КОРОТКІ ПОВІДОМЛЕННЯ

УДК 681.04

Ю.Д. Полисский, канд. техн. наук
Научно-исследовательский ин-т автоматизации черной металлургии
(Украина, 49000, Днепр, ул. Шевченко, 59,
тел. (056) 7443365, e-mail: polissky477@gmail.com)

Преобразование псевдочисел системы остаточных классов со всеми четными модулями в числа системы

Изложен подход к преобразованию псевдочисел системы остаточных классов со всеми четными модулями в числа системы. Подход основан на формировании произвольного набора остатков и проверке на принадлежность данного набора диапазону системы, в которой используются таблицы констант вычитания. В случае невыполнения этого условия для некоторого остатка осуществляется замена этого остатка таким остатком, для которого данное условие выполняется.

К л ю ч е в ы е с л о в а: остаточные классы, диапазон, четные модули, алгоритм.

Викладено підхід до перетворення псевдочисел системи залишкових класів з усіма парними модулями в числа системи. Підхід базовано на формуванні довільного набору залишків і перевірці на приналежність даного набору діапазону системи, в якій використовуються таблиці констант віднімання. У разі невиконання цієї умови для деякого залишку здійснюється заміна цього залишку таким залишком, для якого ця умова виконується.

К л ю ч о в і с л о в а: залишкові класи, діапазон, парні модулі, алгоритм.

Под системой остаточных классов (СОК) [1] понимают систему счисления, в которой произвольное число N представляется в виде набора наименьших неотрицательных остатков по модулям $m_1, m_2, ..., m_n$, т.е. $N = (\alpha_1, \alpha_2, ..., \alpha_n)$. Здесь $\alpha_i = N \pmod{m_i}$. При этом, если числа m_i попарно взаимно простые, то такому представлению соответствует только одно число N диапазона $[0, M)$, где $M = m_1 m_2 ... m_n$. Если системой оснований полиадического кода также является система $m_1, m_2, ..., m_n$, число N в полиадическом коде представляется исключительно в виде $N = \pi_1 + \pi_2 m_1 + ... + \pi_i m_1 m_2 ... m_{i-1} + ... + \pi_{n-1} m_1 m_2 ... m_{n-2} + \pi_n m_1 m_2 ... m_{n-1}$, где $0 \le \pi_i \le m_i - 1$.

В настоящее время для реализации некоторых проблемных операций, например модульного возведения в степень и нахождения дискретного логарифма, предложены решения [2], в которых наряду с использованием систем взаимно простых модулей применяются также системы, где числа m_i не

являются взаимно простыми, в частности в работе [2] они все четные. Однако, если числа m_i не являются взаимно простыми, то представлению $N=(\alpha_1, \alpha_2,...,\alpha_n)$ соответствуют несколько чисел диапазона $[0, M)$.

Устранить данную неоднозначность можно так. Величина M, равная произведению $m_1, m_2, ..., m_n$ в системе взаимно простых модулей m_i, является, по сути, наименьшим общим кратным этих модулей, т.е. $M = m_1\ m_2\ ...\ m_n = \langle m_1, m_2, ..., m_n \rangle$. Если понятие величины M как наименьшего общего кратного распространить на систему модулей, не являющихся взаимно простыми, то и в этом случае каждому числу из $[0, \hat{M})$ будет соответствовать единственный набор $N=(\alpha_1, \alpha_2, ..., \alpha_n)$. При таком обобщении число в полиадическом коде для той же системы модулей, не являющихся взаимно простыми, представляется в виде

$$N = \pi_1 + \pi_2 \langle m_1 \rangle + ... + \pi_i \langle m_1, m_2, ..., m_{i-1} \rangle + ... + \pi_n \langle m_1, m_2, ..., m_{n-1} \rangle,$$
$$0 \le \pi_i \le m_i - 1,\ i = 1, 2, ..., n.$$

Величина $M = m_1\ m_2\ ...\ m_n$ существенно больше $\hat{M} = \langle m_1, m_2, ..., m_n \rangle$. Например для системы четных модулей $m_1 = 10,\ m_2 = 6,\ m_3 = 12,\ m_4 = 8$ получаем $\theta = M / \hat{M} = 48$. Поэтому значительная часть наборов остатков $(\alpha_{m_1}, \alpha_{m_2}, \alpha_{m_3}, \alpha_{m_4})$, составленная из элементов множеств соответственно $\Re_1 = \{0, 1, 2, ..., m_1 - 1\}$, $\Re_2 = \{0, 1, 2, ..., m_2 - 1\}$, $\Re_3 = \{0, 1, 2, ..., m_3 - 1\}$, $\Re_4 = \{0, 1, 2, ..., m_4 - 1\}$, оказывается вне диапазона $[0, \hat{M})$. Будем называть такие наборы псевдочислами системы.

Задача состоит в преобразовании псевдочисел в числа системы, т.е. в переходе от псевдочисел к такому набору остатков $(\alpha_{m_1}, \alpha_{m_2}, \alpha_{m_3}, \alpha_{m_4})$, который принадлежит диапазону $[0, \hat{M})$. Алгоритм решения задачи следующий.

Из множеств $\Re_1, \Re_2, \Re_3, \Re_4$ составляем произвольный набор $(\alpha_{m_1}, \alpha_{m_2}, \alpha_{m_3}, \alpha_{m_4})$ и выполняем проверку на принадлежность этого набора диапазону $[0, \hat{M})$ с помощью таблиц констант вычитания. В случае, если для некоторого остатка α_{m_r}, $r = 1, 2, 3, 4$, из данного набора $(\alpha_{m_1}, \alpha_{m_2}, \alpha_{m_3}, \alpha_{m_4})$ условие не выполняется, выбираем одновременно ближайший меньший $\alpha_{m_м}$ и ближайший больший $\alpha_{m_б}$ остатки из соответствующего множества $\Re_j$, $j = 1, 2, 3, 4$.

Составляем два набора. В первом выполняем замену α_{m_r} на $\alpha_{m_м}$, во втором — замену α_{m_r} на $\alpha_{m_б}$. Затем выполняется проверка на принадлежность каждого из новых наборов диапазону $[0, \hat{M})$. Поскольку алгоритм сходится, после его отработки получаем число системы.

Пример. Рассмотрим систему модулей $m_1 = 10,\ m_2 = 6,\ m_3 = 12,\ m_4 = 8$. Поскольку константы вычитания включают произведения четных модулей, остатки должны быть либо все четные, либо все нечетные. Пусть из множества $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$ выбран элемент $\alpha_{10} = 1$, из множества

$\{1, 2, 3, 4, 5\}$ — элемент $\alpha_6 = 3$, из множества $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$ — элемент $\alpha_{12} = 5$, из множества $\{0, 1, 2, 3, 4, 5, 6, 7\}$ — элемент $\alpha_8 = 5$. Эти элементы составляют набор ($\alpha_{10} = 1, \alpha_6 = 3, \alpha_{12} = 5, \alpha_8 = 5$).

В табл. 1—6 представлен процесс проверки принадлежности набора ($\alpha_{10} = 1$, $\alpha_6 = 3$, $\alpha_{12} = 5$, $\alpha_8 = 5$) диапазону $[0, \hat{M})$, $\hat{M} = \langle m_1, m_2, m_3, m_4 \rangle = \langle 10, 6, 12, 8 \rangle = 120$.

На первой итерации из табл. 1 по остатку $\alpha_{10} = 1$ набора ($\alpha_{10} = 1, \alpha_6 = 3, \alpha_{12} = 5, \alpha_8 = 5$) в блоке А (строка 1 в табл. 2) выбираем строку констант $\widetilde{\Delta}_{10} = 1$, $\widetilde{\Delta}_6 = 1$, $\widetilde{\Delta}_{12} = 1$, $\widetilde{\Delta}_8 = 1$ для модулей соответственно $m_1 = 10$, $m_2 = 6$, $m_3 = 12$, $m_4 = 8$, которую записываем в строку 2 блока А в табл. 2 и вычитаем поэлементно из набора ($\alpha_{10} = 1, \alpha_6 = 3, \alpha_{12} = 5, \alpha_8 = 5$). Получаем новый набор ($\widetilde{\alpha}_{10} = 0, \widetilde{\alpha}_6 = 2, \widetilde{\alpha}_{12} = 4, \widetilde{\alpha}_8 = 4$) — строка 3 в блоке А в табл. 2. Одновременно во вспомогательной табл. 3 строку констант суммируем с предыдущей строкой. В рассматриваемом случае строку 2 суммируем со строкой 1 и получаем результат в строке 3.

На следующей итерации из табл. 4 по остатку $\widetilde{\alpha}_6 = 2$ набора ($\widetilde{\alpha}_{10} = 0, \widetilde{\alpha}_6 = 2, \widetilde{\alpha}_{12} = 4, \widetilde{\alpha}_8 = 4$) в блоке А (строка 3 в табл. 2) выбираем строку констант $\widetilde{\Delta}_6 = 2$, $\widetilde{\Delta}_{12} = 8$, $\widetilde{\Delta}_8 = 4$ для модулей соответственно $m_2 = 6$, $m_3 = 12$, $m_4 = 8$, которую записываем в строку 4 блока А табл. 2 и вычитаем поэлементно из набора ($\widetilde{\alpha}_6 = 2, \widetilde{\alpha}_{12} = 4, \widetilde{\alpha}_8 = 4$) — строка 3 блока А в табл. 2. Получаем новый набор ($\widetilde{\alpha}_6 = 0, \widetilde{\alpha}_{12} = 8, \widetilde{\alpha}_8 = 0$) — строка 5 блока А в табл. 2. Одновременно во вспомогательной табл. 3 строку 4 констант суммируем с предыдущей строкой 3 и получаем результат в строке 5.

Таблица 1

$m_1 = 10$			$m_2 = 6$	$m_3 = 12$	$m_4 = 8$
π_{10}	$\Delta_{10} = \pi_{10}$	$\widetilde{\alpha}_{10} = \widetilde{\Delta}_{10} = \langle \Delta_{10} (\mathrm{mod}\, 10) \rangle$	$\widetilde{\alpha}_6 = \widetilde{\Delta}_6 = \langle \Delta_{10} (\mathrm{mod}\, 6) \rangle$	$\widetilde{\alpha}_8 = \widetilde{\Delta}_8 = \langle \Delta_{10} (\mathrm{mod}\, 8) \rangle$	$\widetilde{\alpha}_8 = \widetilde{\Delta}_8 = \langle \Delta_{10} (\mathrm{mod}\, 8) \rangle$
0	0	0	0	0	0
1	1	1	1	1	1
2	2	2	2	2	2
3	3	3	3	3	3
4	4	4	4	4	4
5	5	5	5	5	5
6	6	6	0	6	6
7	7	7	1	7	7
8	8	8	2	8	0
9	9	9	3	9	1

На третьей итерации обращаемся к табл. 5 для выбора строки констант по остатку $\tilde{\alpha}_{12}=8$ набора ($\tilde{\alpha}_6=0, \tilde{\alpha}_{12}=8, \tilde{\alpha}_8=0$) из блока А в табл. 2. Однако в табл. 5 строка констант для $\tilde{\alpha}_{12}=8$ отсутствует. Следовательно, набор, в котором в сочетании с $\alpha_{10}=1$ и $\alpha_6=3$ находится элемент $\alpha_{12}=5$, не входит в диапазон [0, 120), и значение элемента $\alpha_{12}=5$ необходимо изменить. Для этого из множества {0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11} выбираем новое, в частности ближайшее меньшее нечетное значение элемента $\alpha_{12}=3$, и составляем набор ($\alpha_{10}=1, \alpha_6=3, \alpha_{12}=3, \alpha_8=5$) — строка 1 блока Б в табл. 2. Поскольку по значениям $\alpha_{10}=1$ и $\alpha_6=3$ из элементов α_{12} и α_8 вычитались суммы констант — соответственно числа 9 и 5 (строка 5 в табл. 3), выполним вычитание этих сумм из новых значений $\alpha_{12}=3$ и $\alpha_8=5$. Получаем $\tilde{\alpha}_{12}=6$ и $\tilde{\alpha}_8=0$ — строка 3 блока Б в табл. 2. Перепишем эту строку в качестве нового набора в строку 6 блока А в табл. 2.

Таблица 2

Блок А						Блок Б				
Номер строки	Операция	Остатки для модулей				Операция	Остатки для модулей			
		10	6	12	8		10	6	12	8
1	Исходный набор	1	3	5	5	Новый набор	1	3	3	5
2	Вычитание	1	1	1	1	Вычитание	—	—	9	5
3	Результат	0	2	4	4	Результат	—	—	6	0
4	Вычитание	—	2	8	4	Новый набор	1	3	3	3
5	Результат	—	0	8	0	Вычитание	—	—	—	3
6	Новый набор	—	—	6	0	Результат	—	—	—	0
7	Вычитание	—	—	6	6					
8	Результат	—	—	0	2					

Таблица 3

Номер строки	Операция	Константы для модулей			
		10	6	12	8
1		0	0	0	0
2	Сложение	1	1	1	1
3	Результат	1	1	1	1
4	Сложение	—	2	8	4
5	Результат	—	3	9	5
6	Сложение	—	—	6	6
7	Результат	—	—	3	3

На четвертой итерации из табл. 5 по остатку $\widetilde{\alpha}_{12}=6$ набора ($\widetilde{\alpha}_{12}=6$, $\widetilde{\alpha}_{8}=0$) выбираем строку констант $\widetilde{\Delta}_{12}=6$, $\widetilde{\Delta}_{8}=6$ для модулей соответственно $m_3=12$, $m_4=8$, записываем в строку 7 блока А в табл. 2 и вычитаем поэлементно из набора ($\widetilde{\alpha}_{12}=6, \widetilde{\alpha}_{8}=0$). Получаем ($\widetilde{\alpha}_{12}=0, \widetilde{\alpha}_{8}=2$) — строка 8 блока А в табл. 2.

На пятой итерации обращаемся к табл. 6 для выбора строки констант по остатку $\widetilde{\alpha}_{8}=2$ набора ($\widetilde{\alpha}_{12}=0, \widetilde{\alpha}_{8}=2$) из блока А в табл. 2. Однако в табл. 6 строка констант для $\widetilde{\alpha}_{8}=2$ отсутствует. Следовательно, набор, в котором в сочетании с $\alpha_{10}=1$, $\alpha_{6}=3$ и $\alpha_{12}=3$ находится элемент $\alpha_{8}=5$, не входит в диапазон [0, 120), и значение элемента $\alpha_{8}=5$ необходимо изменить. Для этого из множества {0, 1, 2, 3, 4, 5, 6, 7} выбираем новое, в частности ближайшее меньшее нечетное значение элемента $\alpha_{8}=3$, и составляем набор ($\alpha_{10}=1$, $\alpha_{6}=3$, $\alpha_{12}=3$, $\alpha_{8}=3$) — строка 4 из блока Б в табл. 2. Поскольку по значениям $\alpha_{10}=1, \alpha_{6}=3$ и $\alpha_{12}=3$ из элемента α_{8} вычиталась сумма констант — число 3 (строка 7 в табл. 3), выполним вычитание этого числа из нового значения $\alpha_{8}=3$ — строка 5 блока А в табл. 2. Получаем $\widetilde{\alpha}_{8}=0$ — строка 6 блока Б в табл. 5. Следовательно, набор остатков ($\alpha_{10}=1$, $\alpha_{6}=3, \alpha_{12}=3, \alpha_{8}=3$) принадлежит диапазону [0, 120).

Таблица 4

$m_2=6$			$m_3=12$	$m_4=8$
π_6	$\Delta_6=\pi_6\langle 10\rangle$	$\widetilde{\alpha}_6=\widetilde{\Delta}_6=$ $=\langle\Delta_6(\mathrm{mod}\,6)\rangle$	$\widetilde{\alpha}_{12}=\widetilde{\Delta}_{12}=$ $=\langle\Delta_6(\mathrm{mod}\,12)\rangle$	$\widetilde{\alpha}_8=\widetilde{\Delta}_8=$ $=\langle\Delta_6(\mathrm{mod}\,8)\rangle$
0	0	0	0	0
1	10	4	10	2
2	20	2	8	4
3	30	0	6	6
4	40	4	4	0
5	50	2	2	2

Таблица 5

$m_3=12$			$m_4=8$
π_{12}	$\Delta_{12}=$ $=\pi_{12}\langle 10,6\rangle$	$\widetilde{\alpha}_{12}=\widetilde{\Delta}_{12}=$ $=\langle\Delta_{12}(\mathrm{mod}\,12)\rangle$	$\widetilde{\alpha}_8=\widetilde{\Delta}_8=$ $=\langle\Delta_{12}(\mathrm{mod}\,8)\rangle$
0	0	0	0
1	30	6	6
2	60	0	4
3	90	6	2

Таблица 6

$m_4=8$		
π_8	$\Delta_8=$ $=\pi_8\langle 10,6,12\rangle$	$\widetilde{\alpha}_8=\widetilde{\Delta}_8=$ $=\langle\Delta_8(\mathrm{mod}\,8)\rangle$
0	0	0
1	60	4

Таким образом, рассмотренный алгоритм обеспечивает преобразование псевдочисел системы остаточных классов со всеми четными модулями в числа системы.

Выводы

Предложенный подход к преобразованию псевдочисел системы остаточных классов со всеми четными модулями в числа системы можно рассматривать как направление исследований по повышению эффективности выполняемых операций в системе остаточных классов.

СПИСОК ЛИТЕРАТУРЫ

1. *Акушский И.Я., Юдицкий Д.И.* Машинная арифметика в остаточных классах. М. : Сов. радио, 1968, 440 с.
2. *Полисский Ю.Д.* О некоторых подходах к выполнению проблемных операций в системе остаточных классов // Электрон. моделирование. 2017, **39**, № 4, с. 105—114.

Поступила 25.10.17

REFERENCES

1. Akushskiy, I.Ya. and Yuditskiy, D.I. (1968), *Mashinnaya arifmetika v ostatochnykh klassakh* [Machine arithmetic in the residual classes], Sovetskoe radio, Moscow, USSR.
2. Polissky, Yu.D. (2017), "On some approaches to the implementation of problematic operations in the system of residual classes", *Electronnoe modelirovanie*, Vol. 39, no. 4, pp. 105-114.

Received 25.10.17

Yu.D. Polissky

TRANSFORMATION OF PSEUDO-NUMBERS
OF THE RESIDUAL CLASS SYSTEM WITH ALL EVEN MODULES INTO
THE NUMBERS OF THE SYSTEM

The approach to the transformation of pseudo-numbers of the residual class system with all even modules into the numbers of the system is expounded. The approach is based on the formation of an arbitrary set of residues and verification of the belonging of a given set to the range of the system based on the use of the tables of subtraction constants. If this condition is not fulfilled, for a certain remainder, this residue is replaced by a residue for which this condition is satisfied.

K e y w o r d s: residual classes, range, even modules, algorithm.

ПОЛИССКИЙ Юрий Давидович, канд. техн. наук, ст. науч. сотр. Научно-исследовательского ин-та автоматизации черной металлургии, г. Днепр. В 1960 г. окончил Днепропетровский металлургический ин-т. Область научных исследований — системы и средства управления.