ISSN 2307–3489 (Print), ISSN 2307–6666 (Online)

Наука та прогрес транспорту. Вісник Дніпропетровського національного університету залізничного транспорту, 2016, № 2 (62)

УДК 519.6

Ю. Д. ПОЛИССКИЙ[1*]

[1*]НИИ автоматизации чёрной металлургии, ул. Короленко, 21, Днепропетровск, Украина, 49000,
тел. + 38 (056) 744 33 65, +38 (067) 706 83 11, эл. почта polissky@mail.ru, ORCID 0000-0001-5363-8145

О ВЫПОЛНЕНИИ СЛОЖНЫХ ОПЕРАЦИЙ В НЕПОЗИЦИОННОЙ СИСТЕМЕ СЧИСЛЕНИЯ ОСТАТОЧНЫХ КЛАССОВ

Цель. Работа предполагает теоретическое обоснование методики повышения эффективности выполнения в непозиционной системе счисления остаточных классов сложных, так называемых немодульных, операций, для реализации которых необходимо знание цифр операндов по всем разрядам. **Методика.** Для достижения поставленной цели числа представляются в системе нечётных модулей, при этом результат выполнения операции определяется на основе установления чётности операндов. Определение чётности осуществляется путём нахождения суммы по модулю два значений позиционных характеристик числа по всем его модулям. Алгоритм получения позиционной характеристики включает итерации двух видов. Итерация первого вида состоит в переходе от данного числа к меньшему числу, в котором остатки по одному или нескольким модулям равны нулю. Достигается это вычитанием из всех остатков значения одного из них. Итерация второго вида состоит в переходе от данного числа к меньшему числу за счёт исключения модулей, остатки по которым равны нулю, путём деления данного числа на произведение этих модулей. Итерации выполняются до тех пор, пока остатки по одному, всем или некоторым модулям не окажутся равными нулю, а остальные модули будут исключены. Предлагаемая методика отличается своей простотой и позволяет быстро получить результат операции. **Результаты.** Получены весьма несложные решения немодульных операций определения выхода за пределы диапазона результата сложения или вычитания пары чисел, сравнения пары чисел, определения принадлежности числа данной половине диапазона, определения чётности чисел, представленных в непозиционной системе счисления остаточных классов. **Научная новизна.** Предложены новые эффективные подходы к решению немодульных операций системы счисления остаточных классов. Представляется целесообразным рассматривать данные подходы в качестве направления исследований по повышению эффективности модулярных вычислений. **Практическая значимость.** Рассмотренные решения обладают высоким быстродействием и могут быть эффективными при разработке модулярных вычислительных структур.

Ключевые слова: остаточные классы; число; сложные операции; позиционная характеристика; чётность числа; итерация

Введение

В настоящее время проводятся интенсивные исследования по повышению эффективности вычислений на основе представления чисел в системе остаточных классов (СОК) за счет параллельного выполнения операций над остатками [1, 13].

СОК называется система счисления, в которой произвольное число N представляется в виде набора наименьших неотрицательных остатков по модулям $m_1, m_2, \ldots, m_n$, то есть $N = (\alpha_1, \alpha_2, \ldots, \alpha_n)$. Здесь $\alpha_i = N(\mathrm{mod}\, m_i)$. При этом, если числа m_i взаимно простые, то такому представлению соответствует только одно число N диапазона $[0, M)$, где $M = m_1 m_2 \ldots m_n$.

Преимущества остаточной арифметики подробно изложены в [2, 6, 12]. Однако, возникают определенные трудности [5] при реализации немодульных, так называемых сложных, операций, для выполнения которых необходимо знание цифр операндов по всем разрядам. В связи с важностью и актуальностью разработок по совершенствованию машинной арифметики СОК результаты этих работ систематически рассматривались в периодических научно-технических изданиях [3, 4, 7, 8, 10, 11, 14, 15].

doi 10.15802/stp2016/67297

ISSN 2307–3489 (Print), ISSN 2307–6666 (Online)

Наука та прогрес транспорту. Вісник Дніпропетровського національного університету залізничного транспорту, 2016, № 2 (62)

Цель

Целью данной работы является теоретическое обоснование методики повышения эффективности выполнения в непозиционной системе счисления остаточных классов сложных, так называемых немодульных, операций, для реализации которых необходимо знание цифр операндов по всем разрядам.

Методика

Значительное количество работ по повышению быстродействия сложных операций посвящено системам, в которых один из модулей равен двум. Вместе с тем немодульные операции определения выхода за пределы диапазона результата сложения или вычитания пары чисел, сравнения пары чисел, определения принадлежности числа данной половине диапазона весьма несложно могут быть выполнены в системе нечетных модулей. Так, для сложения или вычитания пары чисел результат определяется в соответствии с табл. 1.

Таблица 1

Определение результата сложения (вычитания) пары чисел

Table 1

Determination the result of addition (subtraction) of a number pair

Число 1	Число 2	Сумма, Разность	Результат
чт	чт	чт	0
чт	чт	нчт	1
чт	нчт	нчт	0
чт	нчт	чт	1
нчт	чт	нчт	0
нчт	чт	чт	1
нчт	нчт	чт	0
нчт	нчт	нчт	1

В табл.1 «чт» и «нчт» обозначают четность и нечетность числа, «0» и «1» – выход и невыход результата за пределы диапазона соответственно.

Сравнение чисел осуществляется вычитанием одного числа из другого и определением результата сравнения в соответствии с табл. 1. При этом результат «0» означает, что «Число 1» больше или равно «Числу 2», результат «1» – «Число 1» меньше «Числа 2».

Определение принадлежности чисел данной половине диапазона производится умножением чисел на 2. При этом все полученные произведения должны быть четными. Для чисел нижней половины диапазона произведения остаются четными, поскольку они не выходят за верхнюю границу диапазона. Для чисел верхней половины диапазона произведения выходят за верхнюю границу диапазона и, соответственно, они становятся нечетными.

Таким образом, реализация рассмотренных сложных операций основана на определении четности операндов.

Алгоритм определения четности числа в нечетной системе модулей состоит в следующем.

Пусть системой оснований полиадического кода также является система $m_1, m_2, \ldots, m_n$. Тогда число N в полиадическом коде представляется следующим образом

$$N = \pi_1 + \pi_2 m_1 + \ldots + \pi_i m_1 m_2 \ldots m_{i-1} + \\ + \cdots + \pi_{n-1} m_1 m_2 \ldots m_{n-2} + \pi_n m_1 m_2 \ldots m_{n-1},$$

где $0 \le \pi_i \le m_i - 1$.

Поскольку все модули нечетные, четность N определяется значением

$$I = \pi_1 + \pi_2 + \ldots + \pi_i + \cdots + \pi_{n-1} + \pi_n.$$

Следовательно, метод базируется на получении суммы значений позиционных характеристик, определяемых в соответствии с выражением

$$N = \pi_1 + m_1(\pi_2 + m_2(\pi_3 + \ldots + m_{i-1}(\pi_i + \\ + \cdots + m_{n-2}(\pi_{n-1} \ldots + m_{n-1}\pi_n))\ldots).$$

Разобьем диапазон M на m_i интервалов длины $m_1 m_2 \ldots m_{i-1} m_{i+1} m_{n-1} m_n$ каждый.

doi 10.15802/stp2016/67297

ISSN 2307–3489 (Print), ISSN 2307–6666 (Online)
Наука та прогрес транспорту. Вісник Дніпропетровського національного університету залізничного транспорту, 2016, № 2 (62)

$$N \in \begin{cases} P_0, & 0 \le N_0 \le \dfrac{M}{m_i} - 1, \\ P_1, & \dfrac{M}{m_i} \le N_1 \le \dfrac{2M}{m_i} - 1, \\ \ldots\ldots\ldots\ldots\ldots\ldots, \\ P_t, & \dfrac{tM}{m_i} \le N_t \le \dfrac{(t+1)M}{m_i} - 1, \\ \ldots\ldots\ldots\ldots\ldots\ldots, \\ P_{m_i - 1}, & \dfrac{(m_i - 1)M}{m_i} \le N_{m_i - 1} \le M - 1. \end{cases}$$

Здесь P_t – t-й интервал, $t = 0,1,2,\ldots,m_i - 1$.

Алгоритм получения позиционной характеристики включает итерации двух видов. Итерация первого вида состоит в переходе от данного числа N к меньшему числу $\tilde{N}$, в котором остатки по одному или нескольким модулям равны нулю. Достигается это вычитанием из всех остатков значения одного из них, $\tilde{N} = N - \alpha_s$, где $\alpha_s = N(\mathrm{mod}\, m_s)$. Таким образом, полученное число становится кратным этим модулям. Поскольку $\alpha_s \le N$, то при переходе от N к $\tilde{N}$ число $\tilde{N}$ не выходит из интервала N - го числа.

Итерация второго вида состоит в переходе от числа $\tilde{N}$ к меньшему числу $\tilde{\tilde{N}}$ за счет исключения модулей, остатки по которым равны нулю, путем деления данного числа на произведение этих модулей. Поскольку при делении на модуль или произведение модулей как самого числа, так и границ интервала соотношение между ними не изменяется, число $\tilde{\tilde{N}}$ не выходит из интервала $\tilde{N}$ - го числа, а поскольку делитель – модуль или произведение модулей – число нечетное, четность $\tilde{\tilde{N}}$ совпадает с четностью $\tilde{N}$.

Итерации выполняются до тех пор, пока остатки по одному, всем или некоторым модулям из $m_1, m_2, \ldots, m_n$ не окажутся равными нулю, а остальные модули будут исключены, то есть

$$N = \left(\alpha_1, \alpha_2, \ldots, \alpha_n\right) \to \tilde{\tilde{N}}(0, \times).$$

При этом

$$I = \pi_1 + \pi_2 + \ldots + \pi_i + \cdots + \pi_{n-1} + \pi_n.$$

Рассмотрим итерацию первого вида подробнее. Пусть $N = \left(\alpha_1, \alpha_2, \ldots, \alpha_s, \ldots, \alpha_n\right)$. Образуем число

$$\tilde{N} = \begin{pmatrix} \tilde{\alpha}_1 = \alpha_1 - \alpha_s, \tilde{\alpha}_2 = \alpha_2 - \\ -\alpha_s, \ldots, \tilde{\alpha}_n = \alpha_n - \alpha_s \end{pmatrix}$$

вычитанием остатка α_s по модулю m_s из остатков по всем модулям числа N. Естественно, все числа $\tilde{N}$ диапазона $[0, M)$ кратны модулю m_s, то есть вероятность $p(\tilde{\alpha}_s = 0) = 1$. При этом диапазон $[0, M)$ окажется разбитым на $K_1 = m_1 m_2 \ldots m_{s-1} m_{s+1} \ldots m_n$ интервалов длины m_s, внутри каждого из которых значения разностей одинаковы и кратны m_s. Может оказаться, что наряду с $\tilde{\alpha}_s = 0$ остатки по некоторому модулю m_s числа $\tilde{N}$ также равны нулю, например, $\tilde{\alpha}_s = 0$, то есть число $\tilde{N}$ кратно модулю m_r. Количество интервалов, внутри которых значения разностей кратны m_r, равно

$$K_2 = \frac{K_1}{m_r} = m_1 \ldots m_{s-1} m_{s+1} \ldots m_{r-1} m_{r+1} \ldots m_n.$$

Поскольку в каждом интервале содержится m_s чисел, то общее количество чисел с $\tilde{\alpha}_r = 0$ равно $K = m_1 \ldots m_{r-1} m_{r+1} \ldots m_n$, то есть вероятность. $p(\tilde{\alpha}_r = 0 / \tilde{\alpha}_s = 0) = \dfrac{1}{m_r}$.

Будем называть модули $m_1, m_2, \ldots, m_n$ рабочими, а объем диапазона M рабочим. Введем ещё один – индикаторный модуль $m_0 = 2$, который не включается в состав рабочих модулей. То есть все действия над операндами выполняются только в системе рабочих модулей в пределах рабочего диапазона. Остаток $\alpha_0(\mathrm{mod}\, \mathrm{m}_0 = 2)$ предназначен лишь для индикации четности исследуемого числа в соответствии с

doi 10.15802/stp2016/67297

ISSN 2307–3489 (Print), ISSN 2307–6666 (Online)

Наука та прогрес транспорту. Вісник Дніпропетровського національного університету залізничного транспорту, 2016, № 2 (62)

$$I = \pi_1 + \pi_2 + \ldots + \pi_i + \cdots + \pi_{n-1} + \pi_n .$$

В табл. 2 представлена работа данного алгоритма (Алгоритм 1) определения четности числа $N = 4483 = (6,3,11,3,1)$ в системе модулей $m_1 = 11, m_2 = 7, m_3 = 13, m_4 = 5, m_5 = 3$.

Из табл. 2 видно, что остаток по индикаторному модулю $\alpha_0 = N(\mathrm{mod}\, m_0) = 1$, то есть число $N = 4483$ – нечетное. Результат достигается за $T_1 = 7$ итераций.

Быстродействие операции определения четности числа можно увеличить на основе алгоритма (Алгоритм 2) с помощью представления чисел в обратных кодах [10]. По данному алгоритму осуществляется одновременное представление чисел в прямом и обратном кодах с выбором на каждой итерации варианта, при котором один или несколько остатков равны нулю. Табл. 3 иллюстрирует процесс определения четности того же числа $N = 4483$ в той же системе модулей

$$m_1 = 11, m_2 = 7, m_3 = 13, m_4 = 5, m_5 = 3 .$$

Таблица 2

Работа Алгоритма 1

Table 2

Work Algorithm 1

Итерация 1	Число	Модули					
		Рабочие					Индик.
		11	7	13	5	3	2
	4483	6	3	11	3	1	0
	-1	1	1	1	1	1	1
	4482	5	2	10	2	0	1
Итерация 2	Число	Модули					
		Рабочие					Индик.
		11	7	13	5	3	2
	4482	5	2	10	2	0	1
	:3	3	3	3	3	0	1
	1494	9	3	12	4	x	1
Итерация 3	Число	Модули					
		Рабочие					Индик.
		11	7	13	5	3	2
	1494	9	3	12	4	x	1
	-4	4	4	4	4	x	0
	1490	5	6	8	0	x	1
Итерация 4	Число	Модули					
		Рабочие					Индик.
		11	7	13	5	3	2
	1490	5	6	8	0	x	1
	:5	5	5	5	0	x	1
	298	1	4	12	x	x	1

doi 10.15802/stp2016/67297

ISSN 2307–3489 (Print), ISSN 2307–6666 (Online)

Наука та прогрес транспорту. Вісник Дніпропетровського національного університету залізничного транспорту, 2016, № 2 (62)

Окончание табл. 2

End of table 2

Итерация 5	Число	Модули					
		Рабочие					Индик.
		11	7	13	5	3	2
	298	1	4	12	x	x	1
	-12	1	5	12	x	x	0
	286	0	6	0	x	x	1
Итерация 6	Число	Модули					
		Рабочие					Индик.
		11	7	13	5	3	2
	286	0	6	0	x	x	1
	:(13*11)	0	3	0	x	x	1
	2	x	2	x	x	x	1
Итерация 7	Число	Модули					
		Рабочие					Индик.
		11	7	13	5	3	2
	2	x	2	x	x	x	1
	-2	x	2	x	x	x	0
	0	x	0	x	x	x	**1**

Сопоставление значений остатков в шестой строке блоков А и В показывает, что количество нулевых остатков в блоке В – больше, чем в блоке А. Поэтому принимаем блок В в качестве активного. Поскольку система модулей нечетная, смена активного блока не изменяет четность числа. В блоке В выполняем деление числа N на (3*5*13). В одиннадцатой строке блока В величина делителя (3*5*13) представлена своими остатками по соответствующим модулям. Результат деления одновременно записывается в двенадцатой строке обоих блоков.

Сопоставление значений остатков в двенадцатой строке блоков А и В показывает, что в блоке А имеется остаток $\alpha_1 = 0$ по модулю $m_1 = 11$. Поэтому принимаем блок А в качестве активного. В семнадцатой строке активного блока А величина делителя (11) представлена своими остатками по соответствующим модулям.

Результат деления одновременно записывается в восемнадцатой строке обоих блоков.

Из очередного сопоставления значений остатков в двадцать второй строке блоков А и В видно, что нулевые остатки в обоих блоках отсутствуют. Поэтому заключительная итерация состоит в вычитании значения остатка $\alpha_2 = 2$ по модулю $m_2 = 7$. Получаем на индикаторном модуле значение остатка $\alpha_0 = 1$.

Результат по данному алгоритму достигается за $T_2 = 4$ итерации, то есть в $\Theta = \frac{T_1}{T_2} = 1,75$ быстрее.

doi 10.15802/stp2016/67297

ISSN 2307–3489 (Print), ISSN 2307–6666 (Online)

Наука та прогрес транспорту. Вісник Дніпропетровського національного університету залізничного транспорту, 2016, № 2 (62)

Таблица 3

Работа Алгоритма 2

Table 3

Work Algorithm 2

Блок А

	Итерация 1	Число	Модули					
2			Рабочие					Индик.
3			11	7	13	5	3	2
4		**4483**	6	3	11	3	1	0
5		-1	1	1	1	1	1	1
6		4482	5	2	10	2	0	1
7	Итерация 2	Число	Модули					
8			Рабочие					Индик.
9			11	7	13	5	3	2
10		**4482**	5	2	10	2	0	1
11								
12								
13	Итерация 3	Число	Модули					
14			Рабочие					Индик.
15			11	7	13	5	3	2
16		**22**	0	1	x	x	x	1
17		:11	0	4	x	x	x	1
18		2	x	2	x	x	x	1
19	Итерация 4	Число	Модули					
20			Рабочие					Контр.
21			11	7	13	5	3	2
22		**2**	x	2	x	x	x	1
23		-2	x	2	x	x	x	0
24		0	0	x	x	x		**1**

Блок В

Итерация 1	Число	Модули					
		Рабочие					Индик.
		11	7	13	5	3	2
	10531	4	3	1	1	1	0
	-1	1	1	1	1	1	1
	10530	3	2	0	0	0	1
Итерация 2	Число	Модули					
		Рабочие					Индик.
		11	7	13	5	3	2
	10530	3	2	0	0	0	1
	:(3*5*13)	8	6	0	0	0	1
	54	10	5	x	x	x	1
Итерация 3	Число	Модули					
		Рабочие					Индик.
		11	7	13	5	3	2
	54	10	5	x	x	x	1
Итерация 4	Число	Модули					
		Рабочие					Контр.
		11	7	13	5	3	2
	4	x	4	x	x	x	1

Результаты

Получены весьма несложные решения немодульных операций определения выхода за пределы диапазона результата сложения или вычитания пары чисел, сравнения пары чисел, определения принадлежности числа данной половине диапазона, определения чётности числа.

Научная новизна и практическая значимость

Предложены новые подходы к решению немодульных операций системы остаточных классов. Представляется целесообразным рассматривать данные подходы в качестве направления исследований по повышению эффективности модулярных вычислений. Рассмотренные решения обладают высоким быстродействием и могут быть реализованы при разработке модулярных вычислительных структур.

doi 10.15802/stp2016/67297

Выводы

Рассмотрены вопросы выполнения немодульных операций в системе остаточных классов. Показано, что эти операции могут быть достаточно несложно реализованы в системе нечетных модулей на основе определения четности операндов. Определение четности осуществляется путем нахождения суммы значений позиционных характеристик числа по модулю два. Алгоритм получения позиционной характеристики включает итерации двух видов: вычитание из всех остатков значения одного из них и исключения модулей, остатки по которым равны нулю. Рассмотренные решения обладают высоким быстродействием и могут быть реализованы при разработке модулярных вычислительных структур. Представляется целесообразным рассматривать предложенные подходы в качестве направления исследований по повышению эффективности немодульных операций в системе остаточных классов.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Акушский, И. Я. Машинная арифметика в остаточных классах / И. Я. Акушский, Д. И. Юдицкий. – Москва : Сов. радио, 1968. – 440 с.
2. Ирхин, В. П. Табличная реализация операций модулярной арифметики / В. П. Ирхин // 50 лет модулярной арифметики : тр. юбил. Междунар. науч.-техн. конф. (23.11–25.11.2005) / Моск. ин-т электрон. техники. – Москва, 2015. – С. 268–273.
3. Кнут, Д. Искусство программирования / Д. Кнут. – Москва : Диалектика-Вильямс, 2013. – 832 с.
4. Колесникова, Т. А. Интеграция украинской отраслевой научной периодики в мировое научно-информационное пространство: проблемы и решения / Т. А. Колесникова // Наука та прогрес транспорту. – 2013. – № 6 (48). – С. 7–22. doi: 10.15802/stp2013/19835.
5. Магомедов, Ш. Г. Преобразование представлений чисел в модулярной арифметике в системах остаточных классов с разными основаниями / Ш. Г. Магомедов // Вестн. Астрахан. гос. техн. ун-та. Серия : «Управление, вычислител. техника, информатика». – Астрахань, 2014. – № 4. – С. 32–39.
6. Методы и алгоритмы округления, масштабирования и деления чисел в модулярной арифметике / Н. И. Червяков [и др.] // 50 лет модуляр. арифметики : тр. юбил. Междунар. науч.-техн. конф. (23.11–25.11.2005) / Моск. ин-т электрон. техники. – Москва, 2005. – С. 291–310.
7. Модулярные параллельные вычислительные структуры нейропроцессорных систем : монография / под ред. Н. И. Червякова. – Москва : Физматлит, 2003. – 288 с.
8. Полисский, Ю. Д. Алгоритм выполнения операции деления чисел на два в системе остаточных классов / Ю. Д. Полисский // Вісн. Дніпропетр. нац. ун–ту залізн. трансп. ім. акад. В. Лазаряна. – Дніпропетровськ, 2007. – Вип. 16. – С. 68–72.
9. Полисский, Ю. Д. Алгоритм выполнения сложных операций в системе остаточных классов с помощью представления чисел в обратных кодах / Ю. Д. Полисский // Электронное моделирование. – 2014. – Т. 36, № 4. – С. 117–122.
10. Полисский, Ю. Д. О выполнении сложных операций в системе остаточных классов / Ю. Д. Полисский // Электронное моделирование. – 2006. – Т. 28, № 3. – С. 117–123.
11. Червяков, Н. И. Методы, алгоритмы и техническая реализация основных проблемных операций, выполняемых в системе остаточных классов / Н. И. Червяков // Инфокоммуник. технологии / Поволж. гос. ун-т телеком. и информ. – Самара, 2011. – № 4. – С. 4–12.
12. Червяков, Н. И. Методы и принципы построения модулярных нейрокомпьютеров / Н. И. Червяков // 50 лет модулярной арифметики : тр. юбил. Междунар. науч.-техн. конф. (23.11–25.11.2005) / Моск. ин-т электрон. техники. – Москва, 2005. – С. 232–242.
13. Boateng, K. O. A Smith-Waterman Algorithm Accelerator Based on Residue Number System / K. O. Boateng, E. Y. Baagyere // Intern. J. of Electronics and Communication Engineering. – 2012. – Vol. 5, № 1. – P. 99–112.
14. Tomczak, T. Hierarchical residue number systems with small moduli and simple converters / T. Tomczak // Intern. J. of Applied Mathematics and Computer Science. – 2011. – Vol. 21. – Iss. 1. – P. 173–192. doi: 10.2478/v10006-011-0013-2.
15. Youssef, M. I. Multi-Layer Data Encryption Using Residue Number System in DNA Sequence / M. I. Youssef, A. E. Emam, M. Abd Elghanym // Intern. J. of Security and Its Applications. – 2012. – Vol. 6, № 4. – P. 1–12.

doi 10.15802/stp2016/67297

ISSN 2307–3489 (Print), ISSN 2307–6666 (Online)

Наука та прогрес транспорту. Вісник Дніпропетровського національного університету залізничного транспорту, 2016, № 2 (62)

Ю. Д. ПОЛІСЬКИЙ[1*]

[1*]НДІ автоматизації чорної металургії, вул. Короленка, 21, Дніпропетровськ, Україна, 49000, тел. + 38 (056) 744 33 65, +38 (067) 706 83 11, ел. пошта polissky@mail.ru, ORCID 0000-0001-5363-8145

ПРО ВИКОНАННЯ СКЛАДНИХ ОПЕРАЦІЙ У НЕПОЗИЦІЙНІЙ СИСТЕМІ ЧИСЛЕННЯ ЗАЛИШКОВИХ КЛАСІВ

Мета. Робота передбачає теоретичне обґрунтування методики підвищення ефективності виконання у непозиційній системі числення залишкових класів складних, так званих немодульних, операцій, для реалізації яких необхідно знати цифри операндів по всіх розрядах. **Методика.** Для досягнення поставленої мети числа представляються в системі непарних модулів, при цьому результат виконання операції визначається на основі встановлення парності операндів. Визначення парності здійснюється шляхом знаходження суми по модулю два значень позиційних характеристик числа по всіх його модулях. Алгоритм отримання позиційної характеристики включає ітерації двох видів. Ітерація першого виду полягає в переході від даного числа до меншого числа, в якому залишки по одному або декількох модулях дорівнюють нулю. Досягається це відніманням із усіх залишків значення одного з них. Ітерація другого виду полягає в переході від даного числа до меншого числа за рахунок виключення модулів, залишки за якими дорівнюють нулю, шляхом ділення цього числа на добуток цих модулів. Ітерації виконуються до тих пір, доки залишки по одному, всім або деяким модулям не стануть дорівнювати нулю, а решта будуть виключені. Запропонована методика відрізняється своєю простотою та дозволяє швидко отримати результат операції. **Результати.** Отримані досить нескладні рішення немодульних операцій визначення виходу за межі діапазону результату додавання або віднімання пари чисел, порівняння пари чисел, визначення приналежності числа даній половині діапазону, визначення парності чисел, представлених у непозиційній системі числення залишкових класів. **Наукова новизна.** Запропоновані нові ефективні підходи до вирішення модульних операцій системи числення залишкових класів. Представляється доцільним розглядати ці підходи як напрямок досліджень по підвищенню ефективності модулярних обчислень. **Практична значимість.** Розглянуті рішення мають високу швидкодію і можуть бути ефективними при розробці модулярних обчислювальних структур.

Ключові слова: залишкові класи; число; складні операції; позиційна характеристика; парність числа; ітерація

YU. D. POLISSKY[1*]

[1*]Automation, Iron and Steel SRI, Korolenko St., 21, Dnipropetrovsk, Ukraine, 49000,
tel. + 38 (056) 744 33 65, +38 (067) 706 83 11, e-mail polissky@mail.ru, ORCID 0000-0001-5363-8145

ABOUT COMPLEX OPERATIONS IN NON-POSITIONAL RESIDUE NUMBER SYSTEM

Purpose. The purpose of this work is the theoretical substantiation of methods for increased efficiency of execution of difficult, so-called not modular, operations in non-positional residue number system for which it is necessary to know operand digits for all grade levels. **Methodology**. To achieve the target the numbers are presented in odd module system, while the result of the operation is determined on the basis of establishing the operand parity. The parity is determined by finding the sum modulo for the values of the number positional characteristics for all of its modules. Algorithm of position characteristics includes two types of iteration. The first iteration is to move from this number to a smaller number, in which the remains of one or more modules are equal to zero. This is achieved by subtracting out of all the residues the value of one of them. The second iteration is to move from this number to a smaller number due to exclusion of modules, which residues are zero, by dividing this number by the product of these modules. Iterations are performed until the residues of one, some or all of the modules equal to zero and other modules are excluded. The proposed method is distinguished by its simplicity and allows you to obtain the result of the operation quickly. **Findings.** There are obtained rather simple solutions of not modular operations for definition of outputs beyond the range of the result of adding or subtracting pairs of numbers, comparing pairs of numbers, determining the number belonging to the specific half of the range, defining parity of numbers presented in non-

doi 10.15802/stp2016/67297

positional residue number system. **Originality**. The work offered the new effective approaches to solve the non-modular operations of the non-positional residue number system. It seems appropriate to consider these approaches as research areas to enhance the effectiveness of the modular calculation. **Practical value**. The above solutions have high performance and can be effective in developing modular computing structures.

Keywords: residue classes; number; complex operations; positional characteristic; parity number; iteration

REFERENCES

1. Akushskiy I.Ya., Yuditskiy D.I. *Arifmetika v ostatochnykh klassakh* [Machine arithmetic in the residual classes]. Moscow, Sovetskoye radio Publ., 1968. 440 p.
2. Irkhin V.P. Tablichnaya realizatsiya operatsiy modulyarnoy arifmetiki [Tabular implementation of modular arithmetic operations]. *Trudy yubileynoy Mezhdunarodnoy nauchno-tekhnicheskoy konferentsii «50 let modulyarnoy arifmetiki (23.11.–25.11.2005)»* [Proc. of Anniversary Intern. Sci. and Techn. Conf. «50 years of modular arithmetic»]. Moscow, 2015, pp. 268-273.
3. Knut D. *Iskusstvo programmirovaniya* [Programming art]. Moscow, Dialektika-Vilyams Publ., 2013. 832 p.
4. Kolesnykova T.O. Integratsiya ukrainskoy otraslevoy nauchnoy periodiki v mirovoye nauchno-informatsionnoye prostranstvo: problemy i resheniya [Integration of Ukrainian industry scientific periodicals into world scientific information space: problems and solutions]. *Nauka ta progres transportu – Science and Transport Progress*, 2013, no. 6 (48), pp. 7-22. doi: 10.15802/stp2013/19835.
5. Magomedov Sh.G. Preobrazovaniye predstavleniy chisel v modulyarnoy arifmetike v sistemakh ostatochnykh klassov s raznymi osnovaniyami [Transformation of numeration in a modular arithmetic in systems of remaining classes with different bases]. *Vestnik Astrakhanskogo gosudarstvennogo tekhnicheskogo universiteta. Seriya: «Upravleniye, vychislitelnaya tekhnika, informatika»* [Bulletin of Astrakhan State and Technical University. Series: «Management, computer technology, informatics»]. Astrakhan, 2014, no. 4, pp. 32-39.
6. Chervyakov N.I., Lavrinenko I.N., Lavrinenko S.V., Mezentseva O.S. Metody i algoritmy okrugleniya, masshtabirovaniya i deleniya chisel v modulyarnoy arifmetike [Methods and rounding algorithms, scaling and dividing numbers in modular arithmetic]. *Trudy yubileynoy Mezhdunarodnoy nauchno-tekhnicheskoy konferentsii «50 let modulyarnoy arifmetiki (23.11.–25.11.2005)»* [Proc. of Anniversary Intern. Sci. and Techn. Conf. «50 years of modular arithmetic»]. Moscow, 2005, pp. 291-310.
7. Chervyakov N.I., Sakhnyuk P.A., Shaposhnikov A.V., Ryadnov S.A. *Modulyarnyye parallelnyye vychislitelnyye struktury neyroprotsessornykh system* [Modular parallel computing structure of neuroprocessor systems]. Moscow, Fizmatlit Publ., 2003. 288 p.
8. Polisskiy Yu.D. Algoritm vypolneniya operatsii deleniya chisel na dva v sisteme ostatochnykh klassov [The algorithm of operation performing of dividing the number by two in the system of residual classes]. *Visnyk Dnipropetrovskoho natsionalnoho universytetu zaliznychnoho transportu imeni akademika V. Lazariana* [Bulletin of Dnipropetrovsk National University of Railway Transport named after Academician V. Lazaryan], 2007, issue 16, pp. 68-72.
9. Polisskiy Yu.D. Algoritm vypolneniya slozhnykh operatsiy v sisteme ostatochnykh klassov s pomoshchyu predstavleniya chisel v obratnykh kodakh [Algorithm to perform complex operations in the residual classes system using representation of numbers in reverse codes]. *Elektronnoye modelirovaniye – Electronic modeling*, 2014, vol. 36, no. 4, pp. 117-122.
10. Polisskiy Yu.D. O vypolnenii slozhnykh operatsiy v sisteme ostatochnykh klassov [About the implementation of complex transactions in the system of residual classes]. *Elektronnoye modelirovaniye – Electronic modeling*, 2006, vol. 28, no. 3, pp. 117-123.
11. Chervyakov N.I. Metody, algoritmy i tekhnicheskaya realizatsiya osnovnykh problemnykh operatsiy, vypolnyaemykh v sisteme ostatochnykh klassov [Methods, algorithms and technical implementation of the basic problem of operations performed in the system of residual classes]. *Infokommunikatsionnyye tekhnologii – Information and Communication Technologies*, 2011, no. 4, pp. 4-12.
12. Chervyakov N.I. Metody i printsipy postroyeniya modulyarnykh neyrokompyuterov [Methods and principles of construction of modular neural computers]. *Trudy yubileynoy Mezhdunarodnoy nauchno-tekhnicheskoy konferentsii «50 let modulyarnoy arifmetiki (23.11.–25.11.2005)»* [Proc. of Anniversary Intern. Sci. and Techn. Conf. «50 years of modular arithmetic»]. Moscow, 2005, pp. 232-242.
13. Boateng K.O., Baagyere E.Y. A Smith-Waterman Algorithm Accelerator Based on Residue Number System. *Intern. Journal of Electronics and Communication Engineering*, 2012, vol. 5, no. 1, pp. 99-112.

doi 10.15802/stp2016/67297

14. Tomczak T. Hierarchical residue number systems with small moduli and simple converters. *Intern. Journal of Applied Mathematics and Computer Science,* 2011, vol. 21, issue 1, pp. 173-192. doi: 10.2478/v10006-011-0013-2.
15. Youssef M.I., Emam A.E. , Abd Elghanym M. Multi-Layer Data Encryption Using Residue Number System in DNA Sequence. *Intern. Journal of Security and Its Applications*, 2012, vol. 6, no. 4, pp. 1-12.

Статья рекомендована к публикации д.физ.-мат.н., проф. С. А. Пичуговым (Украина); проф. О. Е. Потапом (Украина)

Поступила в редколлегию: 08.12.2015
Принята к печати: 24.03.2016

