УДК 681.04

Ю. Д. Полисский, канд. техн. наук
НИИ автоматизации черной металлургии
(Украина, 49000 Днепропетровск,
тел. (056) 7443365, E-mail: polissky@mail.ru)

Некоторые вопросы выполнения сложных операций в системе остаточных классов

Приведено решение задачи деления на два четных чисел, представленных в системе остаточных классов. Метод решения базируется на определении остатка частного по данному модулю на основе полученных остатков частного по остальным модулям системы при условии принадлежности частного первой половине диапазона. В процессе решения основной задачи рассмотрены также решения других задач в системе остаточных классов: разбиение диапазона чисел на интервалы, расширение диапазона чисел, определение принадлежности числа данной половине, построение таблиц выборки констант, необходимых для получения результата.

Наведено розв'язання задачі ділення на два парних чисел, які представлені у системі залишкових класів. Метод розв'язання базується на визначенні залишку частки за даним модулем на базі отриманих залишків частки за рештою модулів системи за умови належності частки до першої половини діапазону. У процесі розв'язування основної задачі розглянуто також розв'язання інших задач у системі залишкових класів: розбиття діапазону чисел на інтервали, розширення діапазону чисел, визначення належності числа до даної половини, побудування таблиць виборки констант, необхідних для отримання результату.

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

Повышение надежности и быстродействия вычислительных структур связано с применением новых принципов, основанных на представлении данных в системе остаточных классов (СОК) [1]. Достоинства СОК, подробно изложенные в [2, 3], заключаются в высокой степени параллелизма при выполнении арифметических операций сложения, вычитания и умножения. Однако возникают определенные трудности при реализации немодульных операций, требующих знания всего числа в целом. К таким операциям относится, в частности, операции деления четного числа на два.

Постановка задачи. Будем использовать определения и обозначения, приведенные в [4]. СОК – это система счисления, в которой произвольное число N представляется в виде набора наименьших неотрицательных остатков по модулям $m_1, m_2, ..., m_n$, т. е. $N = [N(\mathrm{mod}\, m_1), N(\mathrm{mod}\, m_2), ..., N(\mathrm{mod}\, m_n)]$ или $N = (\alpha_1, \alpha_2, ..., \alpha_n)$, где $\alpha_i = N(\mathrm{mod}\, m_i)$. Если все целые числа N при-

надлежат диапазону $[0, M)$, объем которого $M = m_1, m_2, ..., m_n$, а модули m_i взаимно простые, то каждому набору $(\alpha_1, \alpha_2, ..., \alpha_n)$ соответствует только одно число N из этого диапазона.

Будем отличать числа первой и второй половины диапазона. Если $2 = m_1 < m_2 < ... m_n$, то при $0 \le N < M/2$ N — число первой половины, а при $M/2 \le N < M$ N — число второй половины.

Пусть в системе с основаниями $m_1 = 2, m_2, ..., m_n$ даны два числа $N_1 = (\alpha_1, \alpha_2, ..., \alpha_n)$ и $N_2 = (0, 2, ..., 2)$ и пусть $C = (\gamma_1, \gamma_2, ..., \gamma_n)$ — частное от деления N_1 на N_2. Тогда, если деление точно выполнимо, т. е. N_1 кратно N_2, то [4]

$$C \in [0, M/2),\ \gamma_1 = \left(\frac{0}{0}\right)(\mathrm{mod}2),\ \gamma_i = \left(\frac{\alpha_i}{2}\right)(\mathrm{mod}\, m_i),\ i = 2, ..., n. \qquad (1)$$

Тогда все остатки частного, кроме остатка по модулю 2, определяются формальным делением остатков α_i на остатки β_i, $i \ne 1$. Для модуля 2 имеем неопределенность $0/0$, которую требуется раскрыть.

Выполнение сложных операций. Рассмотрим СОК с m_i и m_{i+1}, $m_i < m_{i+1}$. Пусть в этой СОК имеется некоторое число $A^j = (\alpha_i^j, \alpha_{i+1}^j)$, где $\alpha_{i+1}^j = 0$, $j = 0, 1, 2, ..., m_i - 1$. Составим выражение $\Delta_i^j = (\alpha_i^j - \alpha_{i+1}^j)(\mathrm{mod}\, m_i) = \alpha_i^j$. Рассмотрим значения разности при последовательном добавлении к A^j чисел $B^k = 1, 2, ..., k, ..., m_{i+1}$, где $k = (\beta_i^k, \beta_{i+1}^k)$. Получаем $A^{j+1} = A^j + B^k = (\alpha_i^{j+1}, \alpha_{i+1}^{j+1})$, где $\alpha_i^{j+1} = \alpha_i^j + \beta_i^k$, $\alpha_{i+1}^{j+1} = \alpha_{i+1}^j + \beta_{i+1}^k$.

Запишем $\Delta_i^{j+1} = (\alpha_i^{j+1} - \alpha_{i+1}^{j+1})(\mathrm{mod}\, m_i) = (\alpha_i^j + \beta_i^k - \beta_{i+1}^k)(\mathrm{mod}\, m_i)$. Пусть B^k такое, что $\alpha_i^j + \beta_i^k < m_i$. Тогда $\beta_{i+1}^k = \beta_i^k = \beta_1^k$ и $\Delta_i^{j+1} = \alpha_i^j$. Если число B^k такое, что $\alpha_i^j + \beta_i^k = m_i$, то $\beta_{i+1}^k = \beta_i^k = m_i - \alpha_i^j$. Следовательно, $\alpha_i^{j+1} = 0$, $\alpha_{i+1}^{j+1} = \alpha_{i+1}^j + m_i$. В этом случае $\Delta_i^{j+1} = (\alpha_i^{j+1} - \alpha_{i+1}^{j+1})(\mathrm{mod}\, m_i) = (0 - m_i + \alpha_i^j)(\mathrm{mod}\, m_i) = \alpha_i^j$. Если число B^k такое, что $m_i < \alpha_i^j + \beta_i^k < m_{i+1}$, то $\alpha_i^{j+1} = \alpha_i^j + \beta_i^k - m_i$, $\alpha_{i+1}^{j+1} = \beta_i^k$ и $\Delta_i^{j+1} = (\alpha_i^{j+1} - \alpha_{i+1}^{j+1})(\mathrm{mod}\, m_i) = (\alpha_i^j + \beta_i^k - m_i - \beta_i^k)(\mathrm{mod}\, m_i) = \alpha_i^j$. Наконец, при $B^k = m_{i+1}$, при котором $m_i < \alpha_i^j + \beta_i^k$, а $\beta_i^k = (m_{i+1})(\mathrm{mod}\, m_i)$, $\beta_{i+1}^k = m_{i+1}$, получаем $\alpha_i^{j+1} = \alpha_i^j + \beta_i^k - m_i$ и $\alpha_{i+1}^{j+1} = 0$, т. е. $A^{j+1} = (\alpha_i^{j+1}, \alpha_{i+1}^{j+1})$ и $\alpha_{i+1}^{j+1} = 0$, а $\Delta_i^{j+1} = \tilde{\alpha}_i^{j+1}$, где $\tilde{\alpha}_i^{j+1} = (\alpha_i^j + m_{i+1})(\mathrm{mod}\, m_i)$.

Таким образом, после окончания очередного цикла последовательного добавления к A^{j+t}, $t = 1, 2, ..., (m_i - 1) - j$ числа $B = 1, 2, ..., m_{i+1}$ получаем

$$\Delta_i^{j+t} = \tilde{\alpha}_i^{j+t}, \qquad (2)$$

где $\tilde{\alpha}_i^{j+t} = (\alpha_i^j + t\, m_{i+1})(\mathrm{mod}\, m_i)$.

В табл. 1 приведены значения разностей для различных модулей. Поскольку значения разностей одинаковы на интервалах, длина которых $m_4 = 7$, табл. 1 можно сжать, оставив для каждого интервала значения разностей

первого числа интервала и исключив неинформативные столбцы значений остатков (табл. 2). На основании (1) табл. 2 также можно сжать, ограничившись значениями $\tilde{\alpha}_1$ для чисел первой половины, причем только для значений $\tilde{\alpha}_1 = 0$ (табл. 3).

Пусть результат деления на 2 есть

$$C = (\gamma_1, \gamma_2, \gamma_3, \gamma_4). \tag{3}$$

Тогда, составив для (3) разности

$$\tilde{\alpha}_2 = (\gamma_2 - \gamma_4)(\mathrm{mod}\, m_2),\ \tilde{\alpha}_3 = (\gamma_3 - \gamma_4)(\mathrm{mod}\, m_3), \tag{4}$$

определим, совпадает ли (4) с одной из строк табл. 3. В случае совпадения

Таблица 1

Модуль	$m_1 = 2$	$m_2 = 3$	$m_3 = 5$	$m_4 = 7$	Разность		
A^j	α_1	α_2	α_3	α_4	$\tilde{\alpha}_1 = (\alpha_1 - \alpha_4)(\mathrm{mod}\, m_1)$	$\tilde{\alpha}_2 = (\alpha_2 - \alpha_4)(\mathrm{mod}\, m_2)$	$\tilde{\alpha}_3 = (\alpha_3 - \alpha_4)(\mathrm{mod}\, m_3)$
0	0	0	0	0	0	0	0
1	1	1	1	1	0	0	0
2	0	2	2	2	0	0	0
3	1	0	3	3	0	0	0
4	0	1	4	4	0	0	0
5	1	2	0	5	0	0	0
6	0	0	1	6	0	0	0
7	1	1	2	0	1	1	2
8	0	2	3	1	1	1	2
9	1	0	4	2	1	1	2
10	0	1	0	3	1	1	2
11	1	2	1	4	1	1	2
12	0	0	2	5	1	1	2
13	1	1	3	6	1	1	2
. . . . .							
196	0	1	1	0	0	1	1
197	1	2	2	1	0	1	1
198	0	0	3	2	0	1	1
199	1	1	4	3	0	1	1
200	0	2	0	4	0	1	1
201	1	0	1	5	0	1	1
202	0	1	2	6	0	1	1
203	1	2	3	0	1	2	3
204	0	0	4	1	1	2	3
205	1	1	0	2	1	2	3
206	0	2	1	3	1	2	3

$\tilde{\alpha}_1 = 0$, в случае несовпадения $\tilde{\alpha}_1 = 1$, а искомое значение γ_1 определяется из выражения

$$(\gamma_1 - \gamma_4)(\mathrm{mod}\, m_1) = \tilde{\alpha}_1. \qquad (5)$$

Пример 1. Пусть в СОК с модулями $m_1 = 2$, $m_2 = 3$, $m_3 = 5$, $m_4 = 7$ делимое $N_1 = 134 = (0,2,4,1)$, делитель $N_2 = 2 = (0,2,2,2)$. Результат формального деления:

$$C = (\gamma_1 = 0/0,\ \gamma_2 = 1,\ \gamma_3 = 2,\ \gamma_4 = 4). \qquad (6)$$

Составляем разности:

$$\tilde{\alpha}_2 = (\gamma_2 - \gamma_4)(\mathrm{mod}\, m_2) = (1-4)(\mathrm{mod}\, m_2) = 0,$$
$$\tilde{\alpha}_3 = (\gamma_3 - \gamma_4)(\mathrm{mod}\, m_3) = (2-4)(\mathrm{mod}\, m_3) = 3.$$

Поскольку набор $\tilde{\alpha}_2 = 0, \tilde{\alpha}_3 = 3$ не входит в табл. 3, согласно (5) $\tilde{\alpha}_1 = 1$ и $(\gamma_1 - 4)(\mathrm{mod}\, m_1) = 1$. Отсюда $\gamma_1 = (1+4)(\mathrm{mod}\, m_1) = 1$. Таким образом, результат деления: $C = 67 = (1, 1, 2, 4)$. Число строк в табл. 3 находим из выражения

$$K = \frac{(M/(m_1 m_n)) + 1}{2} = \frac{m_2 \ldots m_{n-1} + 1}{2}. \qquad (7)$$

Таблица 2

Модуль	Разность			Модуль	Разность			Модуль	Разность		
A^j	$\tilde{\alpha}_1$	$\tilde{\alpha}_2$	$\tilde{\alpha}_3$	A^j	$\tilde{\alpha}_1$	$\tilde{\alpha}_2$	$\tilde{\alpha}_3$	A^j	$\tilde{\alpha}_1$	$\tilde{\alpha}_2$	$\tilde{\alpha}_3$
0	0	0	0	70	0	1	0	140	0	2	0
7	1	1	2	77	1	2	2	147	1	0	2
14	0	2	4	84	0	0	4	154	0	1	4
21	1	0	1	91	1	1	1	161	1	2	1
28	0	1	3	98	0	2	3	168	0	0	3
35	1	2	0	105	1	0	0	175	1	1	0
42	0	0	2	112	0	1	2	182	0	2	2
49	1	1	4	119	1	2	4	189	1	0	4
56	0	2	1	126	0	0	1	196	0	1	1
63	1	0	3	133	1	1	3	203	1	2	3

Таблица 3

Модуль	Разность		
A^j	$\tilde{\alpha}_1$	$\tilde{\alpha}_2$	$\tilde{\alpha}_3$
0	0	0	0
14	0	2	4
28	0	1	3
42	0	0	2
56	0	2	1
70	0	1	0
84	0	0	4
98	0	2	3

Таблица 4

mod = 3		mod = 5	
Остаток	Константа	Остаток	Константа
0	0	0	0
1	2	1	4
2	1	2	3
		3	2
		4	1

Как видно из (7), пользоваться табл. 3 при решении практических задач нецелесообразно, так как потребуется большой объем памяти для сохранения такой таблицы. В связи с этим предлагается следующий способ определения $\tilde{\alpha}_1$.

Поскольку строки в табл. 3 представляют собой значения разностей первого числа интервала, а эти числа в соответствии с (2) кратны $t\, m_{i+1}$ 1 (в примере кратны 2 m_4 = 14), разделим число каждой строки $A^j = (\tilde{\alpha}_2, \tilde{\alpha}_3)$ табл. 3 на S = 14 = (2, 4). При этом для каждого набора модулей число S является константой, поэтому операцию деления можно заменить операцией выборки констант из соответствующей таблицы. Для данного набора модулей выборка проводится из табл. 4. В результате табл. 3 преобразуется в табл. 5, строки которой принадлежат первой половине диапазона $\lfloor 0, M^1)$, где $M^1 = m_2 m_3$.

Таким образом, для определения остатка γ_1 в (6) необходимо число $D = (\gamma_2, \gamma_3)$ разделить на константу S и определить, относится ли частное $T = \frac{D}{S} = \left(\frac{\gamma_2}{s_2}, \frac{\gamma_3}{s_2}\right)$ к первой половине диапазона л0, M^1). При нечетной системе модулей Т — число первой половины, если $0 \le T \le \frac{M^1 - 1}{2}$, и Т — число второй половины, если $\frac{M^1 - 1}{2} + 1 \le T < M^1$. При выполнении этого условия $\tilde{\alpha}_1$= 0, при невыполнении — $\tilde{\alpha}_1$= 1, а искомое значение γ_1 определяется из выражения (5). При этом определение принадлежности числа T данной половине диапазона осуществляется следующим образом.

На каждой итерации, начиная с первой, определяется принадлежность испытуемого числа данной половине. На первой итерации такое определение однозначно. На очередной итерации рассчитывается значение приведенного остатка, по которому определяется принадлежность испытуемого числа данной половине, и этот результат запоминается в качестве результата всей операции. Расчет выполняется путем вычитания из приведенных остатков предыдущей итерации констант, выбираемых из таблиц. Если полученное значение приведенного остатка не дает однозначного результата, в качестве результата всей операции сохраняется результат предыдущей итерации.

Пример 2. Пусть для той же СОК с модулями m_1= 2, m_2= 3, m_3 = 5, m_4= 7 делимое N_1=140=(0,2,0,0), делитель N_2 = 2 = (0,2,2,2). Результат формального деления:

$$C = \left(\gamma_1 = \frac{0}{0},\ \gamma_2 = 1,\ \gamma_3 = 0,\ \gamma_4 = 0\right).$$

Таблица 5

Модуль	m_2= 3	m_3= 5
A^j	$\tilde{\alpha}_2$	$\tilde{\alpha}_3$
0	0	0
1	1	1
2	2	2
3	0	3
4	1	4
5	2	0
6	0	1
7	1	2

Таблица 6

Модуль			
m_2= 3		m_3= 5	
π_2	$\tilde{\alpha}_2$	π_3	$\tilde{\alpha}_3$
0	0	0	0
$\pi_2^{R1} = 1$	$\tilde{\alpha}_2^{R1} = 1$	1	3
$\pi_2^{R2} = 2$	$\tilde{\alpha}_2^{R2} = 2$	$\pi_3^0 = 2$	$\tilde{\alpha}_3^0 = 1$
		3	4
		4	2

Таблица 7

Остаток	Константа
m_2= 3	m_3= 5
0	0
1	1
2	2

Составляем разности:

$$\widetilde{\alpha}_2 = (\gamma_2 - \gamma_4)\,(\mathrm{mod}\, m_2) = (1-0)\,(\mathrm{mod}\, m_2) = 1,$$

$$\widetilde{\alpha}_3 = (\gamma_3 - \gamma_4)\,(\mathrm{mod}\, m_3) = (0-0)\,(\mathrm{mod}\, m_3) = 0.$$

Делим $A^j = (\widetilde{\alpha}_2, \widetilde{\alpha}_3)$ на $S = (s_2, s_3)$, т. е. $A^j = (1,0)$ на $S = (2,4)$. Получаем $T = (2,0)$.

В соответствии с (4) по значению остатка $\widetilde{\alpha}_2 = 2$ из табл. 6 определяем, что после данной итерации число T принадлежит второй половине диапазона. На следующей итерации для $\widetilde{\alpha}_2 = 1$ из табл. 7 выбираем константу, равную 2, для вычитания из остатка числа T по модулю $m_3 = 5$. Получаем $\widetilde{\alpha}_3 = 3$. По табл. 6 для $\widetilde{\alpha}_3 = 3$ определяем, что T принадлежит первой половине диапазона.Отсюда следует $\widetilde{\alpha}_1 = 0$, и в соответствии с (5) $(\gamma_1 - 4)\,(\mathrm{mod}\, m_1) = 0$. Тогда, $\gamma_1 = (1+ + 4)\,(\mathrm{mod}\, m_1) = 0$. Результат деления $N_1 = 140 =$ (0,2,0,0) на $N_2 = 2 =$ (0,2,2,2) составляет C = = (0, 1, 0, 0) = 70.

Таким образом, метод эффективного решения задачи деления на два чисел, представленных в системе остаточных классов, основан на определении остатка частного по данному модулю исходя из полученных остатков частного по остальным модулям системы при условии принадлежности частного первой половине диапазона. В процессе решения основной задачи решены также задачи разбиения диапазона чисел на интервалы, расширения диапазона чисел, определения принадлежности числа данной половине, построения таблиц выборки констант. Результаты проведенных исследований могут быть использованы для разработки патентноспособных несложных при схемной реализации вычислительных структур.

Solving problem is produced for division even numbers by two in residual class system. The solving method is based on the quotient residue definition to the given modulus on the basis of received quotient residues to the rest systems' modulus on condition that quotient belongs to the first half of range. The solving of some another problems are considered for the residual class system in the process of the main problem decision. These are: the division of the numbers range to the intervals, the number range extension, the definition of the number belonging to given half of range, the building of constants sampling tables which is necessary to receive of result.

1. *Краснобаев В. А.* Методы сравнения чисел, представленных кодом системы остаточных классов // Электрон. моделирование. Радиотехника: Всеукр. межведомств. науч.-техн. сб. — 1988. — **10**, № 2. — С. 84—87.
2. *Акушский И. Я., Юдицкий Д. И.* Машинная арифметика в остаточных классах. — М. : Советское радио, 1968. — 440 с.
3. *Червяков Н. И.* Методы и принципы построения модулярных нейрокомпьютеров. Сайт http://www.computer-museum.ru/, 2005.
4. *Полисский Ю.Д.* О выполнении сложных операций в системе остаточных классов // Электрон. моделирование. — 2006. — **28**, № 3. — С. 117—123.

Поступила 23.01.07;
после доработки 04.02.08

ПОЛИССКИЙ Юрий Давидович, канд. техн. наук. В 1960 г. окончил Днепропетровский металлургический ин-т. Область научных исследований — системы и средства управления.