УДК 681.04

Ю.Д.Полисский

ДЕЛЕНИЕ ЧИСЕЛ В СИСТЕМЕ ОСТАТОЧНЫХ КЛАССОВ НА ДВА

Введение. Проблема повышения производительности вычислительных структур и надежности вычислений может быть эффективно решена на основе представления 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. Несколько сложнее обстоят дела при реализации немодульных операций, требующих знания всего числа в целом. К таким операциям относится, в частности, операции деления числа на два.

Постановка задачи. При изложении статьи будем использовать определения и обозначения, приведенные в [4]. Таким образом, СОК называется система счисления, в которой произвольное число N представляется в виде набора наименьших неотрицательных остатков по модулям $m_1, m_2, \ldots, m_n$, т.е.

$$N = [N \,(\mathrm{mod}\; m_1), N\,(\mathrm{mod}\; m_2), \ldots N\,(\mathrm{mod}\; m_n)]$$

или

$$N = (б_1, б_2, \ldots, б_n) \tag{1}$$

Здесь $б_i = N\,(\mathrm{mod}\; m_i)$. При этом, если числа m_i взаимно простые, то представление числа N в виде (1) является единственным, а объем диапазона $[0, M)$ представимых чисел в этом случае равен

$$M = m_1 m_2 \ldots m_n \tag{2}$$

Пусть $m_n = 2$. Будем отличать числа первой $R1$ и второй $R2$ половины диапазона.

$$N \in \begin{cases} R1,\, 0 \le N < \dfrac{M}{2}, \\ R2,\, \dfrac{M}{2} \le N < M. \end{cases} \tag{3}$$

Пусть в системе с основаниями $m_1, m_2, \ldots, m_n = 2$ даны два числа $N_1 = (б_1, б_2, \ldots, б_n)$ и $N_2 = 2 = (в_1, в_2, \ldots, в_n)$ и пусть $E_1 = (е_1, е_2, \ldots, е_n)$ –

частное от деления N_1 на N_2. Тогда, если деление точно выполнимо, т.е. N_1 кратно N_2, то

$$E \in R1 \tag{4}$$

$$\varepsilon_i = \left(\frac{\alpha_i}{\beta_i}\right)(\mathrm{mod}\ m_i) \tag{5}$$

Тогда все остатки частного, кроме остатка по модулю m_n, определяются формальным делением остатков $б_i$ на остатки $в_i$. Для модуля m_n имеем неопределенность 0/0, которую требуется раскрыть.

Основная часть. Решение поставленной задачи связано с определением принадлежности числа данной половине диапазона. Пусть системой оснований полиадического кода также является система $m_1, m_2, \ldots, m_n = 2$. Тогда число E в полиадическом коде представляется следующим образом

$$E = р_1 + р_2 m_1 + р_3 m_1 m_2 + \ldots + р_i m_1 m_2 \ldots m_{i-1} + р_{n-1} m_1 m_2 \ldots m_{n-2} + р_n m_1 m_2 \ldots m_{n-1}, \tag{6}$$

где $р_i$ - позиционная характеристика числа по модулю m_i, $0 < р_i \le m_i - 1$.

Пусть $E_1 = р_1 + р_2 m_1 + р_3 m_1 m_2 + \ldots + р_i m_1 m_2 \ldots m_{i-1} + р_{n-1} m_1 m_2 \ldots m_{n-2}$.

Число $0 \le р_1 + р_2 m_1 + р_3 m_1 m_2 + \ldots + р_i m_1 m_2 \ldots m_{i-1} + р_{n-1} m_1 m_2 \ldots m_{n-2} < \frac{M}{2}$, т.е. является числом первой половины. Поэтому отношение числа E к первой или второй половине диапазона определяется значением $р_n$, т.е.

$$р_n = \begin{cases} 0, E \in R1, \\ 1, E \in R2. \end{cases} \tag{7}$$

Задача определения принадлежности числа данной половине диапазона сводится, таким образом, к нахождению $р_n$. В [4] предложен простой метод определения принадлежности числа данной половине, основанный на приведении итеративным путем числа E к нижней границе своей половины диапазона, при котором на i-ой итерации определяется приведенный остаток $\tilde{е}_i = р_i m_1 m_2 \ldots m_{i-1} (\mathrm{mod}\, m_i)$ и рассчитывается $E^i = E^{i-1} - \Delta^i$, где $\Delta^i = р_i m_1 m_2 \ldots m_{i-1}$. Поскольку $\tilde{е}_n = р_n m_1 m_2 \ldots m_{n-1} (\mathrm{mod}\, m_n)$, а все модули $m_1, m_2, \ldots, m_n$ нечетные, то $\tilde{е}_n = р_n$. Поэтому условие (7) сводится к определению значения приведенного остатка $\tilde{е}_n$ после выполнения n – ой итерации, т.е.

 ISSN 1562-9945

$$\widetilde{e}_n = \begin{cases} 0, E \in R1, \\ 1, E \in R2. \end{cases} \qquad (8)$$

При этом в соответствии с [4] значения $\widetilde{e}_i$ на i-ой итерации определяются на основании значений $\widetilde{e}_{i-1}$ путем вычитания определенных констант, получаемых простой выборкой из таблиц, предварительно построенных для принятой системы модулей и их упорядоченности. Тогда на каждой итерации выполняется только операция вычитания для все сокращающегося количества модулей.

В результате метод деления на 2 сводится к следующему. После выполнения формального деления и получения значений $\widetilde{e}_1, \widetilde{e}_2, \ldots, \widetilde{e}_{n-1}$ принимаем в качестве остатка e_n по модулю m_n значение, например, $e_n = 0$. Затем описанным выше итеративным путем находим $\widetilde{e}_n$. Поскольку в соответствии с (4) $E \in R1$, полученное значение $\widetilde{e}_n$ должно (8) равняться 0. Если такое условие выполнено, то результатом деления является число $E = (\widetilde{e}_1, \widetilde{e}_2, \ldots, \widetilde{e}_{n-1}, 0)$, в противном случае $E = (\widetilde{e}_1, \widetilde{e}_2, \ldots, \widetilde{e}_{n-1}, 1)$.

Проиллюстрируем изложенное на примере для системы модулей $m_1 = 5$, $m_2 = 7$, $m_3 = 3$, $m_4 = 11$, $m_5 = 2$. Диапазон чисел 0 ÷ 2309. Делимое N_1 = 1846 = (1, 5, 1, 9, 0), делитель N_2 = 2 = (2, 2, 2, 2, 0).

Результат формального деления

$$E = (e_1 = 3, e_2 = 6, e_3 = 2, e_4 = 10, e_5 = 0/0)$$

Принимаем значение $e_5 = 0$.

На первой итерации для $\widetilde{e}_1 = 3$ выбираем из табл.1 $\Delta^1{}_2 = 3, \Delta^1{}_3 = 0, \Delta^1{}_4 = 3, \Delta^1{}_5 = 1$ и получаем E^1 = (0, 3, 2, 7, 1).

На второй итерации для $\widetilde{e}_2 = 3$ выбираем из табл.2 $\Delta^2{}_3 = 1, \Delta^2{}_4 = 10, \Delta^2{}_5 = 0$ и получаем E^2 = (0, 0, 1, 8, 1).

На третьей итерации для $\widetilde{e}_3 = 1$ выбираем из табл.3 $\Delta^3{}_4 = 4, \Delta^3{}_5 = 0$ и получаем E^3 = (0, 0, 0, 4, 1).

Таблица 1

Остатки для mod	Константы для mod			
$m_1 = 5$	$m_2 = 7$	$m_3 = 3$	$m_4 = 11$	$m_5 = 2$
0	0	0	0	0
1	1	1	1	1
2	2	2	2	0
3	3	0	3	1
4	4	1	4	0

Таблица 2

Остатки для mod	Константы для mod		
$m_2 = 7$	$m_3 = 3$	$m_4 = 11$	$m_5 = 2$
0	0	0	0
1	0	4	1
2	0	8	0
3	1	10	0
4	1	3	1
5	2	5	1
6	2	9	0

Таблица 3

Остатки для mod	Константы для mod	
$m_3 = 3$	$m_4 = 11$	$m_5 = 2$
0	0	0
2	2	1
1	4	0

На четвертой итерации для $\tilde{e}_4 = 4$ выбираем из табл.4 $\Delta^4{}_5 = 0$ и получаем $E^4 = (0, 0, 0, 0, 1)$.

Поскольку $\tilde{e}_5 = 1$, то в соответствии с (8) результат деления должен принадлежать второй половине диапазона. Однако по (4) результат деления на 2 относится к первой половине диапазона. Поэтому действительное значение $e_5 = 1$.

Следовательно, результат деления $E = 923 = (3, 6, 2, 10, 1)$.

 ISSN 1562-9945

Структурная схема устройства для выполнения операции деления по данному методу представлена на рисунке.

Таблица 3

Остатки для mod $m_4 = 11$	Константы для mod $m_5 = 2$
0	0
1	0
2	0
3	0
4	0
5	0
6	1
7	1
8	1
9	1
10	1

Таким образом, рассмотрено решение задачи деления на два числа, представленного в системе остаточных классов. Метод решения базируется на определении приведенного остатка по модулю 2 на основе полученных приведенных остатков частного по остальным модулям системы. Такое определение выполняют последовательным вычитанием констант из полученных приведенных остатков частного. При этом константы на каждой итерации выбираются в зависимости от значения остатка, полученного на предыдущей итерации. Предложенный метод имеет высокое быстродействие и позволяет повысить эффективность функционирования вычислительных структур, работающих в системе остаточных классов.

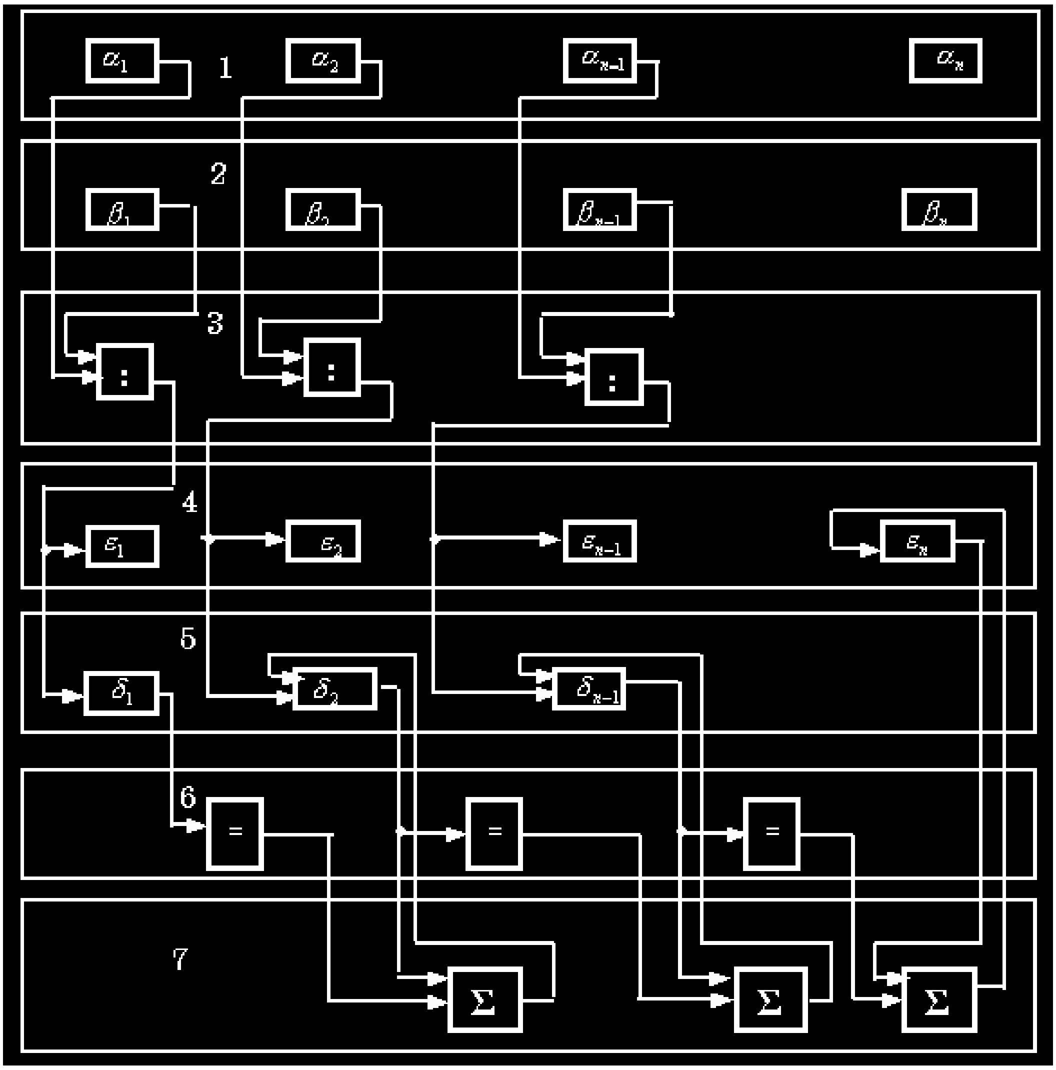

Рисунок 1 - Структурная схема устройства для выполнения операции деления: 1.Регистр делимого; 2.Регистр делителя; 3. Блок модульных делителей; 4.Регистр частного; 5.Блок промежуточных результатов; 6.Блок выбора констант; 7.Блок модульных сумматоров

ЛИТЕРАТУРА

1. Акушский И.Я., Юдицкий Д.И. Машинная арифметика в остаточных классах. - М.: Советское радио, 1968. - 440 с.
2. Кнут Д. Искусство программирования, Т.2. Получисленные алгоритмы. – М.:Вильянс, 2001. – 832 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// Электронное моделирование. – 2006.- Т.28. - №3. – С.117-123.

Получено 18.01.07 г.

 ISSN 1562-9945