УДК 681.4

О некоторых новых алгоритмах обработки информации для выполнения сложных операций в системе остаточных классов

Ю.Д.Полисский[1]

Аннотация – **This work includes the new data processing algorithms to perform complex operations in the system of residual classes. Algorithms are based on the calculation of the above residues in each module and require no change nepozitsionnogo representation of numbers in a positional for further processing in a positional system.**

Ключевые слова – **Тезисы доклада, система остаточных классов, модули, сложные операции, приведенные остатки.**

I. Введение

Перспективным направлением реализации эффективных вычислений является в настоящее время распараллеливание алгоритмов на всех этапах вычислительного процесса. Это достигается путем привлечения новых принципов на основе использования системы остаточных классов (СОК). Преимущество СОК заключается в том, что арифметические операции в ней выполняются без учета переносов из разряда в разряд, что позволяет распараллелить вычислительный процесс на уровне арифметических операций. Однако возникают серьезные трудности при реализации сложных, так называемых немодульных, операций, для выполнения которых необходимо знание цифр операндов по всем разрядам. В связи с этим значительная часть работ по совершенствованию машинной арифметики СОК посвящена ускорению выполнения сложных операций.

II. Постановка задачи

СОК называется система счисления, в которой произвольное число N представляется в виде набора наименьших неотрицательных остатков по модулям, $m_1, m_2, \ldots, m_n$, т.е $N = (\alpha_1, \alpha_2, \ldots, \alpha_n)$. Здесь $\alpha_i = N(\mathrm{mod}\, m_i)$. При этом, если числа m_i взаимно простые, то представление числа N в таком виде является единственным.

Исследования [1]-[3] показали, что реализация каждой из немодульных, сложных операций основана на «внешних» по отношению к системе представления чисел способах. Для этого в явном или неявном виде определяются позиционные характеристики чисел с последующей их обработкой в позиционной системе. Задача заключается в разработке алгоритмов, основанных на «внутренних» по отношению к системе счисления способах без предварительного преобразования непозиционного представления в позиционное.

III. Основная часть

По имеющимся у автора сведениям в работе [4] впервые предложен новый алгоритм, не требующий указанных преобразований, основанный на вычислении лишь «внутренних» характеристик - приведенных остатков первого рода по каждому модулю. В данной работе предлагается алгоритм формирования приведенных остатков второго рода и приводится теоретическое обоснование обоих алгоритмов.

Рассмотрим СОК с m_i и m_{i+1}, $m_i < m_{i+1}$. Пусть в этой СОК имеется некоторое число $A^j = (\alpha^j_i, \alpha^j_{i+1})$, где $\alpha^j_{i+1} = 0$, $j = 0,1,2,\ldots, m_i - 1$. Составим

$$\Delta^j_i = (\alpha^j_i - \alpha^j_{i+1})(\mathrm{mod}\ m_i) = \alpha^j_i. \quad (1)$$

$$\Re^j_i = (\alpha^j_i + \alpha^j_{i+1})(\mathrm{mod}\ m_i) = \alpha^j_i. \quad (2)$$

Рассмотрим значения разности при последовательном добавлении к A^j чисел $B^k = 1,2,\cdots,k,\ldots,m_{i+1}$, где $k = (\beta^k_i, \beta^k_{i+1})$.

Получаем

$$A^{j+1} = A^j + B^k = (\alpha^{j+1}_i, \alpha^{j+1}_{i+1}),$$

где $\alpha_i{}^{j+1} = \alpha_i{}^j + \beta_i{}^k$, $\alpha_{i+1}{}^{j+1} = \alpha_{i+1}{}^j + \beta_{i+1}{}^k$.

Составим

$$\begin{aligned}\Delta^{j+1}{}_i &= (\alpha^{j+1}{}_i - \alpha^{j+1}{}_{i+1})(\mathrm{mod}\ m_i) = \\ &= (\alpha^j_i + \beta^k{}_i - \beta^k{}_{i+1})(\mathrm{mod}\ m_i)\end{aligned}. \quad (3)$$

Пусть B^k такое, что $\alpha_i{}^j + \beta_i{}^k < m_i$. Тогда $\beta_{i+1}{}^k = \beta_i{}^k = \beta_1{}^k$ и $\Delta^{j+1}{}_i = \alpha^j_i$. Если число B^k такое, что $\alpha_i{}^j + \beta_i{}^k = m_i$, то $\beta_{i+1}{}^k = \beta_i{}^k = m_i - \alpha_i{}^j$. Следовательно, $\alpha_i{}^{j+1} = 0$, $\alpha_{i+1}{}^{j+1} = \alpha_{i+1}{}^j + m_i$. В этом случае

$$\begin{aligned}\Delta^{j+1}{}_i &= (\alpha^{j+1}{}_i - \alpha^{j+1}{}_{i+1})(\mathrm{mod}\ m_i) = \\ &= (0 - m_i + \alpha_i{}^j)(\mathrm{mod}\ m_i) = \alpha_i{}^j\end{aligned}. \quad (4)$$

Если же число B^k такое, что $m_i < \alpha_i{}^j + \beta_i{}^k < m_{i+1}$, то $\alpha_i{}^{j+1} = \alpha_i{}^j + \beta_i{}^k - m_i$, $\alpha_{i+1}{}^{j+1} = \beta_i{}^k$ и

[1] Научно-исследовательский институт автоматизации черной металлургии (НИИАчермет), ул.Шевченко, 59, Днепропетровск, 49000, УКРАИНА, E-mail: polissky@mail.ru

$$\Delta^{j+1}{}_i = \left(\alpha^{j+1}{}_i - \alpha^{j+1}{}_{i+1}\right)(\mathrm{mod}\ m_i) = \\ = \left(\alpha^{j}{}_i + \beta^{k}{}_i - m_i - \beta^{k}{}_i\right)(\mathrm{mod}\ m_i) = \alpha^{j}{}_i \quad (5)$$

Наконец, при $B^k = m_{i+1}$, при котором $m_i < \alpha_i{}^j + \beta_i{}^k$, а $\beta_i{}^k = (m_{i+1})(\mathrm{mod}\ m_i)$, $\beta_{i+1}{}^k = m_{i+1}$, получаем $\alpha_i{}^{j+1} = \alpha_i{}^j + \beta_i{}^k - m_i$ и $\alpha_{i+1}{}^{j+1} = 0$. Т.е. получаем $A^{j+1} = (\alpha_i{}^{j+1}, \alpha_{i+1}{}^{j+1})$ и $\alpha_{i+1}{}^{j+1} = 0$, а $\Delta_i{}^{j+1} = \tilde{\alpha}_i{}^{j+1}$, где

$$\tilde{\alpha}_i{}^{j+1} = \left(\alpha_i{}^j + m_{i+1}\right)(\mathrm{mod}\ m_i). \quad (6)$$

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

$$\Delta_i{}^{j+t} = \tilde{\alpha}_i{}^{j+t},$$

где

$$\tilde{\alpha}_i{}^{j+t} = \left(\alpha_i{}^j + t m_{i+1}\right)(\mathrm{mod}\ m_i). \quad (7)$$

Таким образом, весь диапазон чисел оказывается разбитым на $K = m_1 m_2 \ldots m_i \ldots m_{n-1}$ поддиапазонов длины m_n, внутри каждого из которых значения разностей одинаковы. При этом меньшим (большим) из чисел поддиапазона является число с меньшим (большим) значением α_n.

Рассмотрим значения суммы $\Re_i^j$ при последовательном добавлении к A^j чисел $B^k = 1,2,\cdots,k,\ldots,m_{i+1}$, где $k = \left(\beta^k{}_i, \beta^k{}_{i+1}\right)$. Получаем $A^{j+1} = A^j + B^k = \left(\alpha^{j+1}{}_i, \alpha^{j+1}{}_{i+1}\right)$, где $\alpha_i{}^{j+1} = \alpha_i{}^j + \beta_i{}^k$, $\alpha_{i+1}{}^{j+1} = \alpha_{i+1}{}^j + \beta_{i+1}{}^k$.

Составим

$$\Re^{j+1}{}_i = \left(\alpha^{j+1}{}_i + \alpha^{j+1}{}_{i+1}\right)(\mathrm{mod}\ m_i) = \\ = \left(\alpha^{j}{}_i + \beta^{k}{}_i + \beta^{k}{}_{i+1}\right)(\mathrm{mod}\ m_i) \quad (8)$$

Пусть B^k такое, что $\alpha_i{}^j + \beta_i{}^k \le m_i$. Тогда $\beta_{i+1}{}^k = \beta_i{}^k = \beta_1{}^k$ и $\Re^{j+1}{}_i = \alpha^j{}_i + 2\beta_i{}^k$.

Если же число B^k такое, что $m_i < \alpha_i{}^j + \beta_i{}^k < m_{i+1}$, то $\alpha_i{}^{j+1} = \alpha_i{}^j + \beta_i{}^k - m_i$, $\alpha_{i+1}{}^{j+1} = \beta_i{}^k$ и

$$\Re^{j+1}{}_i = \left(\alpha^{j+1}{}_i + \alpha^{j+1}{}_{i+1}\right)(\mathrm{mod}\ m_i) = \\ = \left(\alpha^{j}{}_i + \beta^{k}{}_i - m_i + \beta^{k}{}_i\right)(\mathrm{mod}\ m_i) = \alpha^{j}{}_i + 2\beta_i{}^k. \quad (9)$$

Наконец, при $B^k = m_{i+1}$, при котором $m_i < \alpha_i{}^j + \beta_i{}^k$, а $\beta_i{}^k = (m_{i+1})(\mathrm{mod}\ m_i)$, $\beta_{i+1}{}^k = m_{i+1}$, получаем $\alpha_i{}^{j+1} = \alpha_i{}^j + \beta_i{}^k - m_i$ и $\alpha_{i+1}{}^{j+1} = 0$. Т.е., получаем $A^{j+1} = (\alpha_i{}^{j+1}, \alpha_{i+1}{}^{j+1})$ и $\alpha_{i+1}{}^{j+1} = 0$, а $\Re_i{}^{j+1} = \tilde{\alpha}_i{}^{j+1}$,

где

$$\tilde{\alpha}_i{}^{j+1} = \left(\alpha_i{}^j + m_{i+1}\right)(\mathrm{mod}\ m_i). \quad (10)$$

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

$$\Re_i{}^{j+t} = \tilde{\alpha}_i{}^{j+t},$$

где

$$\tilde{\alpha}_i{}^{j+t} = \left(\alpha_i{}^j + t m_{i+1}\right)(\mathrm{mod}\ m_i). \quad (11)$$

Таким образом, весь диапазон чисел оказывается разбитым на $K = m_1 m_2 \ldots m_i \ldots m_{n-1}$ поддиапазонов длины m_n, поочередно четных и нечетных линейно возрастающих чисел.

IV. Заключение

Предложены новые алгоритмы обработки информации для выполнения сложных операций в системе остаточных классов, основанные на формировании «внутренних» по отношению к системе счисления характеристиках – приведенных остатках первого и второго рода без предварительного преобразования непозиционного представления в позиционное. На основе приведенных остатков эффективно выполняется базовая немодульная операция – сравнение чисел, лежащая в основе всех немодульных, сложных операций.

Список ссылок

[1] Полисский Ю.Д. Методы выполнения немодульных операций в системе остаточных классов/ Матеріали XIV міжнародної конференції з автоматичного управління (Автоматика-2007). - Севастополь, 10-14 вересня 2007 р. – Ч.І – Севастополь: СНЯУЯЄтаП, 2007. - С. 43-45.

[2] Полисский Ю.Д. Выполнение сложных операций в модулярных вычислительных структурах / Матеріали XV міжнародної конференції з автоматичного управління. Автоматика-2008". - Одеса:- 10-14 вересня. – 2008 р. –Ч.І .–Одеса: ОНМА, 2008. - С.43-45.

[3] Полисский Ю.Д. Быстрое выполнение сложных операций в системе остаточных классов / Матеріали XVII міжнародної конференції з автоматичного управління. Автоматика-2010". – Харків:- 27-29 вересня. - 2010 р. – Т.2 .– Харків: ХНУРЕ, 2010. – С.191-192.

[4] М.Г.Факторович, Ю.Д.Полисский. Устройство для сравнения чисел, выраженных в системе остаточных классов. Авт. свид. №608155 М. Кл2 G 06 F 7/04, 1978.