УДК 511.334.12

РАСПАРАЛЛЕЛИВАНИЕ ВЫЧИСЛИТЕЛЬНЫХ ОПЕРАЦИЙ НА ОСНОВЕ МОДУЛЯРНЫХ СТРУКТУР ДАННЫХ

Чернобровкин В.В.

ГБОУ ВПО Сургутский государственный университет, Сургут, e-mail:kooa@adm.surgu.ru

В статье рассматриваются методы повышения скорости вычислительных операций над многоразрядными числами с помощью системы остаточных классов или модулярной системы счисления. Приведено доказательство одного из вариантов китайской теоремы об остатках, лежащей в основе модулярного представления чисел. Образование цифр модулярного представления проводится независимо и каждый разряд несет информацию обо всем числе, что позволяет проводить параллельную обработку в независимых каналах, а также использовать новые методы арифметического контроля. Информация для обработки, представленная в виде вычетов, позволяет использовать исходные данные с большим или сверхбольшим количеством разрядов. Многоразрядные модулярные вычисления, применяемые для задач большой алгоритмической сложности позволяют периодически повышать производительность вычислительной техники.

Ключевые слова: Модулярная система счисления, Китайская теорема об остатках, сравнения, вычеты, вычислительные операции.

PARALLELIZATION OF COMPUTING OPERATIONS ON THE BASIS OF MODULAR DATA STRUCTURES

Chernobrovkin V.V.

SEI HPE «Surgut State University», Surgut, e-mail:kooa@adm.surgu.ru

This article discusses methods to improve the computational speed of operations on multi-bit numbers using a system of residual classes or modular system value. It is given the proof of one embodiment of the Chinese Remainder Theorem, the underlying modular representations of numbers. Spawn figures modular presentation conducted independently and each category contains information about everything including that allows parallel processing of independent channels, as well as the use of new methods of arithmetic control. Information processing, presented in the form of deductions, the original data can be used with large or super- large number of bits. Modular multi-bit computing, applied to problems of great algorithmic complexity, allow increasing productivity calculated inflammatory technology for periodic.

Keywords: system of residual classes, Chinese remainder theorem, comparison, deductions, computing operations.

Введение

Основной стратегией теоретических и практических исследований, осуществляемых в настоящее время, является применение подходов, базирующихся на интенсивном использовании различных форм параллелизма на алгоритмическом, программном и аппаратном уровнях. В связи с чем исключительно большое значение имеют исследования, ориентированные на применение нетрадиционных способов кодирования числовой информации и соответствующих им параллельных вариантов компьютерной арифметики [6]. Возможность применения модулярной системы счисления [1–3,5–10] в вычислительных алгоритмах обусловливается наличием изоморфизма между математическими операциями над целыми числами и соответствующими операциями над системой целых неотрицательных вычетов по взаимно-простым модулям. Сложение, умножение, возведение в целую положительную степень целых положительных чисел сводятся к соответствующим

операциям, выполняемым над множеством вычетов, – представлением этих чисел в модулярной системе счисления.

Целью исследования является исследование вопросов повышения скорости выполнения арифметических операций над многоразрядными числами с применением возможностей модулярной системы счисления, выявление зависимости объема обрабатываемых данных от нетрадиционных способов их представления и времени выполнения вычислительных операций с ними. Это является особенно важным при разработке алгоритмов для решения задач большой вычислительной сложности.

Методы исследования для решения поставленной задачи основываются на системном анализе, теории сравнений, теории чисел и алгоритмов, численных методах.

Фундаментом теоретико-числовой базой модулярной системы является теория сравнений, основы которой были разработаны Эйлером и отечественным математиком П.Л. Чебышевым. Применительно к обработке информации модулярными кодами теория опирается на следующее утверждение. Пусть A и p – два произвольных целых числа, причем p – положительное число, тогда в результате деления числа A на число p получаются частное и остаток [8]. Делимость A на p удовлетворяет равенству

$$\forall A \in Z: A = pl + a \qquad (1)$$

и неравенству

$$0 \le \alpha < p, \qquad (2)$$

где l – частное, α – остаток.

Согласно (1), величина a называется наименьшим неотрицательным вычетом [1, 3, 4–7, 8] целого числа A по модулю p и обозначается символом $|A|_p$.

Для дальнейшего понимания вычислительных операций в модулярной системе проведем доказательство одного из вариантов китайской теоремы об остатках [2–4, 7, 10, которая является фундаментальным положением в основе модулярного представления чисел.

Теорема 1 (Китайская теорема об остатках). Любое целое положительное число A в модулярной системе счисления можно представить в виде набора остатков (вычетов) от деления этого числа на выбранные основания (модули) системы.

Доказательство.

Пусть число A представлено в системе остаточных классов следующим образом:

$$A \leftrightarrow (a_1, a_2, \dots, a_n), \qquad (3)$$

где $a_1, a_2, \dots, a_n$ – наименьшие, неотрицательные вычеты, образованные путем целочисленного деления числа A на выбранные основания

$$P = p_1 * p_2 *, \dots, * p_n = \prod_{i=1}^{n} p_i, \qquad (4)$$

где p_i – взаимно простые числа.

Если $\forall\, i \neq j$, $НОД(p_i, p_j) = 1$, т.е. взаимно простые, то представление числа (3) является единственным, при условии

$$0 \leq A \leq p. \tag{5}$$

Тогда число A может быть представлено следующим образом:

$$\begin{gathered} A \equiv a_1 (mod p_1); \\ A \equiv a_2 (mod p_2); \\ \dots\dots\dots\dots \\ A \equiv a_n (mod p_n); \end{gathered} \tag{6}$$

Теорема доказана.

Формула (6) определяют сравнения, которые показывают, что каждый вычет a_i получается независимо, а значит параллельно от других и содержит информацию обо всём числе. Данное обстоятельство определяет, если для таких вычислений организовать программно-аппаратную вычислительную базу, то вычеты могут образовываться параллельно.

Цифры a_i представления (3) по выбранным модулям образуются следующим образом:

$$a_i = A(mod p_i) = A - \left\lfloor \frac{A}{p_i} \right\rfloor p_i, \ (\forall i \in [1, \dots, n]), \tag{7}$$

где $\left\lfloor \frac{A}{p_i} \right\rfloor$ — целочисленное частное; p_i – взаимно простые числа (основания системы).

Приведем пример, в котором рассмотрим кодирование чисел в модулярной системе счисления на конкретном примере. Пусть даны основания $p_1 = 2$, $p = 3$, $p_3 = 5$, тогда . Отображение всех тридцати чисел в системе оснований p_1, p_2, p_3 приведено в таблице.

Отображение чисел в системе остаточных классов

Десятичное представление числа	0	1	2	3	4	5	6	7	8	9
Изображение чисел в остатках по модулям 2, 3, 5	(0,0,0)	(1,1,1)	(0,2,2)	(1,0,3)	(0,1,4)	(1,2,0)	(0,0,1)	(1,1,2)	(0,2,3)	(1,0,4)
Десятичное представление числа	10	11	12	13	14	15	16	17	18	19
Изображение чисел в остатках по модулям 2, 3, 5	(0,1,0)	(1,2,1)	(0,0,2)	(1,1,3)	(0,2,4)	(1,0,0)	(0,1,1)	(1,2,2)	(0,0,3)	(1,1,4)

Десятичное представление числа	20	21	22	23	24	25	26	27	28	29
Изображение чисел в остатках по модулям 2, 3, 5	(0,2,0)	(1,0,1)	(1,0,2)	(1,2,3)	(0,0,4)	(1,1,0)	(0,2,1)	(1,0,2)	(0,1,3)	(1,2,4)

Как видно из таблицы, все остатки в модулярной системе одноразрядные, что дает преимущества для вычислительных операций перед обычной позиционной системой счисления (ОПСС), особенно если величина разрядов в числах значительно растет.

Над вычетами можно выполнять арифметические операции сложения, вычитания и умножения в кольце вычетов. Все они относятся к модульным операциям, то есть не требуют вычисления позиционных характеристик (ПХ) обрабатываемых чисел и поэтому считаются быстрыми.

Отношение сравнения по модулю натурального числа обладает следующими свойствами:

1) симметричность: $a \equiv a(mod\ m)$;

2) рефлексивность: $a \equiv b(mod\ m) \rightarrow b \equiv a(modm)$;

3) транзитивность: $a \equiv a(mod\ m), b \equiv c(mod\ m), \text{то} a \equiv c\ (mod\ m)$.

Множество вычетов по модулю натурального числа с двумя операциями обладает кольцевыми свойствами:

1) ассоциативность по сложению: $(\forall a, b, \mathbf{c} \in \mathbf{Z_p}), a + (b + \mathbf{c}) = (a + b) + \mathbf{c}$;

2) существование нулевого элемента: $(\exists 0 \in \mathbf{Z_p})(\forall \mathbf{a} \in \mathbf{Z_p}), \quad a + \mathbf{0} = \mathbf{0} + a = a$;

3) существование обратного элемента: $(\forall a \in \mathbf{Z_p})(\exists \mathbf{b} \in \mathbf{Z_p}), \quad a + b = b + a = \mathbf{0}$;

4) ассоциативность по умножению: $(\forall a, b, \mathbf{c} \in \mathbf{Z_p}), \quad a \cdot (b \cdot \mathbf{c}) = (a \cdot b) \cdot \mathbf{c}$;

5) дистрибутивность: $(\forall a, b, \mathbf{c} \in \mathbf{Z_p}), a \cdot (b + \mathbf{c}) = a \cdot b + a \cdot \mathbf{c}, (b + \mathbf{c}) \cdot a = b \cdot a + \mathbf{c} \cdot a$.

Рассматривая вычисления в кольце вычетов $|Z|_{p_i}$ с помощью модулярной арифметики все операции можно разбить на две группы. Пусть операнды *A* и *B*, а также результаты операций $A \pm B$ и $A \cdot B$ представлены соответственно остатками α_i, β_i, γ_i, δ_i по основаниям p_i, где ($\forall i \in [1, \dots, n]$). Причём оба числа и результаты находятся в диапазоне [0, P], то есть

$A = (\alpha_1, \alpha_2, \dots, \alpha_n), B = (\beta_1, \beta_2, \dots, \beta_n)$;

$$A \pm B = |A \pm B|_p = \left|\sum_{i=1}^{n} \left[\left|[A|]_{p_i}\right] \cdot m_i \cdot P_i \pm \sum_{i=1}^{n} \left[\left|[B|]_{p_i}\right] \cdot m_i \cdot P_i \right| = \right.;$$

$$A \cdot B = |A \cdot B|_p = \left|\sum_{i=1}^{n} \left[\left|[A|]_{p_i}\right] \cdot m_i \cdot P_i \cdot \sum_{i=1}^{n} \left[\left|[B|]_{p_i}\right] \cdot m_i \cdot P_i \right| = \right. \quad (8)$$

При этом $A, \quad B, \quad A+B, \quad A-B, \quad A \cdot B, \in |Z|_p$ – кольцо целых чисел.

Так как выражение (8) является прямым следствием фактов теории чисел [2, 3, 5], то результаты аддитивной и мультипликативной операций можно переписать в виде

$$A \pm B \equiv a_i \pm \beta_i \ (mod\ p_i); \ AB \equiv a_i \beta_i \ (mod\ p_i), \text{ при } \forall i \in [1,..n]. \quad (9)$$

Если положить

$$\gamma_i \equiv a_i + \beta_i \ (mod\ p_i), \ \delta_i \equiv a_i \cdot \beta_i \ (mod\ p_i), v_i \equiv a_i - \beta_i \ (mod\ p_i), \quad (10)$$

то цифрами результата являются, соответственно,

$$\gamma_i = a_i + \beta_i - \left|\frac{a_i + \beta_i}{p_i}\right| \cdot p_i;$$

$$\delta_i = a_i \beta_i - \left|\frac{a_i \beta_i}{p_i}\right| \cdot p_i; \quad (11)$$

$$v_i = a_i - \beta_i - \left|\frac{a_i - \beta_i}{p_i}\right| \cdot p_i.$$

Выражения (11) могут быть получены на основании выражения (6).

Из вышеизложенного очевидно, что все вычислительные операции в кольце $|Z|_{p_i}$ полностью распараллеливаются с помощью модулярной системы.

Перейдем к немодульной операции деления в модулярной системе. Если рассматривать представление (3) с условием $a_i = 0, \quad (i = 1,2, \dots, n)$, то операцию деления можно проводить в модулярной системе счисления поразрядно. Пусть числа *A* и *B* представлены по основаниям $p_1, p_2, \dots, p_n$. Тогда они будут иметь представления:

$$A = (a_1, a_2, \dots, a_n), \quad B = (\beta_1, \beta_2, \dots, \beta_n), \quad a_i \neq 0, \quad \beta_i \neq 0, \quad \forall i \in [1, \dots, n]$$

Результат деления $\frac{A}{B} = (q_1, q_2, \dots, q_n)$, (12)

где $q_i \ (\forall i \in [1, \dots, n])$ определяются как решения сравнения;

$$q_i = \frac{a_i}{\beta_i} (mod\ p_i) \equiv \left(a_i \left(\frac{1}{\beta_i}\right) mod\ p_i\right) (mod\ p_i) \ \forall i \in [1, \dots, n]. \quad (13)$$

Очевидно, что деление без остатка двух чисел в модулярной системе осуществляется путем модульного умножения делимого на мультипликативную обратную величину делителя.

Величина $y = \frac{1}{\beta_i} \bmod p_i$ является решением сравнения

$$y\beta_i \equiv 1 \ (mod p_i) \tag{14}$$

и однозначно определена, если β_i и p_i – взаимно простые числа.

Сравнения (13) имеют единственные решения в том случае, когда $\beta_i \neq 0$; a_i может принимать значение 0, поэтому от ограничения $a_i \neq 0$ можно отказаться.

Если число *A* делится нацело на *B*, то представление (7) дает истинное значение для дроби $C = \frac{A}{B}$, где *C* – некоторое целое число; если число *A* не делится нацело на *B*, то представление (7) будет формальным представлением дроби $\frac{A}{B}$; в этом случае $C \equiv \frac{A}{B \ (mod \ P)}$.

Модульные операции и их результаты называются формальными, если при выполнении этих операций пренебрегают возможным выходом за пределы вычислительного диапазона.

Если *A* делится на *B* и среди цифр β_i имеются нулевые значения, то из делимости *A* на *B* следует, что и $a_i = 0$. Таким образом, при поразрядном делении в *i*-м представлении (7) имеет место неопределенность типа, для раскрытия которой необходимо знание о всем числе [1].

Согласно китайской теореме об остатках все операции проходят по *n* каналам. Для этого построим параллельную вычислительную схему следующего вида (рис. 1):

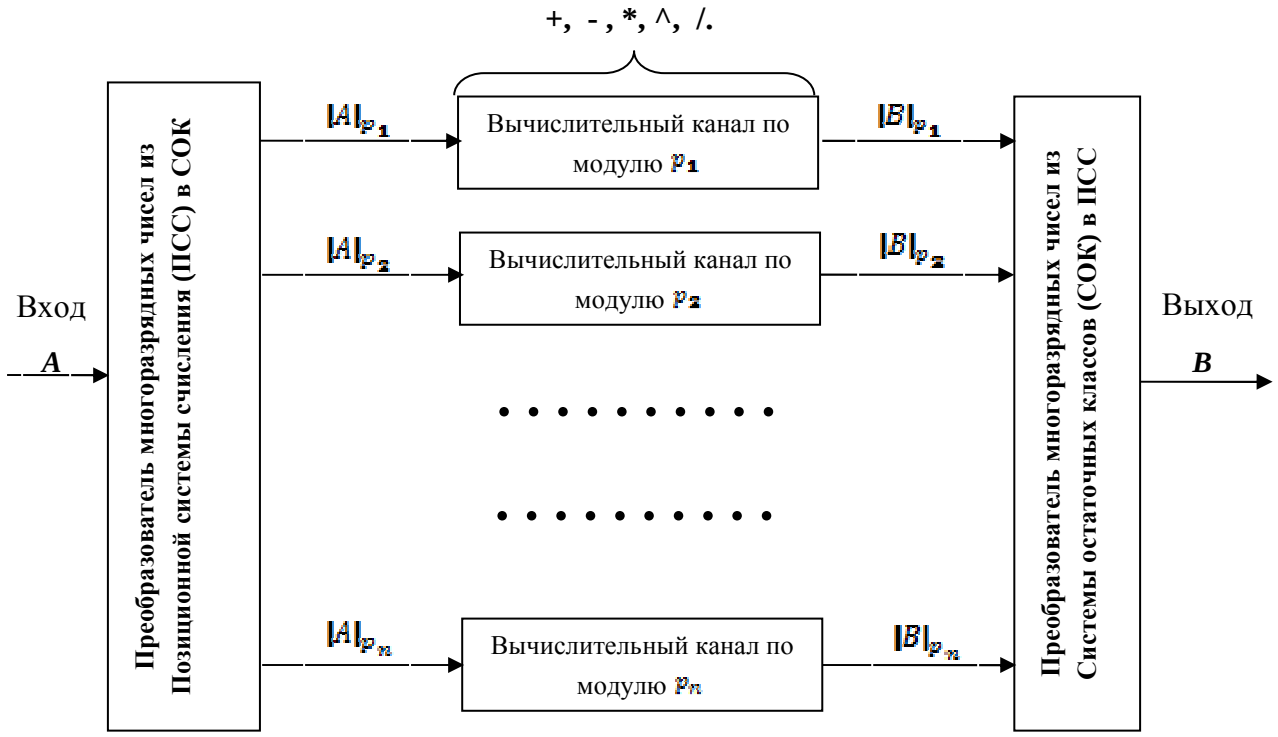

Рис.1. Обобщенная схема обработки многоразрядных чисел в модулярной системе

На схеме показано как *A* – входные многоразрядные данные – преобразуются на основе системы остаточных классов и подаются в *n* каналов обработки. Каждый из *n* каналов вычисляет по выбранному модулю (основанию) p_i входные данные. Затем вычисленные значения поступают в «обратный» преобразователь и выходят в виде результата *B*.

На сравнительных графиках показана зависимость времени выполнения вычислительных операций от разрядности входных данных (рис. 2). Преимущества по времени и объему обрабатываемых данных при параллельной обработке возникают при следующих условиях:

1) разрядность обрабатываемых данных значительная;

2) количество и разрядность выбранных модулей (оснований) унифицированы под обрабатываемые данные.

Все вычислительные операции проводились на процессорах одного класса Intel Core2 Quad.

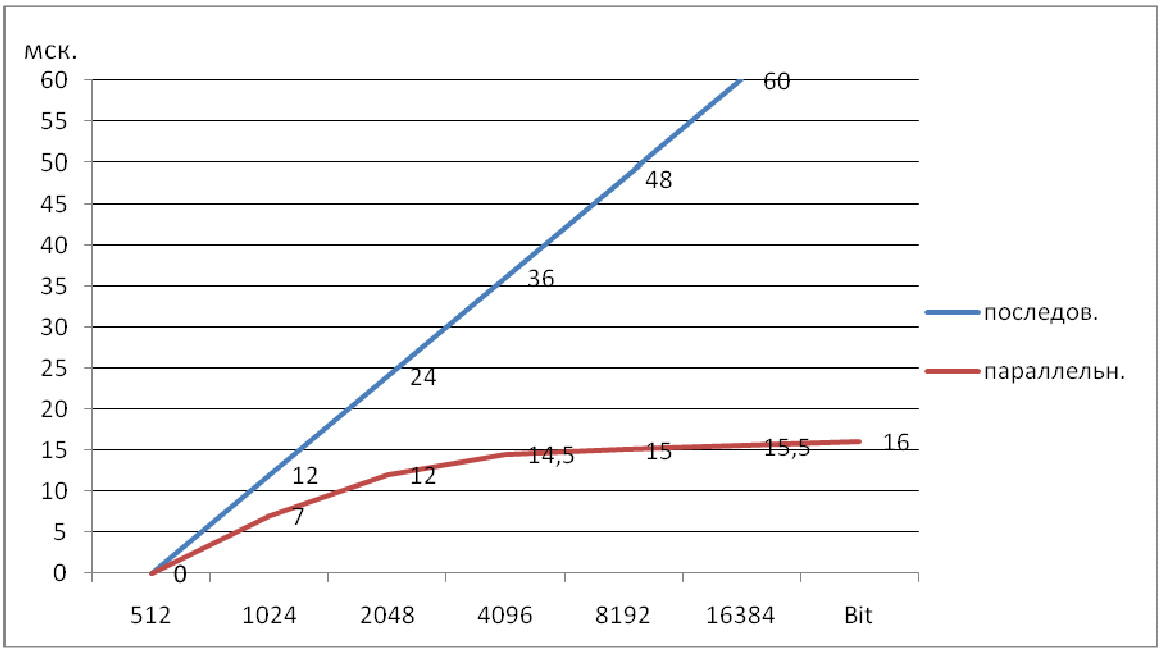

Рис. 2. Сравнительная схема выполнения вычислительных операций

На рис. 2 видно, что график при параллельной обработке данных похож на график функции $y = \log(x)$и лежит ниже линейной зависимость последовательной обработки, что свидетельствует о преимуществах параллельной обработки на основе модулярного представления данных.

Выводы

1. Применение системы остаточных классов для вычислительных операций с многоразрядными данными дает значительное преимущество перед позиционными системами, так как имеет естественную по своей природе параллельность.

2. Вычисление цифр модулярного представления проводится независимо, и каждый вычет несёт информацию обо всём числе, что позволяет проводить параллельную обработку вычетов в независимых каналах и использовать методы арифметического контроля.

3. На основе модулярной системы представления данных возможны разработки параллельных алгоритмов для решения задач большой алгоритмической сложности.

Список литературы

1. Акушский И.Я., Юдицкий Д.М. Машинная арифметика в остаточных классах. – М.: Советское радио, 1968. – 440 с.
2. Бухштаб А.А. Теория чисел. – М: Наука,1977. – 368 с.
3. Виноградов И.М. Основы теории чисел. — М.: Наука, 1981. – 176 с.
4. Инютин С. А. Модулярные вычисления в сверх больших компьютерных диапазонах // Известия высших учебных заведений. – Электроника. – № 6. – 2001. – С. 81–87.
5. Инютин С. А. Вычислительные задачи большой алгоритмической сложности и модулярная арифметика // Вестник Тюменского государственного университета. – 2002. – № 3. – С. 14–23.
6. Коутинхо С. Введение в теорию чисел. Алгоритм RSA. – М.: Постмаркет, 2001. – 45 с.
7. Лобес М.В. Разработка методов и алгоритмов модулярных вычислений для задач большой алгоритмической сложности: дис. … канд. физ.-мат. наук. – Ставрополь, 2009. – 192 с.
8. Модулярные параллельные вычислительные структуры нейропроцессорных систем / Н.И. Червяков. – М.: Физматлит, 2003. – 43с.
9. Ноден П., Ките К. Алгебраическая алгоритмика. – М.: Мир, 1999. – 720 с.
10. Основы теории делимости чисел, решение уравнений в целых числах. Факультативный курс МГИЭТ (ТУ) / В.В. Бардушкин [и др.]. – М., 2003. – 100 с.

Рецензенты:

Бахарев М.С., д.т.н., профессор, профессор кафедры «Нефтегазовое дело» Федеральное государственное бюджетное образовательное учреждение высшего профессионального

образования Сургутский институт нефти и газа, (филиал) Тюменского государственного нефтегазового университета, г. Сургут.

Инютин С.А., д.т.н., профессор, профессор кафедры «Проектирование вычислительных комплексов» ФГБОУ ВПО «МАТИ – Российский государственный технологический университет им. К.Э. Циолковского (МАТИ)» г. Москва.