ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ТЕХНОЛОГИЙ ПЕРЕДАЧИ И ОБРАБОТКИ ИНФОРМАЦИИ И СИГНАЛОВ

УДК 681.3

ЭФФЕКТИВНЫЙ АЛГОРИТМ ТОЧНОГО ОПРЕДЕЛЕНИЯ УНИВЕРСАЛЬНОЙ ПОЗИЦИОННОЙ ХАРАКТЕРИСТИКИ МОДУЛЯРНЫХ ЧИСЕЛ И ЕГО ПРИМЕНЕНИЕ ДЛЯ ВЫЧИСЛЕНИЯ ОСНОВНЫХ ПРОБЛЕМНЫХ ОПЕРАЦИЙ В СИСТЕМЕ ОСТАТОЧНЫХ КЛАССОВ

Бабенко М.Г., Лавриненко И.Н., Ляхов П.А., Червяков Н.И.

В статье приведен обзор и сравнительный анализ методов и алгоритмов определения позиционных характеристик числа в системе остаточных классов. Показано, что в качестве универсальной позиционной характеристики выбраны коэффициенты обобщенной позиционной системы счисления (ОПСС). На ее основе предложены эффективные алгоритмы выполнения основных проблемных операций в системе остаточных классов.

Ключевые слова: система остаточных классов, позиционная характеристика, обобщенная позиционная система счисления

Введение

Современное состояние развития инфокоммуникационных технологий в области обработки и передачи данных характеризуется интенсивным внедрением новых принципов и подходов к обработке информации. Результаты теоретических и практических разработок отечественных и зарубежных специалистов со всей определенностью указывают на то, что одним из перспективных многообещающих путей решения задач сокращения времени обработки данных и повышения надежности вычислительных средств является применение различных форм параллельной обработки данных, в том числе и на основе числовых систем с параллельной структурой. Одним из магистральных направлений среди современных подходов к созданию отказоустойчивых высокопроизводительных средств обработки данных является использование системы остаточных классов (СОК) [1-5].

Арифметика СОК долгое время вызывала интерес только на теоретическом уровне из-за сложности архитектур, определяемых использованием представляемых данных. Однако быстрый рост технологий вычислительной базы делает СОК удобной для многих приложений цифровой обработки данных, криптографии, систем передачи данных, основанных на множественном доступе с кодовым разделением каналов, облачных вычислений и др. [6-14]

Главным преимуществом СОК является разложение динамического диапазона на параллельные каналы с меньшими динамическими диапазонами, определяемыми выбором оснований СОК, которые приводят к операциям без переноса между каналами с различными основаниями и сокращению задержек сигналов [1-4]. В качестве недостатка СОК можно отметить трудность выполнения немодульных операций [5, 7-9, 14], для выполнения которых необходимо знать информацию о величине числа в целом. Существуют разные подходы к определению характеристик числа в системе остаточных классов, указывающих на его величину. Такие характеристики принято называть позиционными.

Система остаточных классов

Основной теоретико-числовой базой системы остаточных классов является теория сравнений. Полной системой вычетов по модулю p называется совокупность p целых чисел, содержащая точно по одному представителю из каждого класса вычетов по модулю p. Каждый класс вычетов по модулю p содержит в точности одно из чисел совокупности всех возможных остатков от деления на p: $\{0,1,...,p-1\}$. Множество $\{0,1,...,p-1\}$ также называется полной системой наименьших неотрицательных вычетов по модулю p.

Один из методов выполнения арифметических операций над длинными целыми числами основан на простых положениях теории чисел. Представление чисел в СОК позволяет заменить операции с большими числами на операции с малыми числами, которые представлены в виде остатков от деления больших чисел на заранее выбранные взаимно-простые модули $p_1, p_2, ..., p_n$. Пусть

$$A \equiv \alpha_1 (\mathrm{mod}\, p_1), \ldots, A \equiv \alpha_n (\mathrm{mod}\, p_n). \quad (1)$$

Тогда целому числу A можно поставить в соответствие кортеж $(\alpha_1, \alpha_2, ..., \alpha_n)$ наименьших неотрицательных вычетов по одному из соответствующих классов. Данное соответствие будет взаимно однозначным, пока $A < p_1 p_2 ... p_n$, в силу Китайской теоремы об остатках (КТО). Кортеж $(\alpha_1, \alpha_2, ..., \alpha_n)$ можно рассматривать как один из способов представления целого числа A в ЭВМ – модулярное представление или представление в СОК.

Основным преимуществом такого представления является тот факт, что выполнение операций сложения, вычитания и умножения реализуется очень просто по формулам:

$$A \pm B = (\alpha_1, \alpha_2, ..., \alpha_n) \pm (\beta_1, \beta_2 ..., \beta_n) = \\ = ((\alpha_1 \pm \beta_1) \bmod p_1, ..., (\alpha_n \pm \beta_n) \bmod p_n); \quad (2)$$

$$A \times B = (\alpha_1, \alpha_2, ..., \alpha_n) \times (\beta_1, \beta_2 ..., \beta_n) = \\ = ((\alpha_1 \times \beta_1) \bmod p_1, ..., (\alpha_n \times \beta_n) \bmod p_n). \quad (3)$$

Эти операции носят название модульных, так как для их выполнения в СОК достаточно одного такта обработки численных значений, причем эта обработка происходит параллельно и значения информации в каждом разряде не зависят от других разрядов.

Основной недостаток модулярного представления чисел состоит в том, что трудно упорядочить множество всех целочисленных кортежей длины n так, чтобы этот порядок соответствовал естественному порядку на множестве целых чисел. Как следствие этого факта, трудно установить, является ли кортеж $(\alpha_1, \alpha_2, ..., \alpha_n)$ большим (меньшим), чем $(\beta_1, \beta_2 ..., \beta_n)$. Трудно также проверить, возникло ли переполнение допустимого диапазона чисел $P = p_1 p_2 ... p_n$ в результате выполнения операций сложения или умножения, но еще труднее выполнить операцию деления. Эти и некоторые другие операции носят название немодульных, так как для их выполнения требуется знание о величине числа в целом, которая называется позиционной характеристикой числа.

Модель целочисленной модулярной арифметики можно задать следующей сигнатурой $\left\langle |P|, |\bullet|^{+}_{p_i}, MO, HO \right\rangle$, где: $|P|$ – полная система вычетов по модулю полного динамического диапазона, $|\bullet|^{+}_{p_i}$ – вычет чисел по модулю p_i, MO – множество модульных операций, к которым относятся арифметические операции сложения, вычитания, умножения и деления нацело или умножение на обратный элемент, HO – множество немодульных операций, к которым относятся расширения база СОК, деления, масштабирования и другие.

Немодульные операции обусловлены знанием числового значения модулярной величины, которая определенным образом связана со значениями компонент модулярного представления. Эти операции являются медленными, что снижает эффективность применения модулярной алгебры. Для реализации немодульных операций используются специальные функционалы, которые определяют количественные характеристики отношения порядка над множеством модулярных векторов. Одно из устоявшихся названий функционалов – позиционная характеристика (ПХ) модулярной величины или числовой величины в модулярном коде. В основе алгоритмов выполнения немодульных операций лежат методы вычисления ПХ, сложность которых непосредственно влияет на скорость выполнения немодульных операций в модулярной алгебре. Поиск эффективных и универсальных ПХ важен для теоретических основ модулярных вычислительных структур и вычислительных средств на их основе.

В настоящее время известны следующие методы определения позиционных характеристик модулярного представления чисел [1-4]: метод ортогональных базисов, метод функции Эйлера, метод интервальных оценок, метод с использованием коэффициентов обобщенной позиционной системы счисления (ОПСС) и другие. Анализ позиционных характеристик показал, что коэффициенты ОПСС представляют собой универсальную характеристику, на основе которой можно эффективно выполнить основные проблемные операции СОК.

Алгоритм эффективного вычисления универсальной позиционной характеристики

Суть метода вычисления ОПСС состоит в следующем. Пусть задана система оснований $p_1, p_2, ..., p_n$ с диапазоном $P = p_1 p_2 ... p_n$ и ортогональными базисами $B_1, B_2, ..., B_n$, которые определяются как

$$B_i \equiv \frac{m_i P}{p_i} \equiv 1 \bmod p_i, \; 1 = \overline{1, n}, \quad (4)$$

где m_i веса ортогональных базисов. Тогда КТО можно представить в виде

$$X = \sum_{i=1}^{n} \alpha_i B_i \bmod P = \sum_{i=1}^{n} \alpha_i B_i - R(x)P, \quad (5)$$

где α_i остатки (вычеты) числа X по $\bmod p$; $R(x)$ – ранг числа. Представим ортогональный базис B_i в ОПСС, тогда

$$B_i = b_{i1} + b_{i2} p_i p_2 + ... + b_{i,n} p_1 p_2 ... p_n, \quad (6)$$

где b_{ij} - коэффициенты ОПСС, $i, j = 1,2,...,n$.

На основе формулы (6) запишем $X_{\text{ОПСС}}$:

$$X_{\text{ОПСС}} = \alpha_1 (b_{11}, b_{12}, ..., b_{1n}) + \alpha_2 (b_{21}, b_{22}, b_{23}, ..., b_{2n}) + \\ + \alpha_3 (b_{31}, b_{32}, ..., b_{3n}) + ... + \alpha_n (b_{n,1}, b_{n,2}, ..., b_{n,n})$$

Так как $B_i \bmod p_i = 0$ для всех $j > i$, то перед первым значившим разрядом будут $i-1$ нулей. Для удобства вычислений базисы можно представить в виде матрицы

$$\begin{vmatrix} b_{11} & b_{12} & \cdots & b_{1n} \\ 0 & b_{22} & \cdots & b_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & b_{nn} \end{vmatrix}. \quad (7)$$

Тогда $X_{\text{ОПСС}}$ запишется как

$$X_{\text{СОК}} \to \begin{vmatrix} |\alpha_1 b_{11}|_{p_1} & |\alpha_2 b_{12}|_{p_1} & \cdots & |a_n b_{1n}|_{p_n} \\ 0 & |\alpha_2 b_{22}|_{p_2} & \cdots & |\alpha_n b_{2n}| p_n \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & |\alpha_n b_{nn}|_{p_n} \end{vmatrix}; \; X_{\text{ОПСС}} \to \overline{+ \quad a_1 \quad a_2 \quad ... \quad a_n}. \quad (8)$$

При этом

$$a_i = \sum_{j=i}^{n} \alpha_i b_{ij} \bmod p_i, \quad (9)$$

где a_i – коэффициенты ОПСС числа x; α_i – вычеты числа x по $\bmod p_i$,

b_{ij} – ортогональные базисы, представленные в ОПСС; $i, j = 1,2,..,n$

При использовании традиционной вычислительной базы произведения $\alpha_i b_{ij} \bmod p_i$ можно поместить в память, а адресами будут являться остатки α_i.

Последовательность вычисления для первого варианта имеет вид

$$\begin{array}{lll} & \text{Адрес ПЗУ} & \text{Выборка из ПЗУ} \quad \text{Модули СОК } p_1 \quad p_2 \quad ... p_n \\ X_{\text{СОК}} \to \begin{cases} a_1 \\ a_2 \\ \vdots \\ a_n \end{cases} & \begin{matrix} \to \\ \to \\ \\ \to \end{matrix} & \begin{matrix} [|\alpha_1 b_{11}]_{p_1}, |\alpha_1 b_{12}|_{p_2}, ..., |\alpha_1 b_{1n}|_{p_n}] \\ [0, \quad |\alpha_2 b_{22}|_{p_2}, ..., |\alpha_2 b_{2n}|_{p_n}] \\ \\ [0, \quad 0, \quad ..., |\alpha_n b_{nn}|_{p_n}] \end{matrix} \\ X_{\text{ОПСС}} \to & & \overline{+ a_1 \quad a_2 \quad ..., a_n} \end{array} \quad (10)$$

Для определения всех цифр ОПСС требуются две операции: одна операция для выборки из памяти и одна операция для суммирования. По сравнению с известным последовательным методом Гарнера выигрыш определяется выражением $3(n-1)/2$. Для реализации этого метода необходимо иметь средства для выполнения модулярных операций, например нейронные сети конечного кольца по p_i основаниям, где $i = 1,2,...,n$ [2-4].

Пример 1. Пусть основания системы $p_1 = 3$, $p_2 = 5$, $p_3 = 7$, $p_4 = 2$. Дано число $x = [2,3,0,1]$, представленное в СОК по выбранным модулям. Найти представления этого числа в ОПСС, то есть $x = [a_1, a_2, a_3, a_4]$. На основании выражения (4) определим ортогональные базисы СОК $B_1 = 70$, $B_2 = 126$, $B_3 = 120$, $B_4 = 105$. Представим базис B_i в ОПСС, тогда b_{ij}:

$$b_{11} = 1,\ b_{12} = 3,\ b_{13} = 4,\ b_{14} = 0,$$
$$b_{21} = 0,\ b_{22} = 2,\ b_{23} = 1,\ b_{24} = 1,$$
$$b_{31} = 0,\ b_{32} = 0,\ b_{33} = 1,\ b_{34} = 1,$$
$$b_{41} = 0,\ b_{42} = 0,\ b_{43} = 0,\ b_{44} = 1.$$

В связи с тем, что константы b_{ij} определяются выбором системы модулей СОК, то их с учетом переноса в *i* разрядах можно поместить в память, тогда процесс преобразований можно представить в виде

	Адрес ПЗУ	Выборки из ПЗУ	Модули СОК 3,5,7,2
$X_{\text{СОК}} \rightarrow$	$a_1 = 2$	$\rightarrow$	[2,1,2,1]
	$a_2 = 3$	$\rightarrow$	[0,1,4,3]
	$a_3 = 0$	$\rightarrow$	[0,0,0,0]
	$a_4 = 1$	$\rightarrow$	[0,0,0,1]
$X_{\text{ОПСС}} \rightarrow$			+[2,2,6,1]

Для определения всех цифр ОПСС требуются две операции: одна операция для выборки из памяти и одна операция для суммирования. По сравнению с последовательным итерационным процессом [12] выигрыш равен $n-1$, где n число модулей СОК.

Алгоритмы использования универсальной позиционной характеристики (УПХ) для вычисления основных проблемных операций в СОК

Метод расширения базы системы остаточных классов. Рассмотрим метод определения вычета по расширенному основанию на основе использования УПХ. Пусть СОК состоит из оснований $p_1, p_2, ..., p_n$. Объем диапазона этой системы будет $P = \prod_{i=1}^{n} p_i$. Добавим к числу оснований СОК новое основание p_{n+1}. Объем диапазона этой системы $P_{n+1} = \prod_{i=1}^{n+1} p_i$. Тогда любое число A из диапазона $[0, P_{n+1})$ в обобщенной системе счисления представляется в виде

$$A = a_{n+1}\prod_{i=1}^{n} p_i + a_n \prod_{i=1}^{n-1} p_i + ... + a_1 p_1 + a_0. \quad (11)$$

Если число A будет лежать в первоначальном диапазоне $[0, P)$, то в ОПСС цифра $a_{n+1} = 0$. Если $a_{n+1} \neq 0$, тогда значение числа A выходит за пределы динамического диапазона. Факт $a_{n+1} = 1$ используется для получения остатка (вычета) от деления числа A на новое основание СОК p_{n+1}.

Пусть число A имело представление $(\alpha_1, \alpha_2, ..., \alpha_n)$ по основаниям $p_1, p_2, ..., p_n$. Добавляем новое основание p_{n+1}, тогда число $A = (\alpha_1, \alpha_2, ..., \alpha_n, |A|_{p_{n+1}})$ в системе оснований $p_1, p_2, ..., p_n, p_{n+1}$ - остаток от деления числа A на p_{n+1}, то есть искомая цифра по новому основанию.

Для определения этой цифры используем метод перевода числа из СОК в ОПСС, включая неизвестную цифру $|A|_{p_{n+1}}$ в проводимые операции. При этом мы параллельно получим цифры ОПСС $\alpha_1, \alpha_2, ..., \alpha_n$ и выражение для цифры α_{n+1}. Но так как по условию число $A \in [0, P)$, то цифра $\alpha_{n+1} = 0$. Из полученного соотношения и определяем искомую цифру $|A|_{p_{n+1}}$. Рассмотрим этот метод на примере 2.

Пример 2. Пусть задана система модулей $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, тогда $P = 30$. И пусть задано число $A = 11 = (1,2,1)$. Расширим систему оснований, добавляя $p_4 = 7$. Тогда $A = 11 = (1,2,1,|A|_7)$ в системе оснований $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, $p_4 = 7$.

Набор констант b_{ij} задается матрицей

$$\begin{vmatrix} 1 & 1 & 2 & 3 \\ 0 & 2 & 1 & 2 \\ 0 & 0 & 1 & 4 \\ 0 & 0 & 0 & 4 \end{vmatrix}.$$

Процесс решения задачи иллюстрирует таблица 1.

Таблица 1. Определение цифр ОПСС

Вычеты числа A по модулю p_i	Модули			
	$p_1 = 2$	$p_2 = 3$	$p_3 = 5$	$p_4 = 5$
1	1	1	2	3
2	0	4	2	4
1	0	0	1	4
$\|A\|_7$	0	0	0	$4\cdot\|x\|_7$
Коэффициенты ОПСС числа A	1	2	1	$5+4\cdot\|x\|_7$

После сложения цифр по модулю p получим $A = (1,2,1,5+4\cdot|x|_7)$, но так как

$|5+4\cdot|x|_7|_7$, но по условию $a_4=0$, то есть $4\cdot|A|_7=-5$ или $|A|_7=-\left|\frac{5}{4}\right|_7=\left|\frac{1}{4}\right|_7(-5)$.

Мультипликативная обратная величина $\left|\frac{1}{4}\right|_7=2$, и так как число 5 отрицательное, возьмем его дополнение по модулю 7. Итак, вычет числа А по модулю 7 определяется выражением $|A|_7=2(7-5)=4$.

Тогда расширенное представление числа будет $A=11=(1,2,1,4)$. Так как результат образования цифр в СОК по новому основанию p_{n+1} зависит только от первых цифр, то операцию расширения вычетов можно проводить сразу по нескольким основаниям.

Деление и масштабирования чисел в СОК. 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]: деление с нулевым остатком, округление и масштабирование, 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

$$\left|\frac{a}{b}\right|_{p_i}=\left|\frac{1}{b}a\right|_{p_i} \tag{12}$$

для всех p_i, где $\left|\frac{1}{b}\right|_{p_i}$ – мультипликативная обратная *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

$$\left(\left|\frac{a}{b}\right|_{p_1},\left|\frac{a}{b}\right|_{p_2},...,\left|\frac{a}{b}\right|_{p_n}\right). \tag{13}$$

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

$$\left|\frac{a}{b}\right|_P\leftrightarrow\left\{\left|\frac{a}{b}\right|_{p_1},\left|\frac{a}{b}\right|_{p_2},...,\left|\frac{a}{b}\right|_{p_n}\right\}, \tag{14}$$

или

$$\frac{|b|_P}{\left|\frac{a}{b}\cdot b\right|_P}\leftrightarrow\frac{\{|b|_{p_1},|...,|b|_{p_n}\}}{\left\{\left|\left|\frac{a}{b}\right|_{p_1}|b|_{p_1}\right|_{p_1},...,\left|\left|\frac{a}{b}\right|_{p_n}|b|_{p_n}\right|_{p_n}\right\}}. \tag{15}$$

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

$$\left|\left|\frac{a}{b}\right|_{p_i}|b|_{p_i}\right|_p=|a|_{p_i}. \tag{16}$$

По уникальности мультипликативной инверсии следует, что

$$\left|\frac{a}{b}\right|_{p_i}\cdot|b|_{p_i}=|a|_{p_i}. \tag{17}$$

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 3. 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

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

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

$$1873/9\leftrightarrow(17,17,13)\cdot(13,25,7)=(18,9,29)\leftrightarrow 6601,$$

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 $\left[\frac{a}{b}=\frac{a-|a|_b}{b}\right]$. Следовательно, в системе вычетов $\left[\frac{a}{b}\right]$ представляется величинами $\left(\left|\frac{a-|a|_b}{b}\right|_{p_1},\left|\frac{a-|a|_b}{b}\right|_{p_2},...,\left|\frac{a-|a|_b}{b}\right|_{p_n}\right)$, 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

$$\left|\frac{a-|a|_b}{b}\right|_{p_i}=\left[\frac{a}{b}\right]_{p_i}=\left|\frac{1}{b}\cdot\left(a-|a|_b\right)\right|_{p_i}. \quad (18)$$

Это уравнение задает цифры системы вычетов для $\left[\frac{a}{b}\right]$ всех таких цифр, что НОД величин p_i и b равен 1. Остальные цифры 5 могут быть найдены с помощью метода расширения базы. Таким образом, алгоритм масштабирования состоит из двух следующих этапов.

1. Деление с нулевым остатком.
2. Расширение базы.

Процесс масштабирования покажем на числовом примере.

Пример 4. 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.

Таблица 2. Результаты вычислений остатка по модулю 5

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

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, результаты занесены в таблицу 2.

Таблица 3. Умножение $a-|a|_5$ на $\left|\frac{1}{5}\right|_{p_i}$

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)		

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, результаты вычислений в таблице 3.

Исходный интервал определения для всего набора модулей был равен [0-209], $\frac{a-|a|_5}{5}$ оказался в интервале [0-41], поэтому остаточное представление $(1,2\ ...4)$ неясно.

Остаток по модулю 5 может быть найден путем расширения базы. Это можно сделать по методу Гарнера или по предложенному методу в работе [9]. Для этого остаток по модулю 5 примем за 0 в первом случае и за $|a|_5$ – во втором, результат работы приведен в таблице 4.

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

Таблица 4. Расширение базы СОК

Расширение базы:	
на основе известного метода Гарнера	на основе предложенного метода
Номер Модули 2, 3, 5, 7 операции $a-\lvert a\rvert_5 \leftrightarrow (1,2,0,4)$ 1. Вычитаем 1 $\frac{(1,1,1,1)}{(0,1,4,3)}$ 2. Умножаем на $\left\lvert\frac{1}{2}\right\rvert_{p_i}$ $\frac{(-,2,3,4)}{(-,2,2,5)}$ 3. Вычитаем 2 $\frac{(-,2,2,2)}{(-,2,2,5)}$ 4. Умножаем на $\left\lvert\frac{1}{3}\right\rvert_{p_i}$ $\frac{(-,-,2,5)}{(-,-,0,1)}$ 5. Вычитаем 1 $\frac{(-,-,1,1)}{(-,-,4,0)}$	Матрица констант для набора с измененным порядком модулей $2,3,5,7$. $\begin{vmatrix}1&1&3&2\\0&2&4&2\\0&0&6&2\\0&0&0&3\end{vmatrix}$ 1. Умножение $\begin{matrix}1\cdot\\2\cdot\\4\cdot\\\lvert a\rvert_5\cdot\end{matrix}\begin{vmatrix}1&1&3&2\\0&2&4&2\\0&0&6&2\\0&0&0&3\end{vmatrix}\rightarrow\begin{vmatrix}1&1&3&2\\0&2&4&2\\0&0&6&2\\0&0&0&3\lvert a\rvert_5\end{vmatrix}$
Если $\left[\frac{a}{5}\right]$ обозначить как z_5, тогда получим $\lvert z_5\rvert+4=0$, отсюда	2. Сложение $(1,2,1,17+3\lvert a\rvert_5)$
6. $\lvert z_5\rvert=-4\bmod 5=1\bmod 5.$ Итак $\left[\frac{a}{5}\right]=(1,2,1,4)\leftrightarrow 11$	3. Вычисление остатка по mod 5 $17+3\lvert a\rvert_5=0$ Или $\lvert a\rvert_5=-17\left\lvert\frac{1}{3}\right\rvert_5 \bmod 5=1$. Итак $\left[\frac{a}{5}\right]=(1,2,1,4)\leftrightarrow 11$

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

Пример 5. Масштабирование положительного числа несколькими модулями. В примере 4 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: расчеты вычислений приведены в таблице 5. Для расширения базы внесем 0 в пропущенные колонки для метода Гарнера и обозначим как $\lvert a\rvert_3$ и $\lvert a\rvert_5$ – для предложенного метода из работы [7], результаты работы методов приведены в таблице 6.

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

Таблица 5. Первый этап масштабирования чисел несколькими модулями

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

Таблица 6. Второй этап масштабирования чисел несколькими модулями

<table>
<tr><th>Метод Гарнера</th><th>Предложенный метод</th></tr>
<tr><td>1. Вычитаем 1. (1, 0, 0, 5)
(1, 1, 1, 1)
(0, 2, 4, 4)
2. Умножаем на $\left\lvert \frac{1}{2} \right\rvert_{p_i}$ (-, 2, 3, 4)
(-, 1, 2, 2)
3. Вычитаем 2. (-, 2, 2, 2)
(-, 2, 0, 0)
4. Тогда $\left\lvert \frac{1}{2} \lvert z \rvert_3 + 2 \right\rvert = 0$ и $\left\lvert \frac{1}{2} \lvert z \rvert_5 + 2 \right\rvert = 0$.
Следовательно, $\lvert z \rvert_3 = 2$ и $\lvert z \rvert_5 = 0$ Отсюда, масштабируемое число $\left\lfloor \frac{89}{15} \right\rfloor$ это $(1, 2, 0, 5) \leftrightarrow 5$.</td><td>Разобьем матрицу констант для измененной последовательности модулей на 2 матрицы
Модули $\begin{vmatrix} 1, & 3, & 1 \\ 0, & 4, & 2 \\ 0, & 0, & 2 \end{vmatrix}$ и $\begin{vmatrix} 1, & 3, & 2 \\ 0, & 4, & 1 \\ 0, & 0, & 3 \end{vmatrix}$
1 Умножаем
$\begin{matrix} 1\cdot \\ 5\cdot \\ \lvert x \rvert_3 \cdot \end{matrix} \begin{vmatrix} 1, & 3, & 1 \\ 0, & 20, & 10 \\ 0, & 0, & 2\cdot\lvert x \rvert_3 \end{vmatrix}$; $\begin{matrix} 1\cdot \\ 5\cdot \\ \lvert x \rvert_3 \cdot \end{matrix} \begin{vmatrix} 1, & 3, & 2 \\ 0, & 20, & 5 \\ 0, & 0, & 9\cdot\lvert x \rvert_3 \end{vmatrix}$
$1, \quad 2, \quad 14 + 2\cdot\lvert x \rvert_3$ $1, \quad 2, \quad 10 + 3\cdot\lvert x \rvert_3$
Отсюда</td></tr>
<tr><td></td><td>$14 + 2\cdot\lvert x \rvert_3 = 0$,
$\lvert x \rvert_3 = -7 \bmod 3 =$
$= 2 \bmod 3$
$10 + 3\cdot\lvert x \rvert_5 = 0$,
$\lvert x \rvert_5 = -10\left\lvert \frac{1}{3} \right\rvert_5 = 20 \bmod 5 = 0 \bmod 5$
$\left\lfloor \frac{89}{15} \right\rfloor = (1, \quad 2, \quad 0, \quad 5) \leftrightarrow 5$</td></tr>
</table>

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 результатом 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 $\left[0,\frac{P}{2b}-1\right]$ 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 следует, что 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 6. 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

Таблица 6. Второй этап масштабирования чисел несколькими модулями

Метод Гарнера	**Предложенный метод**	
1. Вычитаем 1. (1, 0, 0, 5) (1, 1, 1, 1) (0, 2, 4, 4) 2. Умножаем на $\left\|\frac{1}{2}\right\|_{p_i}$ (-, 2, 3, 4) (-, 1, 2, 2) 3. Вычитаем 2. (-, 2, 2, 2) (-, 2, 0, 0) 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.	Разобьем матрицу констант для измененной последовательности модулей на 2 матрицы Модули $\begin{vmatrix}1, & 3, & 1\\ 0, & 4, & 2\\ 0, & 0, & 2\end{vmatrix}$ и $\begin{vmatrix}1, & 3, & 2\\ 0, & 4, & 1\\ 0, & 0, & 3\end{vmatrix}$ 1 Умножаем $\begin{matrix}1\cdot\\ 5\cdot\\ \|x\|_3\cdot\end{matrix}\begin{vmatrix}1, & 3, & 1\\ 0, & 20, & 10\\ 0, & 0, & 2\cdot\|x\|_3\end{vmatrix}$; $\begin{matrix}1\cdot\\ 5\cdot\\ \|x\|_3\cdot\end{matrix}\begin{vmatrix}1, & 3, & 2\\ 0, & 20, & 5\\ 0, & 0, & 9\cdot\|x\|_3\end{vmatrix}$ $1,\quad 2,\quad 14+2\cdot\|x\|_3$ $1,\quad 2,\quad 10+3\cdot\|x\|_3$ Отсюда	
	$14+2\cdot\|x\|_3=0$, $\|x\|_3=-7\bmod 3=$ $=2\bmod 3$	$10+3\cdot\|x\|_5=0$, $\|x\|_5=-10\left\|\frac{1}{3}\right\|_5=20\bmod 5=0\bmod 5$
	$\left[\frac{89}{15}\right]=(1,\quad 2,\quad 0,\quad 5)\leftrightarrow 5$	

Таблица 7. Результаты решения первого этапа примера 6.

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 $\leftrightarrow \left[\frac{P-979}{7\cdot 11}\right]$

целого числа. Результаты выполнения занесены в таблицу 7.

Внесем 0 в пропущенные колонки для расширения базы, см. вычисления, приведенные в таблице 8. Пусть z будет результатом этой операции масштабирования, то есть $z=\left[\frac{P-979}{7\cdot 11}\right]$, тогда $\frac{1}{13}\cdot\frac{1}{9}|z|_{11}+3=0$, $|z|_{11}=1$, $\frac{1}{13}\cdot\frac{1}{9}|z|_{7}+2=0$, $|z|_{7}=4$.

В строку $(0,5,-,-,1)\xleftrightarrow{13,9,2}\left[\frac{P-979}{7\cdot 11}\right]$ 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 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,(9×13) –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 $z=\left[\frac{-979}{77}\right]=-13$.

Таблица 8. К решению примера 6.

	(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)
	(–, 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, 1)
Вычитаем 1	(–, –, 1, 1, 1)
	(–, –, 3, 2, 0)

Разработка метода и алгоритма основного модулярного деления. Рассмотренные модели связаны со специальными случаями и не применимы в

ситуации, когда и делимое, и делитель представляют собой произвольные целые числа.

Различные алгоритмы деления целых чисел $\frac{a}{b}$ можно описать итеративной схемой, использующей так называемый метод спуска Ферма [4]. Конструируется некоторое правило ϕ, 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 ϕ, 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 φ_1, паре (r_2, b) ставится в соответствие q_3, такое, что $r_2 - bq_1 = r_3 \geq 0$, и так далее. Так как последовательное применение операции ϕ приводит к строго убывающей последовательности положительных целых чисел $a \geq r_1 \geq r_2 \geq r_3 \geq ... \geq 0$, 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 K-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 $\sum_{i=1}^{k} q_i + r'_k$. Если $r_k < \frac{b}{2}$, то $r'_k = 0$, а если $r_k > \frac{b}{2}$, то $r'_k = 1$.

Доказательство проведем для случая, когда $b = \lambda \cdot b$ при $\lambda = 1,2,....$ Выполним следующую последовательность действий:

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

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

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

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

$$a\left(1 - \frac{1}{\lambda}\right) - a\frac{1}{\lambda}\left(1 - \frac{1}{\lambda}\right) =$$

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

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

...

$$q_k = \left[\frac{a}{\bar{b}}\right] \cdot \frac{a}{b} \cdot \frac{1}{\lambda}\left(1 - \frac{1}{\lambda}\right)^{k-1};\ q_k = \frac{a_{k-1}}{\bar{b}},\ \bar{b} \leq \lambda_{k+1};$$

$$q_1 + q_2 + ... + q_k = \left[\frac{a}{b}\right] \cdot \frac{1}{\lambda} + \left[\frac{a}{b}\right] \cdot \frac{1}{\lambda} \cdot \left(1 - \frac{1}{\lambda}\right) +$$

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

$$= \left[\frac{a}{b}\right]\frac{1}{\lambda}\left[1 + \left(1 - \frac{1}{\lambda}\right) + \left(1 - \frac{1}{\lambda}\right)^2 + ... + \left(1 - \frac{1}{\lambda}\right)^{k-1}\right] =$$

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

Итак, $\sum_{i=1}^{k} q_i = \left[\frac{a}{b}\right]\left(1 - \left(1 - \frac{1}{\lambda}\right)^k\right)$. Проведенные расчеты на ЭВМ приведены на графике рис. 1, где видно, что в качестве делителя лучшие характеристики получаются при $\lambda = 1,2,3,4$. При $\lambda = 1$ частное представляет собой точное значение, а при $\lambda = 2$ частное при малом числе итераций приближается к точному ее значению. Таким образом, в качестве делителя выбирается величина $b \leq \bar{b} \leq 2b$.

Заметим, что при $\lambda = 1$ 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 $\bar{b}$ целесообразно выбрать равное 2, то есть $b \leq \bar{b} < 2b$. Проблема разработки оптимальных вычислительных алгоритмов деления побуждает к разработке таких операций ϕ_i, которые бы минимизировали число шагов спуска Ферма и вместе с тем достаточно просто реализовывались на заданной вычислительной базе. Кроме того, на способ формирования операции ϕ 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?

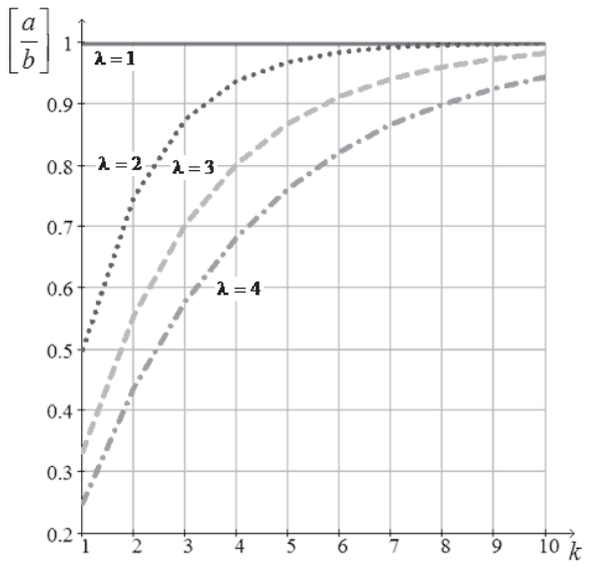

Рис. 1. График зависимости точности вычислений от значения величины делителя и числа итераций

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 $p_1, p_2, ..., p_n$, либо целое положительное число, представляющее собой произведение чисел попарно простых с $p_1, p_2, ..., p_n$. 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 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 $q_i = \left[\frac{a}{b}\right]$. Найденный таким образом q_1 далее используется в рекурсивных соотношениях $a_i = a_{i-1} - bq_i$, $a_0 = a$ и $q_i = \left[\frac{a_{i-1}}{b}\right]$ 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

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

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 $\bar{b}$, который определяется из условия $b \le \bar{b} < 2b$ и удовлетворяет условию алгоритма масштабирования.

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

В таблице 9 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 9 можно аппроксимировать. Для определения $\bar{b}$ можно составить таблицу 10 приблизительного делителя.

Пример 7. 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 $b_9 = 0$, $b_8 = 0$, $b_7 = 0$, $b_6 = 0$, $b_5 = 0$, $b_4 = 0$, $b_3 = 3$,

Таблица 9. Цифры приблизительного делителя

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

Таблица 10. К определению приблизительного делителя

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

$b_2 = 3$, $b_1 = 21$, где b_i определяем из уравнения:

$$b = b_9(23\cdot19\cdot17\cdot13\cdot11\cdot7\cdot5\cdot3) + b_8(23\cdot19\cdot17\cdot13\cdot11\cdot7\cdot5) + b_7(23\cdot19\cdot17\cdot13\cdot11\cdot7) + + + b_6(23\cdot19\cdot17\cdot13\cdot11) + b_5(23\cdot19\cdot17\cdot13) + b_4(23\cdot19\cdot17) + b_3(23\cdot19) + b_2(23) + b_1.$$

Используя таблицу 10 с $b_l = 3$, получаем $\bar{b} = 5\cdot19\cdot23 = 2185$, так как b_i 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 10. 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, которые приведены в таблице 10. 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 и $\bar{b}$ – аппроксимация b.

Модифицируем полученный алгоритм на язык кольцевых операций СОК. Для этого рассмотрим следующий пример.

Пример 8. В остаточной системе, состоящей из модулей 7, 5, 3, 2, необходимо разделить число $a = 201 \to (5,1,0,1)$ на число $b = 8 \to (1,3,2,0)$. Округленное частное обозначим как $q = \left[\frac{a}{b}\right]$.

Решение: вначале преобразуем делитель b в ОПСС в порядке уменьшаемой значимости:

$b = b_4(7\cdot5\cdot3) + b_3(7\cdot5) + b_2 7 + b_1$, тогда $b = 0\cdot(7\cdot5\cdot3) + 0\cdot(7\cdot5) + 1\cdot7 + 1$, где $b_2 = 1$, $b_1 = 1$.

Используя таблицу 1 с 1 с $b_p = b_2$ и $b_i \neq 0$ $i \neq p$, 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 значения a_1 и q_i:

$$q_2 = \left[\frac{a_1}{\bar{b}}\right] = (6,1,0,0) \to 6;$$
$$a_2 = a_1 - bq_1 = (5,4,2,1) - (1,3,2,0 \cdot 6,1,0,0) = $$
$$= (6,1,2,1) \to 41;$$
$$q_3 = \left[\frac{a_2}{\bar{b}}\right] = (2,2,2,0) \to 2;$$
$$a_3 = a_2 - bq_2 = (6,1,2,1) - (1,3,2,0 \cdot 2,2,2,0) = $$
$$= (4,0,1,1) \to 25;$$
$$q_4 = \left[\frac{a_3}{\bar{b}}\right] = (1,1,1,1) \to 1;$$
$$a_4 = (4,0,1,1) - (1,3,2,0 \cdot 1,1,1,1) = (3,2,2,1) \to 17;$$
$$q_5 = \left[\frac{a_4}{\bar{b}}\right] = (1,1,1,1) \to 1);$$
$$a_5 = (3,2,2,1) = (1,3,2,0 \cdot 1,1,1,1) = (2,4,0,1) \to 9;$$
$$q_6 = \left[\frac{a_5}{\bar{b}}\right] = (1,1,1,1) \to 1;$$
$$a_6 = (2,4,0,1) - (1,3,2,0 \cdot 1,1,1,1) = (1,1,1,1).$$

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

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

Действительно $\left[\frac{a}{b}\right] = \left[\frac{201}{8}\right] = 25$.

Заключение

В статье представлены проблемные направления в СОК, исследования которых необходимы при проектировании СОК-архитектур следующего поколения.

1. Исследование позиционных характеристик СОК показывает, что коэффициенты ОПСС представляют собой универсальную позиционную характеристику, на основе которой можно эффективно выполнять основные проблемные операции СОК.

2. Показано, что предложенный метод расширения базы позволяет получить расширенное представление вычетов числа сразу по нескольким дополнительным основаниям, что не снижает быстродействия операции расширения при одновременном расширении на несколько модулей СОК.

3. Исследованы модификации алгоритма масштабирования чисел в СОК, которое состоит из операции деления и расширения базы СОК и реализуется с помощью модульных вычислений. Показано, что при использовании модифицированного алгоритма масштабирования, построенного на основе расширения базы, выигрыш вычислительной сложности равен (n – 1) раз.

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.

Благодарность

Работа выполнена при финансовой поддержке Российского Фонда Фундаментальных Исследований, грант № 13-07-00478-а.

Литература

1. Акушский И.Я., Юдицкий Д.И. Машинная арифметика в остаточных классах. М.: Сов. радио, 1968. – 440 с.
2. Модулярные параллельные вычислительные структуры нейропроцессорных систем. Под ред. Н И. Червякова. М.: ФИЗМАТЛИТ, 2003. – 288 с.

3. Нейрокомпьютеры в остаточных классах. Под ред. А.И. Галушкина. М.: Радиотехника, 2003. – 272 с.
4. Omondi A., Premkumar A. Residue Number Systems. Theory and Implementation. London: Imperial College Press, 2007. – 295 p.
5. Червяков Н.И. Методы, алгоритмы и техническая реализация основных проблемных операций, выполняемых в системе остаточных классов // ИКТ. Т.9, №4, 2011. – С. 4-12.
6. Chervyakov N.I., Veligosha A.V., Tyncherov K.T., Velikikh S.A. Use of modular coding for high-speed digital filter design // Cybernetics and Systems Analysis. No. 34, 1998. – P. 254-260.
7. Zheng XD., Xu J., Li W. Parallel DNA arithmetic operation based on n-moduli set // Applied Mathematics and Computation. №212(1), 2009. – P. 177-184.
8. Gomathisankaran M., Tyagi A., Namuduri K. HORNS: A homomorphic encryption scheme for Cloud Computing using Residue Number System // Information Sciences and Systems (CISS)., 45th Annual Conference, 2011. – P.1-5.
9. Alia G., Martinelli E. NEUROM: a ROM based RNS digital neuron // Neural Networks. №18, 2005. – P. 179-189.
10. Червяков Н.И. Реализация высокоэффективной модулярной цифровой обработки сигнала на основе программируемых логических интегральных схем // Нейрокомпьютеры: разработка, применения. №10, 2006. – С. 27-36.
11. Червяков Н.И., Тынчеров К.Т., Велигоша А.В. Высокоскоростная цифровая обработка сигналов с использованием непозиционной арифметики // Радиотехника. №10, 1997. – С. 23-29.
12. Червяков Н.И., Евдокимов А.А., Галушкин А.И., Лавриенко И.Н., Лавриенко А.В. Применение искусственных нейронных сетей и системы остаточных классов в криптографии. М.: ФИЗМАТЛИТ, 2012. – 280 с.
13. Червяков Н.И. Организация арифметических расширителей в микропроцессорных системах, базирующихся на множественном представлении информации // Управляющие системы и машины. №1, 1987. – С. 26-29.
14. Червяков Н.И. Методы и принципы построения модулярных нейрокомпьютеров // 50 лет модулярной арифметике, сборник трудов Юбилейной МНТК. М.: ОАО «Ангстрем», МИЭТ, 2006. – С. 239-249.

THE EFFECTIVE ALGORITHM OF EXACT DEFINITION OF UNIVERSAL POSITIONAL CHARACTERISTICS OF MODULAR NUMBERS AND ITS APPLICATION TO CALCULATION OF THE MAIN AREAS OF OPERATIONS IN THE SYSTEM OF RESIDUAL CLASSES

Babenko M.G., Lavrinenko I.N., Lyakhov P.A., Chervyakov N.I.

The paper gives an overview and comparative analysis of methods and algorithms for determining the positional characteristics in the residue number system. It is shown that as a universal positional characteristics choose the coefficients of a generalized positional number system (GPNS). Proposed are effective algorithms perform critical operations to the system of residual classes.

Keywords:

Бабенко Михаил Григорьевич, к.ф-м.н., доцент Кафедры прикладной математики и математического моделирования (ПММ) Северо-Кавказского федерального университета (СКФУ). Тел. (8-865) 238-80-84. E-mail: whbear@yandex.ru

Лавриненко Ирина Николаевна, к.ф-м.н., доцент Кафедры высшей алгебры и геометрии СКФУ. Тел. (8-865) 277-56-26. E-mail: k-fmf-primath@stavsu.ru

Ляхов Павел Алексеевич, к.ф-м.н., доцент кафедры ПММ СКФУ. Тел. 8-962-028-72-14. E-mail: ljahov@mail.ru

Червяков Николай Иванович, д.т.н., профессор, Заслуженный деятель науки и техники РФ, заведующий Кафедрой ПММ СКФУ. Тел. (8-865) 275-35-64. E-mail: k-fmf-primath@stavsu.ru