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

Наука та прогрес транспорту. Вісник Дніпропетровського національного університету залізничного транспорту, 2016, № 63 (3)

ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНІ ТЕХНОЛОГІЇ ТА МАТЕМАТИЧНЕ МОДЕЛЮВАННЯ

УДК 519.6

Ю. Д. ПОЛИССКИЙ[1*]

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

О ПРЕОБРАЗОВАНИИ ПРЕДСТАВЛЕНИЙ ЧИСЕЛ В ОСТАТКАХ ИЗ ОДНОЙ СИСТЕМЫ МОДУЛЕЙ В ДРУГУЮ

Цель. В работе предполагается провести теоретическое обоснование одного из подходов к повышению эффективности выполнения в непозиционной системе счисления остаточных классов немодульной, так называемой сложной операции, для реализации которой необходимо знание цифр операндов по всем разрядам. Операция заключается в преобразовании представления числа из одной системы модулей представлением его в другой системе модулей. **Методика.** Инструментами методики исследований являются системный анализ, теория чисел, китайская теорема об остатках. Методика использует представление числа, как своими остатками, так и в полиадическом коде и базируется на определении остатка по данному модулю на основе полученных остатков по остальным модулям исходной системы. Такое определение выполняют последовательным вычитанием констант из получаемых остатков исходного числа и подсуммированием этих констант к результатам, которые образуются по искомым модулям. При этом константы на каждой итерации выбираются из предварительно рассчитанных таблиц, в зависимости от значения остатка в анализируемом разряде. Предложенный метод алгоритмически прост и при схемной реализации позволяет создавать вычислительные структуры высокой производительности и надежности. **Результаты.** В работе выполнено теоретическое обоснование рассматриваемого подхода для получения эффективного решения немодульной операции преобразования в системе остаточных классов для перехода от представления числа одной системой модулей к его представлению другой системой модулей. **Научная новизна.** Автором предложено теоретическое обоснование представленного подхода к решению немодульной операции преобразования в системе остаточных классов для перехода от представления числа в одной системе модулей к его представлению в другой системе модулей. Данный подход целесообразно рассматривать в качестве одного из направлений исследования путей повышения эффективности вычислений. **Практическая значимость**. Важность теоретических выводов и полученных результатов исследования заключается в том, что обоснован простой и эффективный подход к решению задачи выполнения немодульной операции преобразования в системе остаточных классов для перехода от представления числа в одной системе модулей к его представлению в другой системе модулей. Рассмотренные решения обладают высоким быстродействием и могут быть эффективными при разработке модулярных вычислительных структур для перспективных информационных технологий.

Ключевые слова: остаточные классы; число; сложные операции; позиционная характеристика; системы модулей; итерация

doi 10.15802/stp2016/74735

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

Наука та прогрес транспорту. Вісник Дніпропетровського національного університету залізничного транспорту, 2016, № 63 (3)

Введение

Одним из перспективных направлений повышения эффективности вычислений является применение параллельной обработки данных с использованием новых принципов на основе представления данных в системе остаточных классов (СОК) [1]. Достоинства СОК подробно изложены в [4, 5, 7, 8]. Однако возникают определенные трудности [17, 18] при реализации немодульных, так называемых сложных, операций. В связи с важностью и актуальностью разработок по остаточной арифметике результаты этих работ систематически рассматривались в периодических научно-технических изданиях [6, 16, 19, 20, 21].

При выполнении некоторых сложных операций в системе остаточных классов возникает необходимость в переходе от представления числа в одной системе модулей к представлению данного числа в другой системе модулей. Решение такой задачи может потребоваться, например, при расширении диапазона представления чисел [15], определении ранга числа [13], модульном делении чисел в тех случаях, когда осуществляется деление на число, кратное одному или нескольким модулям системы [12]. Поэтому операция перехода от одной системы модулей к другой, при которой по известным остаткам числа для некоторых модулей СОК определяют значения остатков этого же числа по другим модулям, относится к одной из основных немодульных операций в системе остаточных классов.

Цель

Целью данной работы является теоретическое обоснование одного из подходов к повышению эффективности выполнения в непозиционной системе счисления остаточных классов немодульной, так называемой сложной, операции, для реализации которой необходимо знание цифр операндов по всем разрядам. Операция заключается в преобразовании представления числа одной системой модулей представлением его другой системой модулей.

Методика

Инструментами методики исследований являются системный анализ [2], теория чисел [9], китайская теорема об остатках [3,10,11]. При изложении статьи будем использовать определения и обозначения, приведенные в [14]. 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 $M = m_1 m_2 \ldots m_n$.

Пусть $N^1{}_1 = (\alpha^1{}_1, \alpha^1{}_2, \ldots . \alpha^1{}_r)$ – число в системе модулей $m_1, m_2, \ldots, m_r$, $M_1 = m_1 m_2 \ldots m_r$, то же число $N^1{}_1 = N^1{}_2 = (\tilde{\alpha}_1, \tilde{\alpha}_2, \ldots . \tilde{\alpha}_s)$ в системе модулей $\tilde{m}_1, \tilde{m}_2, \ldots, \tilde{m}_s$, $M_2 = \tilde{m}_1 \tilde{m}_2 \ldots \tilde{m}_s$ и $M_2 \geq M_1$. Необходимо построить алгоритм перехода от представления числа $N^1{}_1$ остатками $\alpha^1{}_1, \alpha^1{}_2, \ldots . \alpha^1{}_r$ к его представлению остатками $\tilde{\alpha}_1, \tilde{\alpha}_2, \ldots . \tilde{\alpha}_s$.

Впервые решение данной задачи предложено в классической работе [1]. В статье [14] рассмотрено еще одно алгоритмическое решение, позволяющее упростить практическую реализацию и ускорить получение результата. Метод основан на итерационном алгоритме вычитания из исходного числа и добавления к искомому числу некоторых констант. В настоящей статье приведено обоснование данного подхода.

Пусть системой оснований полиадического кода также является система $m_1, m_2, \ldots, m_r$. Число N_1 в полиадическом коде представляется следующим образом

$$N_1 = \pi_1 + \pi_2 m_1 + \ldots + \pi_i m_1 m_2 \ldots m_{i-1} + \\ + \cdots + \pi_r m_1 m_2 \ldots m_{r-1},$$

где $0 \leq \pi_i \leq m_i - 1$. Тогда

$$\tilde{\alpha}_j = (\pi_1 + \pi_2 m_1 + \ldots + \pi_i m_1 m_2 \ldots m_{i-1} + \\ + \cdots + \pi_r m_1 m_2 \ldots m_{r-1}) (\mathrm{mod}\, \tilde{m}_j), j = 1, 2, \ldots, s$$

doi 10.15802/stp2016/74735

ISSN 2307–3489 (Print), ISSN 2307–6666 (Online)
Наука та прогрес транспорту. Вісник Дніпропетровського національного університету залізничного транспорту, 2016, № 63 (3)

Процесс определения слагаемых Δ_i описывается следующими зависимостями:

– для первого слагаемого

$$\Delta_1 = \pi_1 = N^1{}_1 (\mathrm{mod}\, m_1) = \alpha^1{}_1,$$

$$\Delta_1 (\mathrm{mod}\, m_i) = \alpha^1{}_1 (\mathrm{mod}\, m_i),\ i = 1,2,\ldots,r,$$

$$\Delta_1 (\mathrm{mod}\, \tilde{m}_j) = \alpha^1{}_1 (\mathrm{mod}\, \tilde{m}_j),\ j = 1,2,\ldots,s;$$

– для второго слагаемого

$$N^2{}_1 = N^1{}_1 - \alpha^1{}_1 = \pi_i \prod_1^{i-1} m_t + \cdots + \pi_{r-1} \prod_1^{r-2} m_v + \pi_r \prod_1^{r-1} m_w,$$

$$N^2{}_1 = (0, \alpha^2{}_2, \alpha^2{}_3, \cdots, \alpha^2{}_i, \cdots, \alpha^2{}_r),$$

$$\alpha^2{}_i = \alpha^1{}_i - \alpha^1{}_1, i = 2,\ldots,r,$$

$$N^2{}_1 (\mathrm{mod}\, m_2) = (\pi_2 m_1)(\mathrm{mod}\, m_2) = \alpha^2{}_2,$$

$$\pi_2 = (\frac{\alpha^2{}_2}{m_1})(\mathrm{mod}\, m_2),$$

$$\Delta_2 = m_1 (\frac{\alpha^1{}_2}{m_1})(\mathrm{mod}\, m_2),$$

$$\Delta_2 (\mathrm{mod}\, m_i) = (m_1 (\frac{\alpha^1{}_2}{m_1})(\mathrm{mod}\, m_2))(\mathrm{mod}\, m_i),$$

$$i = 2,\ldots,r,$$

$$\Delta_2 (\mathrm{mod}\, \tilde{m}_j) = (m_1 (\frac{\alpha^1{}_2}{m_1})(\mathrm{mod}\, m_2))(\mathrm{mod}\, \tilde{m}_j),$$

$$j = 1,2,\ldots,s;$$

– для третьего слагаемого

$$N^3{}_1 = N^2{}_1 - \alpha^2{}_2 = \pi_i \prod_1^{i-1} m_t + \cdots + \pi_{r-1} \prod_1^{r-2} m_v + \pi_r \prod_1^{r-1} m_w,$$

$$N^3{}_1 = (0, 0, \alpha^3{}_3, \cdots, \alpha^3{}_i, \cdots, \alpha^3{}_r),$$

$$\alpha^3{}_i = \alpha^2{}_i - \alpha^2{}_2, i = 3,\ldots,r,$$

$$N^3{}_1 (\mathrm{mod}\, m_3) = (\pi_3 m_1 m_2)(\mathrm{mod}\, m_3) = \alpha^3{}_3,$$

$$\pi_3 = (\frac{\alpha^3{}_3}{m_1 m_2})(\mathrm{mod}\, m_3),$$

$$\Delta_3 = m_1 m_2 (\frac{\alpha^3{}_3}{m_1 m_2})(\mathrm{mod}\, m_3),$$

$$\Delta_3 (\mathrm{mod}\, m_i) = (m_1 m_2 (\frac{\alpha^3{}_3}{m_1 m_2})(\mathrm{mod}\, m_3))(\mathrm{mod}\, m_i),$$

$$i = 3,\ldots,r,$$

$$\Delta_3 (\mathrm{mod}\, \tilde{m}_j) = (m_1 m_2 (\frac{\alpha^3{}_3}{m_1 m_2})(\mathrm{mod}\, m_3))(\mathrm{mod}\, \tilde{m}_j),$$

$$j = 1,2,\ldots,s.$$

Наконец, для r – го слагаемого

$$N^r{}_1 = N^{r-1}{}_1 - \alpha^{r-1}{}_{r-1} = \pi_r \prod_1^{r-1} m_w,$$

$$N^i{}_1 = (0,0,0,\cdots,0,\cdots,0,\alpha^i{}_r),$$

$$\alpha^r{}_r = \alpha^{r-1}{}_r - \alpha^{r-1}{}_{r-1},$$

$$N^r{}_1 (\mathrm{mod}\, m_r) = (\pi_r \prod_1^{r-1} m_w)(\mathrm{mod}\, m_r) = \alpha^r{}_r,$$

$$\pi_r = (\frac{\alpha^r{}_r}{\prod_1^{r-1} m_w})(\mathrm{mod}\, m_r),$$

$$\Delta_i = \prod_1^{r-1} m_w (\frac{\alpha^r{}_r}{\prod_1^{r-1} m_w})(\mathrm{mod}\, m_r),$$

$$\Delta_i (\mathrm{mod}\, \tilde{m}_j) = (\prod_1^{r-1} m_w (\frac{\alpha^r{}_r}{\prod_1^{r-1} m_w})(\mathrm{mod}\, m_r))(\mathrm{mod}\, \tilde{m}_j),$$

$$j = 1,2,\ldots,s.$$

Следовательно, метод базируется на получении итеративным путем слагаемых Δ_i. Табл.

doi 10.15802/stp2016/74735

ISSN 2307–3489 (Print), ISSN 2307–6666 (Online)
Наука та прогрес транспорту. Вісник Дніпропетровського національного університету залізничного транспорту, 2016, № 63 (3)

1–3 поясняют, например, для системы модулей $m_1 = 5,\ m_2 = 7,\ m_3 = 3,\ \tilde{m}_1 = 11,\ \tilde{m}_2 = 13$ формирование слагаемых Δ_i в соответствии с приведенными выше зависимостями.

Таблица 1

Table 1

Модули						
5			7	3	11	13
π_1	Δ_1	$\alpha^1{}_1$	$\alpha^1{}_2$	$\alpha^1{}_3$	$\tilde{\alpha}^1_1$	$\tilde{\alpha}^1_2$
0	0	0	0	0	0	0
1	1	1	1	1	1	1
2	2	2	2	2	2	2
3	3	3	3	0	3	3
4	4	4	4	1	4	4

Таблица 2

Table 2

Модули					
7			3	11	13
π_2	$\Delta_2 = \pi_2 m_1$	$\alpha^2{}_2$	$\alpha^2{}_3$	$\tilde{\alpha}^2_1$	$\tilde{\alpha}^2_2$
0	0	0	0	0	0
1	5	5	2	5	5
2	10	3	1	10	10
3	15	1	0	4	2
4	20	6	2	9	7
5	25	4	1	3	12
6	30	2	0	8	4

Таблица 3

Модули				
3			11	13
π_3	$\Delta_3 = \pi_3 m_1 m_2$	$\alpha^3{}_3$	$\tilde{\alpha}^3_1$	$\tilde{\alpha}^3_2$
0	0	0	0	0
1	35	2	2	9
2	70	1	4	5

Проиллюстрируем изложенное для перехода от представления числа $N^1{}_1 = 59 = (4, 3, 2)$ в системе модулей $m_1 = 5,\ m_2 = 7,\ m_3 = 3$, $M_1 = m_1 m_2 m_3 = 5 \cdot 7 \cdot 3 = 105$ к его представлению в системе модулей $\tilde{m}_1 = 11, \tilde{m}_2 = 13$, $M_2 = \tilde{m}_1 \tilde{m}_2 = 11 \cdot 13 = 143$, $M_2 > M_1$. До определения значений остатков $\tilde{\alpha}_1$ и $\tilde{\alpha}_2$ примем их начальные значения равными нулю, то есть $N^1{}_2 = (0,0)$.

На первой итерации из табл. 1 для $\alpha^1{}_1 = 4$ выбираем константы 4, 4, 1 соответственно по модулям $m_1 = 5, m_2 = 7, m_3 = 3$, которые вычитаем из остатков 4, 3, 2. Получаем $N^1{}_1 = 55 = (0,6,1)$. Из этой же табл. 1 для $\alpha^1{}_1 = 4$ выбираем константы 4, 4 по модулям $\tilde{m}_1 = 11, \tilde{m}_2 = 13$ соответственно, которые прибавляем к остаткам 0, 0. В результате получаем $N^1{}_2 = (4,4)$.

На второй итерации из табл. 2 для $\alpha^2{}_2 = 6$ выбираем константы 6, 2 по модулям $m_2 = 7, m_3 = 3$ соответственно, которые вычитаем из остатков 6, 1. Получаем $N^2{}_1 = 35 = (0,0,2)$. Из этой же табл. 2 для $\alpha^2{}_2 = 6$ выбираем константы 9, 7 по модулям $\tilde{m}_1 = 11, \tilde{m}_2 = 13$ соответственно, которые прибавляем к остаткам 4, 4. В результате получаем $N^2{}_2 = (2,11)$.

На третьей итерации из табл. 3 для $\alpha^3{}_3 = 2$ выбираем константу 2 по модулю $m_3 = 3$, которую вычитаем из остатка 2. Получаем $N^3{}_1 = 35 = (0,0,0)$. Из этой же табл. 3 для $\alpha^3{}_3 = 2$ выбираем константы 2, 9 по модулям $\tilde{m}_1 = 11, \tilde{m}_2 = 13$ соответственно, которые прибавляем к остаткам 2, 11. В результате получаем $N^3{}_2 = 59 = (4,7)$.

Результаты

Получено эффективное решение немодульной операции системы остаточных классов для перехода от представления числа одной системой модулей к его представлению другой системой модулей.

doi 10.15802/stp2016/74735

Научная новизна и практическая значимость

Предложено теоретическое обоснование одного подхода к решению немодульной операции системы остаточных классов для перехода от представления числа одной системой модулей к его представлению другой системой модулей. Данный подход целесообразно рассматривать в качестве одного из направлений по исследованию путей повышения эффективности вычислений при разработке модулярных вычислительных структур.

Выводы

Рассмотрен один из подходов к решению задачи перехода от представления числа одной системой модулей к его представлению другой системой модулей. Подход базируется на определении остатка по данному модулю на основе полученных остатков по остальным модулям системы. Такое определение выполняют последовательным вычитанием констант из полученных остатков и подсуммированием этих констант к результатам, которые образуются по данному модулю. При этом константы на каждой итерации выбираются в зависимости от значения остатка в анализируемом разряде. Предложенный метод алгоритмически прост и при схемной реализации позволяет создавать вычислительные структуры высокой производительности и надежности.

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. Вдовин, В. М. Теория систем и системный анализ / В. М. Вдовин, Л. Е. Суркова, В. А. Валентинов. – Москва : Дашков и К°, 2010. – 640 с.
3. Габидулин, Э. М. Защита информации: учеб. пособие / Э. М. Габидулин, А. С. Кшевецкий, А. И. Колыбельников. – Москва : МФТИ, 2011. – 262 с.
4. 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.
5. Кнут, Д. Искусство программирования. Т. 2. Получисленные алгоритмы / Д. Кнут. – Москва : Диалектика-Вильямс, 2013. – 832 с.
6. 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.
7. Методы и алгоритмы округления, масштабирования и деления чисел в модулярной арифметике / Н. И. Червяков [и др.] // 50 лет модулярной арифметики : тр. юбил. Междунар. науч.-техн. конф. (23.11–25.11.2005) / Моск. ин-т электрон. техники. – Москва, 2015. – С. 291–310.
8. Модулярные параллельные вычислительные структуры нейропроцессорных систем : монография / под ред. Н. И. Червякова. – Москва : Физматлит, 2003. – 288 с.
9. Нестеренко, Ю. В. Теория чисел : учебник / Ю. В. Нестеренко. – Москва : Академия, 2008. – 272 с.
10. Нестерова, Л. Ю. Китайская теорема об остатках в области главных идеалов / Л. Ю. Нестерова, С. В. Феклистов // Молодой ученый. – 2014. – № 19. – С. 1–4.
11. Переславцева, О. Н. Распараллеливание алгоритмов с применением китайской теоремы об остатках / О. Н. Переславцева // Вестн. Тамбов. ун-та. Серия : Естеств. и техн. науки. – 2009. – № 4, т.14. – С. 779–781.
12. 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.
13. Полисский, Ю. Д. Выполнение сложных операций в модулярных вычислительных структурах / Ю. Д. Полисский // Автоматика-2008 : доп. XV міжнар. конф. з автоматичного управління (23.09–26.09.2008) / НУ «Одеська морська академія» – Одеса, 2008. – Ч. І. – С. 444–446.
14. Полисский, Ю. Д. О выполнении сложных операций в системе остаточных классов / Ю. Д. Полисский // Электронное моделирование. – 2006. – Т. 28, № 3. – С. 117–123.
15. Поліський, Ю. Д. Про один метод розширення діапазону зображення чисел у системі залишкових класів / Ю. Д. Поліський // Математичне моделювання. – 2007. – № 2. – С. 16–17.
16. Приближенный метод выполнения немодульных операций в системе остаточных классов /

doi 10.15802/stp2016/74735

Н. И. Червяков, В. М. Авербух, М. Г. Бабенко [и др.] // Фундаментальные исследования. – 2012. – № 6 (1). – С. 189–193.

17. Червяков, Н. И. Методы, алгоритмы и техническая реализация основных проблемных операций, выполняемых в системе остаточных классов / Н. И. Червяков // Инфокоммуникационные технологии / Поволж. гос. ун-т телеком. и информатики. – Самара, 2011. – № 4. – С. 4–12.
18. 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.
19. 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.
20. 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.
21. 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.

Ю. Д. ПОЛІСЬКИЙ[1*]

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

ПРО ПЕРЕТВОРЕННЯ ПРЕДСТАВЛЕННЯ ЧИСЕЛ У ЗАЛИШКАХ ІЗ ОДНІЄЇ СИСТЕМИ МОДУЛІВ В ІНШУ

Мета. У роботі передбачається провести теоретичне обґрунтування одного з підходів до підвищення ефективності виконання в непозиційній системі числення залишкових класів немодульної, так званої складної операції, для реалізації якої необхідно знання цифр операндів в усіх розрядах. Операція полягає в перетворенні представлення числа з однієї системи модулів поданням його в іншій системі модулів. **Методика.** Інструментами методики досліджень являються системний аналіз, теорія чисел, китайська теорема про залишки. Методика використовує представлення числа як своїми залишками, так і в поліадичнім коді та базується на визначенні залишку по даному модулю на основі отриманих залишків по решті модулів вихідної системи. Таке визначення виконують послідовним відніманням констант із одержуваних залишків вихідного числа і додаванням цих констант до результатів, які утворюються по шуканим модулям. При цьому константи на кожній ітерації вибираються з попередньо розрахованих таблиць, залежно від значення залишку в аналізованому розряді. Запропонований метод алгоритмічно простий та при схемній реалізації дозволяє створювати обчислювальні структури високої продуктивності й надійності. **Результати.** У роботі виконано теоретичне обґрунтування розглянутого підходу для отримання ефективного вирішення немодульної операції перетворення в системі залишкових класів для переходу від подання числа однією системою модулів до його подання іншою системою модулів. **Наукова новизна.** Автором запропоновано теоретичне обґрунтування представленого підходу до вирішення немодульної операції перетворення в системі залишкових класів для переходу від представлення числа в одній системі модулів до його представлення в іншій системі модулів. Даний підхід доцільно розглядати в якості одного з напрямків дослідження шляхів підвищення ефективності обчислень. **Практична значимість.** Важливість теоретичних висновків та отриманих результатів дослідження полягає в тому, що обґрунтовано простий і ефективний підхід до вирішення задачі виконання немодульної операції перетворення в системі залишкових класів для переходу від представлення числа в одній системі модулів до його представлення в іншій системі модулів. Розглянуті рішення мають високу швидкодію та можуть бути ефективними при розробці модулярних обчислювальних структур для перспективних інформаційних технологій.

Ключові слова: залишкові класи; число; складні операції; позиційна характеристика; системи модулів; ітерація

doi 10.15802/stp2016/74735

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

Наука та прогрес транспорту. Вісник Дніпропетровського національного університету залізничного транспорту, 2016, № 63 (3)

YU. D. POLISSKY[1*]

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

ON THE TRANSFORMATION OF REPRESENTATION OF NUMBERS IN THE RESIDUO FROM ONE MODULE SYSTEM TO ANOTHER

Purpose. The purpose of this work is the theoretical foundation of one of the approaches to improve the effectiveness of the number system in nonpositional residual classes non-modular, so-called complex operation, the realization of which requires knowledge of all the digits of operands charges. The operation consists in transformation of the representation of one of the modules of its representation in the other system of modules. **Methodology.** The tools of research methodology are the system analysis, theory of numbers, the Chinese remainder theorem. The technique uses a representation of number as its residues, and in the polyadic code and is based on the determination of the balance of the module based on the obtained residues on the remaining modules of the original system. Such a determination is performed by sequentially subtracting of constants from the obtained residues of the original number and summing of these constants to the results, which are formed by the required modules. Thus, constant at each iteration are selected from pre-calculated tables depending on the value of the residue in the analyzed discharge. The proposed method is algorithmically simple and at circuit implementation can create the computational structures of high performance and reliability. **Findings.** The theoretical justification for this approach to obtain effective solutions of non-modular transformation operation in the system of residual classes for transition from representation of the number by the one system of units to its representation by the other system of modules. **Originality.** A theoretical justification of the proposed approach to the solution of a non-modular conversion operations in the residue number system for the transition from representation of number in one system of units to its representation in the other system of modules was proposed. This approach is appropriate to consider as one of the areas of research ways to improve the computational efficiency. **Practical value.** It follows from the importance of the theoretical conclusions and results of the study. It consists in the fact that it is justified a simple and effective approach to the problem of implementation of non-modular conversion operations in the residue number system for the transition from representation of the number in one system of units to its representation in the other system of modules. The above mentioned solutions have a high speed and may be effective in the development of modular computing structures for advanced information technologies.

Keywords: residual classes; number; complex operations; positional characteristic; system of modules; iteration

REFERENCES

1. Akushskiy I.Ya., Yuditskiy D.I. *Mashinnaya arifmetika v ostatochnykh klassakh* [Machine arithmetic in the residual classes]. Moscow, Sovetskoye radio Publ., 1968. 440 p.
2. Vdovin V.M., Surkova L.Ye., Valentinov V.A. *Teoriya sistem i sistemnyy analiz* [Systems theory and systems analysis]. Moscow, Dashkov i K° Publ., 2010. 640 p.
3. Gabidulin E.M., Kshevetskiy A.S., Kolybelnikov A.I. *Zashchita informatsii* [Data protection]. Moscow, MFTI Publ., 2011. 262 p.
4. Irkhin V.P. Tablichnaya realizatsiya operatsiy modulyarnoy arifmetiki [Tabular implementation of modular arithmetic operations]. *Trudy yubileynoy Mezhdunarodnoy nauchno-tekhnicheskoy konferentsii «50 let modulyarnoy arifmetiki»* [Proc. of Anniversary Intern. Sci. and Techn. Conf. «50 years of modular arithmetic»]. Moscow, 2015, pp. 268-273.
5. Knut D. *Iskusstvo programmirovaniya. Tom 2. Poluchislennyye algoritmy* (Programming art. Vol. 2. Seminumerical algorithms). Moscow, Dialektika-Vilyams Publ., 2013. 832 p.
6. 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 prohres transportu – Science and Transport Progress*, 2013, no. 6 (48), pp. 7-22. doi: 10.15802/stp2013/19835.
7. 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 algorithms for rounding, scaling, and dividing numbers in modular arithmetic]. *Trudy yubileynoy Mezhdunarodnoy nauchno-tekhnicheskoy konfer-*

doi 10.15802/stp2016/74735

entsii «50 let modulyarnoy arifmetiki» [Proc. of Anniversary Intern. Sci. and Technical Conf. «50 years of modular arithmetic»]. Moscow, 2015, pp. 291-310.

8. Chervyakov N.I. *Modulyarnyye parallelnyye vychislitelnyye struktury neyroprotsessornykh sistem* [Modular parallel computing structure of neuroprocessor systems]. Moscow, Fizmatlit Publ., 2003. 288 p.
9. Nesterenko Yu.V. *Teoriya chisel* [Number theory]. Moscow, Akademiya Publ., 2008. 272 p.
10. Nesterova L.Yu., Feklistov S.V. Kitayskaya teorema ob ostatkakh v oblasti glavnykh idealov [Chinese remainder theorem in principal ideal]. *Molodoy uchenyy – Young Scientist*, 2014, no. 19, pp. 1-4.
11. Pereslavtseva O.N. Rasparallelivanie algoritmov s primeneniyem kitayskoy teoremy ob ostatkakh [Parallelization of the algorithms using the Chinese remainder theorem]. *Vestnik Tambovskogo universiteta. Seriya: Estestvennyye i tekhnicheskiye nauki* [Bulletin of Tambov University. Series: Natural and Technical Sciences], 2009, no. 4, pp. 779-781.
12. 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 Univesity of Railway Transport named after Academician V. Lazaryan], 2007, issue 16, pp. 68-72.
13. Polisskiy Yu.D. Vypolneniye slozhnykh operatsiy v modulyarnykh vychislitelnykh strukturakh [Performing of complex operations in modular computing structures]. *Dopovidi XV mizhnarodnoi konferentsii z avtomatichnoho upravlinnia «Avtomatika-2008»* [Proc. of the XV Intern. Conference on Automatic Control «Automation-2008»]. National University «Odessa Maritime Academy», Odessa, 2008, Part I, pp. 444-446.
14. Polisskiy Yu.D. O vypolnenii slozhnykh operatsiy v sisteme ostatochnykh klassov [On the implementation of complex operations in the residue number system]. *Elektronnoye modelirovaniye – Electronic Modeling*, 2006, vol. 28, no. 3, pp.117-123.
15. Polisskiy Yu.D. Pro odyn metod rozshyrennia diapazonu zobrazhennia chysel u systemi zalyshkovykh klasiv [A method for expanding the range of image numbers in the system of residual classes]. *Matematychne modeliuvannia – Mathematical Modelling*, 2007, no. 2, pp. 16-17.
16. Chervyakov N.I., Averbukh V.M., Babenko M.G. Priblizhennyy metod vypolneniya nemodulnykh operatsiy v sisteme ostatochnykh klassov [An approximate method for performing non-modular operations in the residue number system]. *Fundamentalnyye issledovaniya – Fundamental Research*, 2012, no. 6 (1), pp. 189-193.
17. Chervyakov N.I. Metody, algoritmy i tekhnicheskaya realizatsiya osnovnykh problemnykh operatsiy, vypolnyayemykh v sisteme ostatochnykh klassov [Methods, algorithms and technical implementation of the basic problem operations performed in the system of remaining classes]. *Infokommunikatsionnyye tekhnologii – Information and Communication Technologies*, 2011, no. 4, pp. 4-12.
18. 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»* [Proc. of Anniversary International Sci. and Technical Conf. «50 years of modular arithmetic»]. Moscow, 2005, pp. 232-242.
19. Boateng K.O., Baagyere E.Y. A Smith-Waterman Algorithm Accelerator Based on Residue Number System. *International Journal of Electronics and Communication Engineering*, 2012, vol. 5, no. 1, pp. 99-112.
20. Tomczak T. Hierarchical residue number systems with small moduli and simple converters. *International Journal of Applied Mathematics and Computer Science*, 2011, vol. 21, issue 1, pp. 173-192. doi: 10.2478/v10006-011-0013-2
21. Youssef M.I., Emam A.E., Abd Elghanym M. Multi-Layer Data Encryption Using Residue Number System in DNA Sequence. *International 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: 11.03.2016
Принята к печати: 08.06.2016

