное пересечение $I_{\tilde{X}/\mathrm{P}}$ и $I_{\tilde{Y}/\mathrm{P}}$.

Если пересечение не пусто, то его результат может быть представлен интервалом

$$I_{\tilde{X}/\mathrm{P}} \cap I_{\tilde{Y}/\mathrm{P}} = \left[\max\left(\downarrow \frac{\tilde{X}}{\mathrm{P}}, \downarrow \frac{\tilde{Y}}{\mathrm{P}} \right),\ \min\left(\uparrow \frac{\tilde{X}}{\mathrm{P}}, \uparrow \frac{\tilde{Y}}{\mathrm{P}} \right) \right],$$

причем в этом случае в соответствии с (4) $d\left(I_{\tilde{X}/\mathrm{P}} \cap I_{\tilde{Y}/\mathrm{P}}\right) \ge 0$.. Если $d\left(I_{\tilde{X}/\mathrm{P}} \cap I_{\tilde{Y}/\mathrm{P}}\right) < 0$, то $I_{\tilde{X}/\mathrm{P}} \cap I_{\tilde{Y}/\mathrm{P}} = \varnothing$.. Если $I_{\tilde{X}/\mathrm{P}}$ и $I_{\tilde{Y}/\mathrm{P}}$ пересекаются, то справедливо одно из утверждений:

1. Модулярные числа $\tilde{X}$ и $\tilde{Y}$ равны. В этом случае всякая немодульная операция над ними выполняется интуитивным образом.

2. Модулярные числа различны, но отношение их разности к произведению модулей СОК находится в пределах погрешностей, определяющих диаметры характеристик $I_{\tilde{X}/\mathrm{P}}$ и $I_{\tilde{Y}/\mathrm{P}}$. В этом случае выполнение всякой немодульной операции над числами $\tilde{X}$ и $\tilde{Y}$ при помощи $I_{\tilde{X}/\mathrm{P}}$ и $I_{\tilde{Y}/\mathrm{P}}$ может дать некорректный результат, поэтому следует прибегнуть к использованию точных методов, например, преобразовав $\tilde{X}$ и $\tilde{Y}$ в ОПСС.

Таким образом, **достаточным условием** корректности выполнения немодульных операций над модулярными числами $\tilde{X}$ и $\tilde{Y}$ с помощью их интервальных позиционных характеристик $I_{\tilde{X}/\mathrm{P}}$ и $I_{\tilde{Y}/\mathrm{P}}$ является пустое пересечение $I_{\tilde{X}/\mathrm{P}} \cap I_{\tilde{Y}/\mathrm{P}} = \varnothing$..

Теорема. Если для модулярных чисел $\tilde{X}$ и $\tilde{Y}$ их интервальные характеристики $I_{\tilde{X}/\mathrm{P}}$ и $I_{\tilde{Y}/\mathrm{P}}$ корректны (см. определение выше), а $I_{\tilde{X}/\mathrm{P}} \cap I_{\tilde{Y}/\mathrm{P}} = \varnothing$., то результат всякой немодульной операции над $\tilde{X}$ и $\tilde{Y}$, выполняемой при помощи $I_{\tilde{X}/\mathrm{P}}$ и $I_{\tilde{Y}/\mathrm{P}}$, будет корректным.

Доказательство теоремы исходит из замечания, что большинство немодульных операций над модулярными числами, так или иначе, сводятся к сравнению по величине этих чисел. Поэтому можно считать, что немодульная операция над $\tilde{X}$ и $\tilde{Y}$, выполняемая при помощи $I_{\tilde{X}/\mathrm{P}}$ и $I_{\tilde{Y}/\mathrm{P}}$, некорректна, если истинно одно из следующих утверждений:

$$I_{\tilde{X}/\mathrm{P}} \le I_{\tilde{Y}/\mathrm{P}} \wedge \tilde{X} > \tilde{Y};$$

$$I_{\tilde{X}/\mathrm{P}} \ge I_{\tilde{Y}/\mathrm{P}} \wedge \tilde{X} < \tilde{Y}.$$

Далее доказывается невозможность выполнения ни одного из этих утверждений.

Представленная теорема является **обоснованием достоверности** немодульных операций. Это означает, что всякая немодульная операция над модулярными числами, выполняемая с помощью их интервальных позиционных характеристик, либо будет выполнена корректно, либо будет сделан вывод о невозможности ее корректного выполнения. Арифметические операции сложения и вычитания интервальных характеристик определяются следующими формулами [2, 4]:

$$I_{\tilde{X}/\mathrm{P}} + I_{\tilde{Y}/\mathrm{P}} = \left[\left(\downarrow\frac{\tilde{X}}{\mathrm{P}} + \downarrow\frac{\tilde{Y}}{\mathrm{P}}\right), \left(\uparrow\frac{\tilde{X}}{\mathrm{P}} + \uparrow\frac{\tilde{Y}}{\mathrm{P}}\right)\right]; \quad (5)$$

$$I_{\tilde{X}/\mathrm{P}} - I_{\tilde{Y}/\mathrm{P}} = \left[\left(\downarrow\frac{\tilde{X}}{\mathrm{P}} - \uparrow\frac{\tilde{Y}}{\mathrm{P}}\right), \left(\uparrow\frac{\tilde{X}}{\mathrm{P}} - \downarrow\frac{\tilde{Y}}{\mathrm{P}}\right)\right]. \quad (6)$$

Умножение и деление определяется аналогичным образом [6, 7]. Правила выполнения основных немодульных операций в СОК с использованием интервальных позиционных характеристик модулярных чисел аналогичны правилам, справедливым для точечного представления приближенной позиционной характеристики, представленным в работах [5, 6]. Пусть, например, $\tilde{X} = \langle x_1, x_2, ..., x_n \rangle$ и $\tilde{Y} = \langle y_1, y_2, ..., y_n \rangle$ – модулярные числа, а $I_{\tilde{X}/\mathrm{P}}$ и $I_{\tilde{Y}/\mathrm{P}}$ – их интервальные позиционные характеристики, вычисленные в соответствии с (3) и отвечающие необходимому и достаточному условиям корректности немодульных операций. Тогда сравнение по величине $\tilde{X}$ и $\tilde{Y}$ определится следующим образом:

$$I_{\tilde{X}/\mathrm{P}} - I_{\tilde{Y}/\mathrm{P}} = 0 \Rightarrow \tilde{X} = \tilde{Y};$$

$$I_{\tilde{X}/\mathrm{P}} - I_{\tilde{Y}/\mathrm{P}} > 0 \Rightarrow \tilde{X} > \tilde{Y};$$

$$I_{\tilde{X}/\mathrm{P}} - I_{\tilde{Y}/\mathrm{P}} < 0 \Rightarrow \tilde{X} < \tilde{Y}.$$

Определение переполнения при сложении чисел в СОК выполняется следующим образом:

$$I_{\tilde{X}/\mathrm{P}} + I_{\tilde{Y}/\mathrm{P}} \ge 1 \Rightarrow \left(\tilde{X} + \tilde{Y}\right) \ge \mathrm{P};$$

$$I_{\tilde{X}/\mathrm{P}} + I_{\tilde{Y}/\mathrm{P}} < 0 \Rightarrow \left(\tilde{X} + \tilde{Y}\right) < \mathrm{P}.$$

Аналогично определяются и другие немодульные операции, такие как контроль переполнения при умножении, определение знака модулярного числа в дополнительном коде, вычитание с возможностью получения отрицательного результата и т.д.

Примеры. Будем использовать следующие модули СОК: $p_1 = 7$, $p_2 = 9$, $p_3 = 11$, $p_4 = 13$, их мультипликативные инверсии:

$$\left|\mathrm{P}_1^{-1}\right|_{p_1} = 6, \quad \left|\mathrm{P}_2^{-1}\right|_{p_2} = 5, \quad \left|\mathrm{P}_3^{-1}\right|_{p_3} = 9,$$

$$\left|\mathrm{P}_4^{-1}\right|_{p_4} = 10.$$

1) Выполним сравнение $\tilde{X} = \langle 4, 0, 6, 10 \rangle$ и $\tilde{Y} = \langle 0, 2, 10, 1 \rangle$. Для этого определим их интервальные характеристики в соответствии с выражением (3), округляя границы до двух разрядов:

$$\downarrow\frac{\tilde{X}}{\mathrm{P}} \approx 0{,}01, \quad \uparrow\frac{\tilde{X}}{\mathrm{P}} \approx 0{,}04,$$

$$\downarrow\frac{\tilde{Y}}{\mathrm{P}} \approx 0{,}05, \quad \uparrow\frac{\tilde{Y}}{\mathrm{P}} \approx 0{,}08,$$

таким образом $I_{\tilde{X}/\mathrm{P}} = [0{,}01; 0{,}04]$, $I_{\tilde{Y}/\mathrm{P}} = [0{,}05; 0{,}08]$. Данные характеристики корректны, а $I_{\tilde{X}/\mathrm{P}} \cap I_{\tilde{Y}/\mathrm{P}} = \varnothing$, поэтому за-

ключаем, что операция сравнения чисел $\tilde{X}$ и $\tilde{Y}$ с их помощью будет выполнена верно. Выполняя вычитание в соответствии с (6), получим

$$I_{\tilde{X}/\mathrm{P}} - I_{\tilde{Y}/\mathrm{P}} = [-0{,}07;\ -0{,}01] < 0,$$

поэтому $\tilde{X} < \tilde{Y}$. И действительно

$$\tilde{X} = \langle 4,0,6,10 \rangle \mapsto 270_{10};$$
$$\tilde{Y} = \langle 0,2,10,1 \rangle \mapsto 560_{10}.$$

2) Пусть $\tilde{X} = \langle 1,\ 6,\ 5,7 \rangle$, $\tilde{Y} = \langle 3,\ 6,\ 0,11 \rangle$ и требуется определить, произойдет или нет переполнение при их сложении. Определяем интервальные позиционные характеристики: $I_{\tilde{X}/\mathrm{P}} = [0{,}014;0{,}04]$, $I_{\tilde{Y}/\mathrm{P}} = [0{,}05;0{,}08]$. Данные характеристики отвечают необходимому и достаточному условиям корректности выполнения немодульной операции. В соответствии с (5) имеем:

$$I_{\tilde{X}/\mathrm{P}} + I_{\tilde{Y}/\mathrm{P}} = [1{,}01;1{,}08] > 1,$$

следовательно, при сложении $\tilde{X}$ и $\tilde{Y}$ произойдет переполнение. В правильности полученного вывода можно убедиться, преобразовав операнды в позиционную систему:

$$\tilde{X} = \langle 1,6,5,7 \rangle \mapsto 6000_{10};$$
$$\tilde{Y} = \langle 3,6,0,11 \rangle \mapsto 3300_{10}.$$

Вычисление первой границы интервальной характеристики требует n обращений к LUT-памяти за значениями мультипликативных инверсий, n умножений, n делений и одну операцию n-операндного суммирования с отбрасыванием целой части, которая выполнится (последовательно) также за n тактов. При вычислении второй границы значения произведений модулярных разрядов и соответствующих мультипликативных инверсий (слагаемые Ni в (3)) уже будут вычислены, поэтому необходимо лишь поделить их на модули СОК, округлив соответствующим образом, и сложить. Таким образом, вычисление интервальной позиционной характеристики требует выполнения $6n$ операций над машинными числами (n – количество модулей СОК). Для сравнения, алгоритм Гарнера [3], основанный на использовании в качестве позиционной характеристики коэффициентов ОПСС, требует для их определения в среднем n^2 операций.

Заключение

Предложен асимптотически быстрый метод выполнения немодульных операций в СОК, основанный на использовании интервальных позиционных характеристик для оценки величины модулярных чисел. Данный метод обеспечивает достоверность выполняемых операций в отличие от приближенного метода и не требует больших вычислительных либо аппаратурных затрат в отличие от известных точных методов. Алгоритм вычисления интервальных позиционных характеристик не требует работы с числами, выходящими за пределы разрядной сетки, а его временная сложность линейна по количеству модулей СОК. Таким образом, предложенный метод является полезной альтернативой известным методам выполнения немодульных операций в СОК.

Список литературы

1. Машинная арифметика в остаточных классах / И.Я. Акушский, Д.И. Юдицкий. – М.: Советское радио, 1968. – 440 с.

2. Введение в интервальные вычисления / Г. Алефельд, Ю. Херцбергер. – М.: Мир, 1987. – 360 с.

3. Кнут Д. Искусство программирования для ЭВМ. Т. 2. Получисленные алгоритмы. – М.: Мир, 1977. – 728 с.

4. Достоверные вычисления. Базовые численные методы. / У. Кулиш, Д. Рац, Р. Хаммер, М. Хокс. – М.-Ижевск: НИЦ «Регулярная и хаотическая динамика», 2005. – 496 с.

5. Червяков Н.И. Методы, алгоритмы и техническая реализация основных проблемных операций, выполняемых в системе остаточных классов // Инфокоммуникационные технологии. – 2011. – № 4. – С. 4–12.

6. Приближенный метод выполнения немодульных операций в системе остаточных классов / Н.И. Червяков, В.М. Авербух, М.Г. Бабенко, П.А. Ляхов, А.В. Гладков, А.В. Гапочкин // Фундаментальные исследования. – 2012. – № 6. – С. 189–193.

7. Omondi A. Residue Number Systems theory and Implementation. – London: Imperial College Press, 2007. – 312 p.

8. Wilkinson J.H. Rounding Errors in algebraic processes. – N.Y.: Dover Publications, 1994. – 160 p.

References

1. Akushskiy I.Ya., Yuditskiy D.I. *Mashinnaya arifmetika v ostatochnykh klassakh* [Machine arithmetic in residue classes]. Moscow, «Sovetskoe radio», 1968. 440 p.

2. Alefeld G., Herzberger J. *Vvedenie v interval'nye vychislenija* [Introduction to interval computations]. Moskow, «World», 1987. 360 p.

3. Knut D. *Iskusstvo programmirovanija dlja JeVM. T. 2. Poluchislennye algoritmy* [The Art of Computer Programming. Vol. 2: Seminumerical Algorithms]. Moscow, «World», 1977. 728 p.

4. Kulisch U., Ratz D., Hammer R., Hocks M. *Dostovernye vychislenija. Bazovye chislennye metody.* [Numerical Toolbox for Verified Computing I. Basic Numerical Problems]. Moscow-Izhevsk, «R&C Dynamics», 2005. 496 p.

5. Chervyakov N.I. *Metody, algoritmy i tekhnicheskaya realizatsiya osnovnykh problemnykh operatsiy, vypolnyaemykh v sisteme ostatochnykh klassov* – Methods, algorithms and technical implementation of the basic problematic operations performed in the residue number system. Infokommunikatsionnye tekhnologii – Infocommunication Technology. 2011, no. 4. pp. 4–12.

6. Chervyakov N.I., Averbukh V.M., Babenko M.G., Lyakhov P.A.,Gladkov A.V., Gapochkin A.V. *Priblizhennyj metod vypolnenija nemodul'nyh operacij v sisteme ostatochnyh klassov* – Approximate method of implementation non-modular operations in the residue number system – Fundamental Research. 2012, no.6. pp. 189-193.

7. Omondi, Amos R., Benjamin Premkumar. *Residue number systems theory and implementation*. London: Imperial College Press, 2007. 312 p.

8. Wilkinson J.H. *Rounding Errors in algebraic processes*. N.Y.: Dover Publications, 1994. 160 p.

Рецензенты:

Частиков А.В., д.т.н., профессор, декан факультета прикладной математики и телекоммуникаций Вятского государственного университета, г. Киров;

Страбыкин Д.А., д.т.н., профессор, заведующий кафедрой электронных вычислительных машин Вятского государственного университета, г. Киров.

Работа поступила в редакцию 22.02.2013