УДК 681.3

Н.И. Червяков, И.Н. Лавриненко,
С.В. Лавриненко, О.С. Мезенцева

МЕТОДЫ И АЛГОРИТМЫ ОКРУГЛЕНИЯ, МАСШТАБИРОВАНИЯ И ДЕЛЕНИЯ ЧИСЕЛ В МОДУЛЯРНОЙ АРИФМЕТИКЕ

(Ставропольский военный институт связи ракетных войск)

Рассмотрены методы и алгоритмы деления числа в модулярном коде на одно из оснований или их произведение. Разработан метод деления числа в модулярном коде при произвольных значениях делимого и делителя.

В связи с тем, что модулярная арифметика целочисленная, то при вычислениях промежуточные значения операндов могут переполнять динамический диапазон. Подобная проблема может возникнуть и в традиционных компьютерах, если они оперируют с целыми числами. Во избежание переполнения надо промасштабировать (уменьшить) значения операндов. Промасштабированные величины затем используются в следующих итерациях. Это означает, что операция масштабирования должна применяться к данным с использованием заранее заданной константы, которая округляется до ближайшего целого. Все эти операции связаны с операцией деления.

В данной работе рассмотрим проблемы округления, масштабирования и деления в СОК. Поскольку СОК не является взвешенной системой счисления, операция деления, которая включает сравнение по величине двух операндов, не может считаться простой.

Деление в модулярной арифметике относится к немодульным операциям и является одной из важнейших операций в модулярной компьютерной арифметике, так как лежит в основе многих других операций и входит в состав операций вычислительных алгоритмов.

Операцию деления в СОК можно отнести к одной из трех различных форм [1, 2]:

1. Деление с нулевым остатком.
2. Округление и масштабирование.
3. Основное деление.

Рассмотрим все основные формы модулярного деления.

Деление с нулевым остатком

Для этой формы деления известно, что делимое представляет собой целое число, кратное делителю, а также известно, что делитель и P являются взаимно простыми. Эта категория имеет ограниченную область использования, поскольку должно быть известно априори, удовлетворены ли условия, необходимые для осуществления операции. Для этого алгоритма используется следующая теорема 1.

Теорема 1

Если a делится на b без остатка и наибольший общий делитель (НОД) величин a и b равен 1, то

$$\left|\frac{a}{b}\right|_{p_i} = \left|\frac{1}{b}a\right|_{p_i} \qquad (1)$$

для всех p_i, где $\left|\frac{1}{b}\right|_{p_i}$ – мультипликативная обратная к b величина, взятая по модулю p_i.

Доказательство.

Предположим, что необходимые два условия удовлетворены, тогда a/b это целое число, представленное в остатках имеет вид

$$\left(\left|\frac{a}{b}\right|_{p_1}, \left|\frac{a}{b}\right|_{p_2}, \mathbf{K}, \left|\frac{a}{b}\right|_{p_n}\right). \qquad (2)$$

Выполним вычисление $\frac{a}{b}\cdot a$ в остаточном коде:

$$\left|\frac{a}{b}\right|_P \leftrightarrow \left\{\left|\frac{a}{b}\right|_{p_1}, \left|\frac{a}{b}\right|_{p_2}, \mathbf{K}, \left|\frac{a}{b}\right|_{p_n}\right\} \tag{3}$$

или

$$\frac{|b|_P}{\left|\frac{a}{b}\cdot b\right|_P} \leftrightarrow \frac{\{|b|_{p_1}, |b|_{p_2}, \mathbf{K}, |b|_{p_n}\}}{\left\{\left|\left|\frac{a}{b}\right|_{p_1}|b|_{p_1}\right|_{p_1}, \left|\left|\frac{a}{b}\right|_{p_2}|b|_{p_2}\right|_{p_2}, \mathbf{K}, \left|\left|\frac{a}{b}\right|_{p_n}|b|_{p_n}\right|_{p_n}\right\}}. \tag{4}$$

Так как $\left|\frac{a}{b}\cdot b\right|_P = |a|_P$, следовательно

$$\left|\left|\frac{a}{b}\right|_{p_i}|b|_{p_i}\right| = |a|_{p_i}. \tag{5}$$

По уникальности мультипликативной инверсии следует, что

$$\left|\frac{a}{b}\right|_{p_i} = \left|\frac{1}{b}a\right|_{p_i}.$$

Если b не делит a, то величина $\frac{a}{b}$ не является целой и выражение $\left|\frac{a}{b}\right|_{p_i}$ не определено. Следовательно, (1) не имеет смысла.

Пример 1. Деление с нулевым остатком.

Для модулей p_1=29, p_2=32 и p_3=31 разделим число 1872 на 9.

Решение. Остаточное представление 1872 – это (16, 16, 12). Остаточное представление 9 это – (9, 9, 9), тогда для 1872/9=208 остаточный код

$$\left\{16\cdot\left|\frac{1}{9}\right|_{29}, 16\cdot\left|\frac{1}{9}\right|_{32}, 12\cdot\left|\frac{1}{9}\right|_{31}\right\} = (5,16,22) \leftrightarrow 208.$$

С другой стороны, если мы делим 1873 на 9 (1873 не делится на 9 без остатка), то получим

$1873 \leftrightarrow (17,17,13)\cdot(13,25,7) = (18,9,29) \leftrightarrow 6601$, что абсолютно неправильно.

Масштабирование целых положительных чисел

При делении этой формы делимое является произвольным, а делителем может быть любой сомножитель P, представляющий собой произведение первых степеней некоторых модулей. Это деление аналогично делению на степень числа 2 в двоичной арифметике в том смысле, что деление на числа, принадлежащие определенному ограниченному множеству, выполняется быстрее, чем деление на произвольный делитель. Деление в любой целочисленной системе счисления определяется формулой $a = \left[\frac{a}{b}\right]\cdot b + |a|_b$, где a представляет собой делимое, b – делитель, $\left[\frac{a}{b}\right]$ – целая часть отношения a к b (частное), а $|a|_b$ – остаток (наименьший целый положительный остаток). Целью алгоритма масштабирования является нахождение $\left[\frac{a}{b}\right]$ для значений b из ограниченной области. Заметим, что $\left[\frac{a}{b}\right] = \frac{a-|a|_b}{b}$. Следовательно, в системе вычетов $\left[\frac{a}{b}\right]$ представляется величинами $\left(\left|\frac{a-|a|_b}{b}\right|_{p_1}, \left|\frac{a-|a|_b}{b}\right|_{p_2}, \mathbf{K}, \left|\frac{a-|a|_b}{b}\right|_{p_n}\right)$, где $\left|\frac{a-|a|_b}{b}\right|_{p_i}$ принимают целые значения. Если b совпадает с одним из p_i или является произведением первых степеней некоторых модулей p_i, то $|a|_b$ можно найти. Тогда по теореме, используемой в форме деления с нулевым остатком, для всех i, для которых НОД величин p_i и b равен 1, можно получить

$$\left|\frac{a-|a|_b}{b}\right|_{p_i} = \left[\frac{a}{b}\right]_{p_i} = \left|\frac{1}{b}\cdot\left(a-|a|_b\right)\right|_{p_i}. \qquad (6)$$

Это уравнение задает цифры системы вычетов для $\left[\frac{a}{b}\right]$ для всех таких цифр, что НОД величин p_i и b равен 1. Остальные цифры

могут быть найдены с помощью метода расширения базы. Таким образом, алгоритм масштабирования состоит из двух этапов:

1. Деление с нулевым остатком.

2. Расширение базы.

Процесс масштабирования покажем числовым примером.

Пример 2. Масштабирование положительного числа единичным модулем.

Для модулей p_1=2, p_2=3, p_3=5 и p_4=7 определим остаточное представление значения целого числа $\left[\frac{a}{5}\right]$. Пусть a имеет остаточный код $(1, 2, 4, 3) \leftrightarrow 59$. В качестве делителя используется модуль p_3.

Решение. Сначала определим остаточное представление числа, которое делится на 5 и является ближайшим целым к a, не превышающим a, то есть $a - |a|_5$. Это можно найти путем вычитания остатка a по модулю 5.

Модули	2	3	5	7	
	$59 \leftrightarrow (1,$	2,	4,	3)	
Вычитаем $\|a\|_5 = 4 \leftrightarrow$	(0	1,	4,	4)	
	(1, 1, 0, 6)				$\leftrightarrow a - \|a\|_5$

Результат делится на 5 кроме модуля p_3, который сам является делителем. Все модули простые по отношению к делителю. Применяем метод деления с нулевым остатком, при этом остаточную цифру по модулю 5 временно игнорируем.

Умножаем на $\left\|\frac{1}{5}\right\|_{p_i}$	$a - \|a\|_5$	$\leftrightarrow$	(1, 1, –, 6)		
		$\leftrightarrow$	(1, 2, –, 3)	2,3,7 $\leftrightarrow$	$\frac{a - \|a\|_5}{5}$
			(1, 2, –, 4)		

Исходный интервал определения для всего набора модулей был равен [0-209], а $\frac{a - |a|_5}{5}$ оказался в интервале [0-41], поэтому оста-

точное представление (1, 2, –, 4) не ясно. Остаток по модулю 5 может быть найден путем расширения базы. Это можно сделать по методу Гарнера или предложенному методу в работе [3]. Для этого остаток по модулю 5 примем за 0 в первом случае и за $|a|_5$ – во втором.

Расширение базы:

на основе известного метода Гарнера	на основе предложенного метода

на основе известного метода Гарнера

Номер операции	Модули	2,	3,	5,	7
	a -$\|a\|_5$ $\leftrightarrow$	(1,	2,	0,	4)
1.	Вычитаем 1	(1,	1,	1,	1)
		(0,	1,	4,	3)
2.	Умножаем на $\left\|\frac{1}{2}\right\|_{p_i}$	(-,	2,	3,	4)
		(-,	2,	2,	5)
3.	Вычитаем 2	(-,	2,	2,	2)
		(-,	0,	0,	3)
4.	Умножаем на $\left\|\frac{1}{3}\right\|_{p_i}$	(-,	-,	2,	5)
		(-,	-,	0,	1)
5.	Вычитаем 1	(-,	-,	1,	1)
		(-,	-,	4,	0)

Если $\left[\frac{a}{5}\right]$ обозначить как z_5, тогда получим $|z_5|+4=0$, отсюда

6. $|z_5|=-4 \bmod 5 = 1 \bmod 5$.

Итак $\left[\frac{a}{5}\right]=(1,\ 2,\ 1,\ 4) \leftrightarrow 11.$

на основе предложенного метода

Матрица констант для набора с измененным порядком модулей

2,	3,	5,	7
1	1	3	2
0	2	4	2
0	0	6	2
0	0	0	3

1. Умножение

1·	1	1	3	2	$\rightarrow$	1	1	3	2
2·	0	2	4	2	$\rightarrow$	0	2	4	2
4·	0	0	6	2	$\rightarrow$	0	0	6	2
$\|a\|_5$·	0	0	0	3	$\rightarrow$	0	0	0	$3\|a\|_5$

2. Сложение $\quad (1,\ 2,\ 1,\ 17+3|a|_5)$

3. Вычисление остатка по mod 5

$17+3|a|_5=0$

Или $|a|_5=-17\left|\frac{1}{3}\right|_5 \bmod 5 \equiv$

$\equiv -34 \bmod 5 \equiv -4 \bmod 5 \equiv 1 \bmod 5$.

Итак $\left[\frac{a}{5}\right]=(1,\ 2,\ 1,\ 4) \leftrightarrow 11.$

В методе Гарнера для замены вычитания сложением необходимо использовать дополнительный код, при этом для вычитания необ-

ходимо две операции. Выигрыш предложенного метода оценивается как $\frac{3(n-1)}{3} = n-1$.

Пример 3. Масштабирование положительного числа несколькими модулями.

В примере 2 коэффициентом масштабирования был только один модуль. В этом примере коэффициентом масштабирования будет произведение двух модулей, а именно $3 \times 5 = 15$. Вначале делим на 3 и полученное частное является новым делимым для делителя, равного 5, деление на 5 выдает значения целого числа частного. Для завершения операции масштабирования необходимо выполнить операцию расширения базы. Изменение последовательности деления сначала выполнить деление на 5, а затем на 3 не меняет результата.

Для модулей p_1=2, p_2=3, p_3=5 и p_4=7 число a=89 $\leftrightarrow$(1, 2, 4, 5) масштабируем коэффициентом 15. Обозначим результат $\left[\frac{a}{15}\right]$ как z.

Решение.

Модули	2, 3, 5, 7	
Остаточное представление для a	(1, 2, 4, 5)	
Вычитаем $\lvert a\rvert_3 = 2$	(0, 2, 2, 2)	
	(1, 0, 2, 3)	$\overset{2,3,5,7}{\leftrightarrow} \quad a - \lvert a\rvert_3$
Умножаем на $\left\lvert \frac{1}{3} \right\rvert_{P_i}$	(1, –, 2, 5)	
	(1, –, 4, 1)	$\overset{2,\ 5,7}{\leftrightarrow} \ \frac{a - \lvert a\rvert_3}{3}$
Вычитаем $\lvert a\rvert_5 = 4$	(0, –, 4, 4)	
	(1, –, 0, 4)	$\overset{2,\ 3,7}{\leftrightarrow} \ \frac{a - \lvert a\rvert_3}{3} - \lvert a\rvert_5$
Умножаем на $\left\lvert \frac{1}{5} \right\rvert_{P_i}$	(1, –, –, 3)	
	(1, –, –, 5)	

Для расширения базы внесем 0 в пропущенные колонки для метода Гарнера и обозначим как $|a|_3$ и $|a|_5$ – для предложенного метода.

<table>
<tr><th>Метод Гарнера</th><th>Предложенный метод</th></tr>
<tr><td>1. Вычитаем 1 $\begin{array}{r}(1,\ 0,\ 0,\ 5)\\ (1,\ 1,\ 1,\ 1)\\ \hline (0,\ 2,\ 4,\ 4)\end{array}$
2. Умножаем на $\left|\frac{1}{2}\right|_{p_i}$ $\begin{array}{r}(-,\ 2,\ 3,\ 4)\\ (-,\ 1,\ 2,\ 2)\end{array}$
3. Вычитаем 2 $\begin{array}{r}(-,\ 2,\ 2,\ 2)\\ (-,\ 2,\ 0,\ 0)\end{array}$
4. Тогда $\left|\frac{1}{2}|z|_3+2\right|=0$ и $\left|\frac{1}{2}|z|_5+2\right|=0$.
Следовательно, $|z|_3=2$ и $|z|_5=0$.
Отсюда, масштабируемое число $\left[\frac{89}{15}\right]$ это $(1, 2, 0, 5)\leftrightarrow 5$.</td><td>Разобьем матрицу констант для измененной последовательности модулей на 2 матрицы
Модули $\underline{2,\ 7,\ 3}$ $\underline{2,\ 7,\ 5}$
$\begin{vmatrix}1, & 3, & 1\\ 0, & 4, & 2\\ 0, & 0, & 2\end{vmatrix}$ $\begin{vmatrix}1, & 3, & 2\\ 0, & 4, & 1\\ 0, & 0, & 3\end{vmatrix}$
1. Умножаем
$\begin{array}{r}1\cdot\\ 5\cdot\\ |x|_3\cdot\end{array}\begin{vmatrix}1, & 3, & 1\\ 0, & 20, & 10\\ 0, & 0, & 2\cdot|x|_3\end{vmatrix}$; $\begin{array}{r}1\cdot\\ 5\cdot\\ |x|_5\cdot\end{array}\begin{vmatrix}1, & 3, & 2\\ 0, & 20, & 5\\ 0, & 0, & 9\cdot|x|_5\end{vmatrix}$
$\underline{1,\ 2,\ 14+2\cdot|x|_3}$ $\underline{1,\ 2,\ 10+3\cdot|x|_5}$
Отсюда
$14+2\cdot|x|_3=0,$
$|x|_3=-7\bmod 3\equiv 2\bmod 3$
$10+3\cdot|x|_5=0,$
$|x|_5=-10\left|\frac{1}{3}\right|_5\equiv 20\bmod 5\equiv$
$\equiv 0\bmod 5$
$\left[\frac{89}{15}\right]=(1, 2, 0, 5)\leftrightarrow 5$</td></tr>
</table>

Итак, для масштабирования числа большим коэффициентом масштаба используется последовательное деление на простые числа и расширение базы модулей СОК.

Математические модели масштабируемых чисел другого знака

Отрицательные числа в СОК можно записать как $P-a$. Если известно, что число отрицательное, то легко можно его определить из $P-a$, затем проводится масштабирование на b, получаем $\left[\frac{a}{b}\right]$ и затем представляем результаты как P+$\left[\frac{a}{b}\right]$. Если же знак неизвестен, то возникает определенная сложность. При масштабировании отрицательного числа как будто бы число положительное, резуль-

татом будет $\frac{P}{b}+\left[\frac{a}{b}\right]$ вместо необходимого P+$\left[\frac{a}{b}\right]$. Поэтому перед масштабированием необходимо определить знак a, этого процесса можно избежать, если принять во внимание следующее обстоятельство: деление на b отображает все числа в интервале $\left[0,\frac{P}{2}-1\right]$ в интервал $\left[0,\frac{P}{2b}-1\right]$ и все числа в интервале $\left[\frac{P}{2},P-1\right]$ в интервал $\left[\frac{P}{2b},\frac{P-1}{2}\right]$. Отсюда можно выполнить вначале деление числа на b, а затем, принимая во внимание интервал, в котором находится $\left|\left[\frac{a}{b}\right]\right|_P$, определяется знак a. Если a – отрицательное число $\left|-\frac{P}{b}\right|_P$, то к нему прибавляется по модулю P для получения правильного ответа P+$\left[\frac{a}{b}\right]$.

Определение интервала, в котором находится $\left[\frac{a}{b}\right]$ требует такого же количества времени, что и для определения знака числа. Однако, как было рассмотрено в предыдущем примере, процесс масштабирования требует операции расширения базы модулей СОК на основе цифр ОПСС, поэтому можно определить местонахождение числа $\left[\frac{a}{b}\right]$ путем использования цифр ОПСС.

Рассмотрим метод одновременного масштабирования и распознавания знака.

Пример 4. Одновременное масштабирование и определение знака.

Для модулей p_1=13, p_2=9, p_3=11, p_4=7 и p_5=2 масштабируем число $a=-979\leftrightarrow(9,\ 2,\ 0,\ 1,\ 1)$ на число $b=7\cdot11$ с округлением до ближайшего целого числа.

Модули	13, 9, 11, 7, 2	
Остаточное представление числа a	(9, 2, 0, 1, 1)	
Вычитаем 1	(1, 1, 1, 1, 1)	
	(8, 1, 10, 0, 0)	
Умножаем на $\left\|\frac{1}{7}\right\|_{P_I}$	(2, 4, 8, –, 1)	
	(3, 4, 3, –, 0)	
Вычитаем 3	(3, 3, 3, –, 1)	
	(0, 1, 0, –, 1)	
Умножаем на $\left\|\frac{1}{11}\right\|_{P_I}$	(6, 5, –, –, 1)	
	(0, 5, –, –, 1)	$13, 9, 2 \atop \leftrightarrow \left[\frac{P-979}{7\cdot 11}\right]$

Внесем 0 в пропущенные колонки для расширения базы

	(0, 5, 0, 0, 1)
Вычитаем 0	(0, 0, 0, 0, 0)
	(0, 5, 0, 0, 1)
Умножаем на $\left\|\frac{1}{13}\right\|_{P_I}$	(–, 7, 6, 6, 1)
	(–, $\boxed{8}$, 0, 0, 1)
Вычитаем 8	(–, 8, 8, 1, 0)
	(–, 0, 3, 6, 1)
Умножаем на $\left\|\frac{1}{9}\right\|_{P_I}$	(–, –, 5, 4, 1)
	(–, –, 4, 3, $\boxed{1}$)
Вычитаем 1	(–, –, 1, 1, 1)
	(–, –, 3, 2, 0)

Пусть z будет результатом этой операции масштабирования, то есть $z = \left[\frac{P-979}{7\cdot 11}\right]$, тогда:

$$\frac{1}{13}\cdot\frac{1}{9}|z|_{11}+3=0,\ |z|_{11}=1, \qquad \frac{1}{13}\cdot\frac{1}{9}|z|_{7}+2=0,\ |z|_{7}=4.$$

В строку (0, 5, –, –, 1) $\overset{13,9,2}{\leftrightarrow}\left[\frac{P-979}{7\cdot 11}\right]$ добавляем $|z|_{11}$, $|z|_7$, тогда остаточное представление z будет равно (0, 5, 1, 4, 1). В зависимости от знака *a*, остаточное представление z будет либо $\left[\frac{a}{b}\right]$, либо $P+\left[\frac{a}{b}\right]$. Цифры ОПСС для z по модулям 13, 4, 2 были вычислены на протяжении процесса масштабирования и обозначились $\square$ в преобразованиях. Отсюда z можно выразить как $z=1(9\cdot 13)+8(13)+0(1)$.

Если a – положительное число, то $|a|_P$ должно быть в интервале $\left[0,\frac{P/2-1}{77}\right]$ или $[0,(9\cdot 13)-1]$. Так как наиболее значимой цифрой ОПСС $|z|_P$ является 1, то $|z|_P$ не может входить в этот интервал. Отсюда *a* должно быть отрицательным. Следовательно, для получения правильного результата необходимо $\left[-\frac{P}{b}\right]_P$ сложить с $|z|_P$. Для завершения примера необходимо число (0, 0, 8, 4, 0), которое является величиной $\left|-\frac{P}{b}\right|_P$ сложить с числом (0, 5, 1, 4, 1). Результатом является число $z=\left[\frac{-979}{77}\right]=-13$.

Разработка метода и алгоритма основного модулярного деления

Рассмотренные модели связаны со специальными случаями и неприменимы в ситуации, когда и делимое, и делитель представляют собой произвольные целые числа. Последний случай представлен формой 3.

Различные алгоритмы деления целых чисел $\frac{a}{b}$ можно описать итеративной схемой, используемой так называемый метод спуска Ферма [4]. Конструируется некоторое правило j, которое каждой

паре целых положительных чисел a и b ставит в соответствие некоторое целое положительное q такое, что $a-bq=r>0$. Тогда деление a на b осуществляется по следующему правилу: согласно операции j паре чисел a и b ставится в соответствие число q_1, такое, что $a - bq_1 = r_1 \geq 0$. Если $r_1<b$, то деление закончено, если же $r_1 \geq b$, то, согласно j, паре чисел (r_1, b) ставится в соответствие q_2, такое, что $r_1 - bq_1 = r_1 \geq 0$.

Если ($r_2 < b$), то деление завершается, если же ($r_2 \geq b$), то, согласно j_1, паре (r_2, b) ставится в соответствие q_3 такое, что $r_2 - bq_3 = r_3 \geq 0$ и так далее. Так как последовательное применение операции j приводит к строго убывающей последовательности положительных целых чисел $a \geq r_1 > r_2 > r_3 > \mathbf{K} \geq 0$, то процесс является конечным и алгоритм реализуется за конечное число шагов.

В общем случае b может быть и не равным модулю или их произведению. Здесь встает проблема выбора b таким, чтобы оно было равным либо модулю, либо их произведению. Если эта проблема будет решена, тогда итерации могут быть сведены к процессу масштабирования, которые рассмотрены выше. Для решения этой проблемы вначале докажем теорему о границах изменения b.

Теорема. 2. Если на К-шаге зафиксирован случай $0 \leq r_{k-1} - bq_k = r_k < b$, тогда частное q от деления целых чисел a на b будет равно $\sum_{i=1}^{k} q_1 + r_k'$. Если $r_k < \frac{b}{2}$, то $r_k' = 0$, а если $r_k > \frac{b}{2}$, то $r_k' = 1$.

Доказательство. Докажем для случая, если $\bar{b} = l \cdot b$ при $l = 1,2,\mathbf{K}$. Для доказательства выполним следующую последовательность действий:

$$q_1 = \left[\frac{a}{b}\right] = \frac{1}{l}\left[\frac{a}{b}\right] \text{ при } a = a_0$$

$$a_1 = a_0 - bq_1 = a - b\frac{1}{l}\left[\frac{a}{b}\right] = a - a\frac{1}{l} = a\left(1 - \frac{1}{l}\right);$$

$$q_2 = \left[\frac{a_1}{\bar{b}}\right] = \frac{a_1}{l \cdot b} = \frac{a(1-\frac{1}{l})}{l \cdot b} = \left[\frac{a}{b}\right]\frac{1}{l}(1-\frac{1}{l});$$

$$a_2 = a_1 - bq_2 = a\left(1-\frac{1}{l}\right) - b\left[\frac{a}{b}\right]\frac{1}{l}\left(1-\frac{1}{l}\right) = a\left(1-\frac{1}{l}\right) - a\frac{1}{l}\left(1-\frac{1}{l}\right) =$$

$$= a\left(1-\frac{1}{l}\right)\left(a-\frac{1}{l}\right) = a\left(1-\frac{1}{l}\right)^2;$$

$$q_3 = \left[\frac{a_2}{\bar{b}}\right] = \left[\frac{a_{12}}{l\cdot y}\right] = \frac{a(1-\frac{1}{l})^2}{l\cdot b} = \left[\frac{a}{b}\right]\frac{1}{l}(1-\frac{1}{l})^2;$$

$$a_3 = a_2 - bq_3 = a\left(1-\frac{1}{l}\right)^2 - a\left[\frac{a}{b}\right]\frac{1}{l}\left(1-\frac{1}{l}\right)^2 = a\left(1-\frac{1}{l}\right)^2\cdot\left(1-\frac{1}{l}\right) = a\left(1-\frac{1}{l}\right)^3;$$

$$q_4 = \left[\frac{a_3}{\bar{b}}\right] = \frac{a-(1-\frac{1}{l})^3}{l\cdot b} = \frac{a}{b}\frac{1}{l}(1-\frac{1}{l})^3$$

……

$$q_k = \left[\frac{a}{\bar{b}}\right]\cdot\frac{a}{b}\frac{1}{l}(1-\frac{1}{l})^{k-1};\ q_k = \frac{a_{k-1}}{\bar{b}},\ \bar{b} \le l_{k-1}$$

$$q_1 + q_2 + \mathbf{K} + q_k = \left[\frac{a}{b}\right]\cdot\frac{1}{l} + \left[\frac{a}{b}\right]\cdot\frac{1}{l}\cdot\left(1-\frac{1}{l}\right) + \left[\frac{a}{b}\right]\cdot\frac{1}{l}\cdot\left(1-\frac{1}{l}\right)^2 +$$

$$+\left[\frac{a}{b}\right]\cdot\frac{1}{l}\cdot\left(1-\frac{1}{l}\right)^3 + \mathbf{K} + \left[\frac{a}{b}\right]\cdot\frac{1}{l}\cdot\left(1-\frac{1}{l}\right)^{k-1} =$$

$$= \left[\frac{a}{b}\right]\cdot\frac{1}{l}\cdot\left[1+\left(1-\frac{1}{l}\right)+\left(1-\frac{1}{l}\right)^2 + \mathbf{K} + \left(1-\frac{1}{l}\right)^{k-1}\right] =$$

$$= \left[\frac{a}{b}\right]\cdot\left(1-\left(1-\frac{1}{l}\right)^k\right).$$

Итак, $\sum_{i=1}^{k} q_i = \left[\frac{a}{b}\right]\cdot\left(1-\left(1-\frac{1}{l}\right)^k\right)$.

Проведенные расчеты на ЭВМ приведены на графике рисунком 1.

Из рисунка 1 видно, что в качестве делителя лучшие характеристики получаются при $l = 1;2$. При $l = 1$ частное представляет собой точное значение, а при $l = 2$ частное при малом числе итераций приближается к точному ее значению. Таким образом, в качестве делителя выбирается величина $b \le \bar{b} < 2b$.

Заметим, что при $l = 1$ сумма $\sum_{i=1}^{k} q_i = \left[\frac{a}{b}\right] = \frac{a}{b}$. Для вычисления частного с точностью 0.9 и выше значение l целесообразно выбрать равное двум, то есть $b \le \bar{b} < 2b$.

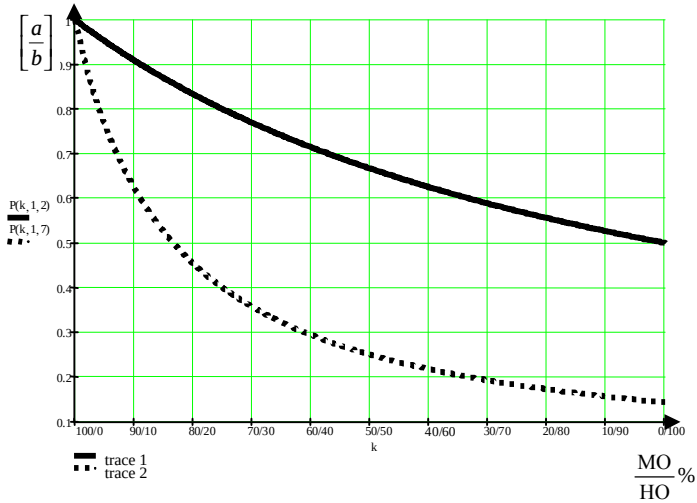

Рисунок 1 – График зависимости значения величины частного от значения величины делителя и числа итераций

Проблема разработки оптимальных вычислительных алгоритмов деления побуждает к разработке таких операций j_1, которые бы минимизировали число шагов спуска Ферма и вместе с тем достаточно просто реализовывались на заданной вычислительной базе. Кроме того, на способ формирования операции j существенно влияет также принятая система кодирования числовой информации. Теперь возникает еще одна проблема, каким образом полученный приблизительный делитель $\bar{b}$ свести либо к величине одного модуля или их произведению?

Предлагается модифицированный модулярный алгоритм деления целых чисел на основе метода спуска Ферма, который направлен на использование деления на приблизительный делитель $\bar{b}$, в предположении, что $\bar{b}$ либо целое положительное число попарно простое с p_1, p_2, $\ldots p_n$, либо целое положительное число, представляющее собой произведение чисел, попарно простых с p_1, p_2, $\ldots p_n$. Этот приблизительный делитель выберем из значения делителя, используемого в применении алгоритма масштабирования. Так как в этом случае b не равно $\bar{b}$ ошибка деления будет представлена в частном, которое при выполнении итерации будет уменьшаться до нуля.

Допустим, что и делимое a и делитель b являются положительными числами, и что значение для $\bar{b}$ найдено в соответствии с условием $b \le \bar{b} < 2b$, где $\bar{b}$ – это допустимый делитель для алгоритма масштабирования. Метод нахождения $\bar{b}$, удовлетворяющий этому условию, рассмотрен выше.

В алгоритме деления первым этапом является этап вычисления частного по алгоритму масштабирования, при котором $q_1 = \left[\frac{a}{b}\right]$. Найденный таким образом q_1 далее используется в рекурсивных соотношениях $a_i = a_{i-1} - bq_i, a_0 = a$ и $q_i = \left[\frac{a_{i-1}}{\bar{b}}\right]$ для получения q_2, q_3 и так далее.

Эта повторяющаяся процедура продолжается до тех пор, пока q_i=0, либо до a_i =0.

Если это возникает на r-ом повторении, то $q = \left[\frac{a}{b}\right] = \sum q_i + q_r'$,

где $q' = \begin{cases} q_r, \text{если } q_r \neq 0 \text{ и } a_r = 0; \\ 1, \text{если } q_r = 0 \text{ и } a_{r-1} \ge b \text{ для любых } \bar{b} \neq b; \\ 0, \text{иначе.} \end{cases}$.

Действительность этого алгоритма зависит от трех предпосылок:

1. Или q_i, или a_i становится нулевым после последнего числа повторений.

2. Ряд $\prod_{i=0}^{r-1} q_i + q'_r$ должен быть равен $\left[\frac{a}{b}\right]$.

3. Для любого b существует подходящий $\bar{b}$. Причем $\bar{b}$ определяется из условия $b \le \bar{b} < 2b$ и удовлетворяющий условию алгоритма масштабирования.

Таблица 1 – Цифры приблизительного делителя

если $b_i = 0$ для $i \neq k$		если $b_i \neq 0$ для $i \neq k$	
b_p	Q	b_p	Q
1	1	1	2
2	2	2	3
3	3	3	5
4	5	4	5
5	5	5	3·2
6	3·2	6	7
7	5·2	7	5·2
8	5·2	8	5·2
9	5·2	9	5·2
10	5·2	10	11
11	11	11	13
12	13	12	13
13	13	13	7·2
14	7·2	14	5·3
15	5·3	15	17
16	17	16	17
17	17	17	19
18	19	18	19
19	19	19	7·3
20	7·3	20	7·3
21	7·3	21	7·3
22	11·2	22	23

Приблизительный делитель $\bar{b}$ можно найти путем использования наиболее значимой ненулевой цифры, представленного $\bar{b}$ в полиадической системе счисления. Эту ненулевую цифру заменим ближайшим простым числом или произведением простых чисел. Тогда делитель $\bar{b}$ можно представить в виде простого числа или произ-

ведения простых чисел, что позволит использовать для вычисления частного алгоритм масштабирования.

Для определения $\bar{b}$ можно составить таблицу 1 приблизительного делителя.

В таблице 1 приведен список допустимых значений $\bar{b}$ для системы модулей 23, 19, 17, 13, 11, 7, 5, 3, и 2.

Если система модулей СОК выбрана иной, то таблицу 1 можно аппроксимировать.

Пример 5. В остаточной системе, состоящей из модулей 23, 19, 17, 13, 11, 7, 5, 3, и 2 (P=223092870) делим a=10304312 на b=1401. Округленное частное $q = \left[\frac{a}{b}\right]$.

Решение. Вначале представим b в обобщенной позиционной системе счисления в порядке уменьшаемой значимости b_9=0, b_8=0, b_7=0, b_6=0, b_5=0, b_4=0, b_3=3, b_2=3, b_1=21, где b_i определяем из уравнения

$$b = b_9(23\cdot 19\cdot 17\cdot 13\cdot 11\cdot 7\cdot 5\cdot 3) + b_8(23\cdot 19\cdot 17\cdot 13\cdot 11\cdot 7\cdot 5) +$$
$$+ b_7(23\cdot 19\cdot 17\cdot 13\cdot 11\cdot 7) + + b_6(23\cdot 19\cdot 17\cdot 13\cdot 11) + b_5(23\cdot 19\cdot 17\cdot 13) +$$
$$+ b_4(23\cdot 19\cdot 17) + b_3(23\cdot 19) + b_2 23 + b_1$$

Используя таблицу 1 с $b_l = b_3$, получаем $\bar{b} = 5\cdot 19\cdot 23 = 2185$, так как b_l является наиболее значимой ненулевой цифрой обобщенной позиционной системы и определяется выражением $\bar{b} = Q\prod_{i=1}^{k-1} p_i$, где Q дано в таблице 1.

Отсюда: $q_1 = \left[\frac{a}{b}\right] = \left[\frac{10304312}{2185}\right] = 4715$;

$a_1 = a_0 - bq_1 = 10304312 - (1401)\cdot(4715) = 3698597$;

$q_2 = \left[\frac{3698597}{2185}\right] = 1692$;

$a_2 = 3698597 - (1401)\cdot(1692) = 1328105$.

Далее получаем остальные значения a_i и q_i

q_3 =607,	a_3 =477698;
q_4 =218,	a_4 =172280;
q_5 =78,	a_5 =63002;
q_6 =28,	a_6 =23774;
q_7 =10,	a_7 =9764;
q_8 =4,	a_8 =4160;
q_9 =1,	a_9 =2759;
q_{10} =1,	a_{10} =1358;
$q_{11}=\left[\frac{1358}{2185}\right]=0$.	

Так как $q_r = 0$ (то есть $q_{11} = 0$), но $a_{r-1} \geq b$, то $q'_r = 0$. Следовательно,

$$q=\sum_{i=1}^{10} q_i = 4715+1692+607+218+78+28+10+4+1=7354.$$

Полученный результат можно легко проверить обычным делением a =10304312 на b =1401. для вычисления округленного частного потребовалось десять итераций, так как числа были выбраны обдуманно, чтобы получилось много операций. Это происходит в тех случаях, если a – большое число, а b – относительно малое число, а $\bar{b}$ – аппроксимация b.

Модифицируем полученный алгоритм на язык кольцевых операций системы остаточных классов. Для этого рассмотрим следующий пример.

Пример 6. В остаточной системе, состоящей из модулей 7, 5, 3, 2 необходимо разделить число a =201 $\rightarrow$ (5, 1, 0, 1) на число b =8 $\rightarrow$ (1, 3, 2, 0). Округленное частное обозначим как $q=[a/b]$.

Решение. Вначале преобразуем делитель b в ОПСС в порядке уменьшаемой значимости:

$b = b_4(7\cdot 5\cdot 3)+b_3(7\cdot 5)+b_2 7+b_1$, тогда $b = 0\cdot(7\cdot 5\cdot 3)+0\cdot(7\cdot 5)+1\cdot 7+1$, где $b_2 = 1, b_1 = 1$.

Используя таблицу 1 с $b_p = b_2$ и $b_i \neq 0$ для $i \neq p$, получим $\bar{b} = Q\prod_{i=1}^{p-1} p_i$, где $Q = 2$ или $\bar{b} = 2 \cdot 7$.

Далее по алгоритму масштабирования, изложенному выше находим $q_1 = \left[\frac{a}{b}\right]$, где $\bar{b}$ – это произведение двух модулей $7 \cdot 2$.

$$q_1 = (0,4,2,0) \to 14.$$

Используя q_1 найдем

$$a_1 = a_0 - bq_1 = (5,1,0,1) - (1,3,2,0 \cdot 0,4,2,0) = (5,4,2,1) \to 89.$$

Далее получаем остальные значения a_i и q_i:

$$q_2 = \left[\frac{a_1}{\bar{b}}\right] = (6,1,0,0) \to 6,\ a_2 = a_1 - bq_1 = (5,4,2,1) - (1,3,2,0 \cdot 6,1,0,0) =$$
$$= (6,1,2,1) \to 41;$$

$$q_3 = \left[\frac{a_2}{\bar{b}}\right] = (2,2,2,0) \to 2,\ a_3 = a_2 - bq_2 = (6,1,2,1) - (1,3,2,0 \cdot 2,2,2,0) =$$
$$= (4,0,1,1) \to 25;$$

$$q_4 = \left[\frac{a_3}{\bar{b}}\right] = (1,1,1,1) \to 1,\ a_4 = (4,0,1,1) - (1,3,2,0 \cdot 1,1,1,1) = (3,2,2,1) \to 17;$$

$$q_5 = \left[\frac{a_4}{\bar{b}}\right] = (1,1,1,1),\ a_5 = (3,2,2,1) - (1,3,2,0 \cdot 1,1,1,1) = (2,4,0,1) \to 9;$$

$$q_6 = \left[\frac{a_5}{\bar{b}}\right] = (1,1,1,1) \to 1,\ a_6 = (2,4,0,1) - (1,3,2,0 \cdot 1,1,1,1) = (1,1,1,1).$$

Так как $a_5 > \frac{b}{2}$, то $q_6 = 1$. Следовательно,

$$q = \sum_{i=1}^{b} q_i = (0,4,2,0) + (6,1,0,0) + (2,2,2,0) + (1,1,1,1) + (1,1,1,1) + (1,1,1,1) =$$
$$= (4,0,1,1) \to 25.$$

Действительно $[a/b] = [201/8] = 25$.

Выводы

1. Показано, что деление в модулярной арифметике имеет три формы: деление с нулевым остатком, округление, масштабирование и основное деление.

2. Разработаны алгоритмы масштабирования чисел с одинаковыми и разными знаками, которые состоят из операции деления и расширения базы и реализуются с помощью модульных вычислений. Показано, что при использовании разработанного метода при расширении чисел выигрыш достигает $(n - 1)$ раза.

3. Доказана теорема о модульном выполнении значения частного в случае, если делимое и делитель являются произвольными числами.

4. Разработан итерационный модулярный метод общего деления на основе модификации метода спуска Ферма, исходными данными которого являются произвольные значения делимого и делителя. При этом приблизительный делитель выбирается равным простому числу или их произведению, который в дальнейшем используется в итерациях получения промежуточных и окончательного значений частного. Представленная в частном ошибка при выполнении итераций уменьшается до нуля. Если допустимая ошибка задана не выше 0.1, то достаточно провести всего четыре итерации.

5. Определено правило выбора приблизительного делителя на основе свойств обобщенной позиционной системы счисления, которое позволяет делитель представить в виде простого числа или произведений простых чисел, на основе которых происходит округление делимого с целью выполнения алгоритма деления с нулевым остатком.

Литература

1. Акушский И.Я., Юдицкий Д.И. Машинная арифметика в остаточных классах. – М.: Советское радио, 1968. – 440 с.
2. Srabo N., Tanaka R. Residue arithmetic and its applications to computer technology. – New-York, 1967.
3. Червяков Н.И., Мезенцева О.С., Лавриненко И.Н., Сивоплясов Д.В. Метод расширения динамического диапазона модулярного нейрокомпьютера // Нейрокомпьютеры: разработка, применение. – 2005. – № 7. – С. 64-69.
4. Амербаев В.М. Теоретические основы машинной арифметики. – Алма-Ата: Наука, 1976. – 324 с.