УДК 519.6

МОДУЛЬНОЕ УМНОЖЕНИЕ ЧИСЕЛ В НЕПОЗИЦИОННОЙ СИСТЕМЕ СЧИСЛЕНИЯ КЛАССА ВЫЧЕТОВ В ОТРИЦАТЕЛЬНОМ ЧИСЛОВОМ ДИАПАЗОНЕ

Загуменная Е. В., к.т.н.
Харьковский Национальный технический университет сельского хозяйства имени Петра Василенко
Тел. (057) 712-35-37

***Аннотация* – в данной статье рассмотрена операция модульного умножения в отрицательном числовом диапазоне на основе класса вычетов.**

***Ключевые слова* – числовой диапазон, модульное учножение, информационное сжатие данных.**

Постановка проблемы. Результаты исследований в области создания вычислительных средств обработки информации показали, что использование непозиционной системы счисления класса вычетов (КВ) в качестве системы счисления компьютерных вычислительных средств, предназначенных для реализации в положительном числовом диапазоне целочисленных арифметических операций сложения, вычитания и умножения, может существенно повысить производительность решения задач определенного класса. Однако необходимо отметим, что существует многочисленный класс алгоритмов и задач (задачи маршрутизации, задачи оптимизации и пр.), где кроме выполнения целочисленных арифметических операций сложения, вычитания и умножения в положительном числовом диапазоне существуют необходимость реализации перечисленных выше арифметических операций в отрицательном числовом диапазоне.

Анализ последних исследований и публикаций. В литературе уже были описаны табличные методы и алгоритмы модульного умножения чисел в непозиционной системе счисления класса вычетов [1-3]. Поиск путей упрощения структуры табличного вычислительного средства обусловил необходимость совершенствования методов и алгоритмов реализации модульных операций, позволяющих повысить эффективность применения табличного метода в КВ. Так [3] представлен метод табличной реализации операции модульного умножения.

Особенностью реализации данного метода является возможность уменьшения количества оборудования за счет сокращения на (50-70)% логических элементов «И» в узлах таблицы ПЗУ, непосредственно реализующих операцию модульного умножения по произвольному m_i модулю КВ. Это возможно за счет использования свойств симметрии таблицы реализации $a_i b_i (\mathrm{mod}\, m_i)$ модульной операции умножения. Недостаток рассмотренного метода состоит в том, что его использование не дает возможности создать табличный метод реализации операции умножения в КВ в отрицательном числовом диапазоне.

Цель статьи. Создание универсальных вычислительных средств обработки информации при решении задач маршрутизации и оптимизации.

Основная часть. Для построения метода табличной реализации умножения в КВ как для положительного, так и для отрицательного числовых диапазонов представим входные числа A и B в следующем виде (искусственная форма представления чисел в КВ [4])

$$A' = A + m/2 \text{ и } B' = B + m/2,$$

для m – четных чисел;

$$A' = A + (m-1)/2 \text{ и } B' = B + (m-1)/2,$$

для m – нечетныхчисел.

Если, например, m – четное число, тогда выполняются следующие соотношения

$$\begin{cases} -m/2 \le A(B) < m/2, 0 \le A'(B') < m-1, \\ -m/2 \le A \cdot B < m/2, 0 \le (A \cdot B)' < m-1. \end{cases}$$

Очевидно, что

$$(A \cdot B)' = A \cdot B + m/2. \qquad (1)$$

Тогда имеем

$$(A' \cdot B') \bmod m = \left[(A + m/2)(B + m/2) \right] \bmod m = \left[AB (\mathrm{mod}\ m/2) + m/2 \cdot (A + B + m/2) \right] \bmod m. \qquad (2)$$

Из выражения (1) очевидно, что

$$A \cdot B = A' \cdot B' - m/2 \cdot (A + B + m/2). \qquad (3)$$

Подставим выражение (3) в формулу (1). Получим, что

$$(A \cdot B)' = A' \cdot B' - m/2 \cdot (A + B + m/2) + m/2. \qquad (4)$$

В выражении (4) есть член, который имеет численное значение $m/2$. Он и обуславливает ошибку в вычислении значения $A' \cdot B' (\mathrm{mod}\, m)$. Таким образом формулы для вычисления $A \cdot B (\mathrm{mod}\, m)$ имеют следующий вид для m – четных чисел

$$\left[(A \cdot B) \bmod m/2 \right]' = (A' \cdot B') \bmod m + m/2, \tag{5}$$

или

$$\left[(A \cdot B) \bmod m/2 \right]' = (A' \cdot B') \bmod m. \tag{6}$$

Для m нечетного имеем

$$\left[(A \cdot B) \bmod (m-1)/2 \right]' = (A' \cdot B') \bmod m + (m-1)/2, \tag{7}$$

или

$$\left[(A \cdot B) \bmod (m-1)/2 \right]' = (A' \cdot B') \bmod m. \tag{8}$$

Учитывая выражения (1-8), выводим соотношение для реализации модульного умножения для положительного и отрицательного числовых диапазонов

$$\begin{aligned} &a_i' = a_i + m_i/2,\ \ a_i' = a_i' + (m_i - 1)/2;\ \ a_i' = [\gamma_{a_i}', (a_i')^*]; \\ &b_i' = b_i + m_i/2,\ \ b_i' = b_i' + (m_i - 1)/2;\ \ b_i' = [\gamma_{b_i}', (b_i')^*]. \end{aligned} \tag{9}$$

Для m_i – четного

$$\gamma_{a_i}'(\gamma_{b_i}') = \begin{cases} 0, \text{если } 0 \le a_i'(b_i') \le m_i/2, \\ 1, \text{если } m_i/2 < a_i'(b_i') \le m_i - 1. \end{cases} \tag{10}$$

Для m_i – нечетного

$$\gamma_{a_i}'(\gamma_{b_i}') = \begin{cases} 0, \text{если } 0 \le a_i'(b_i') \le (m_i - 1)/2, \\ 1, \text{если } (m_i - 1)/2 < a_i'(b_i') \le m_i - 1. \end{cases} \tag{11}$$

Числовая часть $(a_i')^*\,[(b_i')^*]$ кода информационного сжатия данных определяется следующим образом. Для m_i – четного

$$(a_i')^*[(b_i')^*] = \begin{cases} a_i'\,(b_i'), \text{если } 0 \le a_i'(b_i') \le m_i/2; \\ \overline{a_i'}\,(\overline{b_i'}) = m_i - a_i'(b_i'), \\ \text{если } m_i/2 < a_i'(b_i') \le m_i - 1. \end{cases} \tag{12}$$

при этом $0 \le (a_i')^*\,[(b_i')^*] \le m_i/2.$

Для m_i – нечетного числа

$$(a_i')^*[(b_i')^*] = \begin{cases} a_i'\,(b_i'), \text{если } 0 \le a_i'(b_i') \le (m_i - 1)/2; \\ \overline{a_i'}\,(\overline{b_i'}) = m_i - a_i'(b_i'), \\ \text{если } (m_i - 1)/2 < a_i'(b_i') \le m_i - 1. \end{cases} \tag{13}$$

при этом $0 \le (a_i')^*\,[(b_i')^*] \le (m_i - 1)/2.$

Результат $(a_i' \cdot b_i') \bmod m_i$ операции представляется в коде информационного сжатия данных, т.е. в виде $\{\gamma_i', [(a_i')^*(b_i')^*] \bmod m_i\}$, тогда

$$(a_i' \cdot b_i') \bmod m_i = \begin{cases} [(a_i')^* \cdot (b_i')^*] \bmod m_i, \\ \text{если } (\gamma'_{a_i} + \gamma'_{b_i}) = 0 \pmod 2; \\ m_i - [(a_i')^* \cdot (b_i')^*] \bmod m_i, \\ \text{если } (\gamma'_{a_i} + \gamma'_{b_i}) = 1 \pmod 2. \end{cases} \quad (14)$$

при этом $0 \le [(a_i')^* \cdot (b_i')^*] \bmod m_i \le m_i - 1$.

Формула для определения произведения двух чисел в КВ имеет следующий вид

$$(A \cdot B) \bmod M == (A' \cdot B') \bmod M = [(a_1', a_2', ..., a_i', ..., a_n') \cdot (b_1', b_2', ..., b_i', ..., b_n')] \bmod M$$
$$(a_2' \cdot b_2') \bmod m_2, ..., (a_i' \cdot b_i') \bmod m_i, ..., (a_n' \cdot b_n') \bmod m_n]. \quad (15)$$

Так, как все модули $\{m_i\}$, $i = \overline{1, n}$ КВ, (за исключением возможно только одного основания), нечетные

Так, как все модули $\{m_i\}$, $i = \overline{1, n}$ КВ, (за исключением возможно только одного основания), нечетные числа, то в дальнейшем, без потери общности рассуждений, будем считать, что основание КВ нечетные числа. Формула (15) с учетом кода информационного сжатия данных имеет следующий вид

$$(A' \cdot B') \bmod M = (\{[\gamma'_{a_1}, (a_1')^*] \cdot [\gamma'_{b_1}, (b_1')^*]\} \bmod m_1,$$
$$\{[\gamma'_{a_2}, (a_2')^*] \cdot [\gamma'_{b_2}, (b_2')^*]\} \bmod m_2, ..., \{[\gamma'_{a_i}, (a_i')^*] \cdot [\gamma'_{b_i}, (b_i')^*]\} \bmod m_i, ..., [\gamma'_{a_n}, (a_n')^*] \cdot$$
$$\cdot [\gamma'_{b_n}, (b_n')^*]\} \bmod m_n) = (\{\gamma_1', [(a_1')^* \cdot (b_1')^*] \bmod m_1\},$$
$$\{\gamma_2', [(a_2')^* \cdot (b_2')^*] \bmod m_2\}, ..., \{\gamma_i', [(a_i')^* \cdot (b_i')^*] \bmod m_i\}, ..., \{\gamma_n', [(a_n')^* \times (b_n')^*] \bmod m_n\}), \quad (16)$$

где

$$(a \cdot b_i^{'}) \bmod m_i = \{[\gamma_{a_i}^{'}, (a_i^{'})^*] \cdot [\gamma_{b_s}, (b_i^{'})^*]\} \bmod m_i = \{\gamma_i^{'}, [(a_i^{'})^* \cdot (b_i^{'})^*]\} \bmod m_i. \quad (17)$$

Исходя из (16) ÷ (17) где, а также учитывая, что (9) ÷ (15), для $m-$нечетного получим следующие соотношение для реализации модульной операции алгебраического умножения в КВ

$$\begin{cases} \{(a_i \cdot b_i) \bmod [(m_i - 1)/2]\}^{'} = \\ = \{[(\gamma_{a_i}, a_i) \cdot (\gamma_{b_i}, b_i)] \bmod [(m_i - 1)/2]\}^{'} = (a_i^{'} \cdot b_i^{'}) \bmod m_i + (m_i - 1)/2 = \\ = \{[\gamma_{a_i}^{'}, (a_i^{'})^*] \cdot [\gamma_{b_i}^{'}, (b_i^{'})^*]\} \bmod m_i + (m_i - 1)/2 = \{\gamma_i^{'}, [(a_i^{'})^* \cdot (b_i^{'})^*] \bmod m_i + (m_i - 1)/2; \\ \{(a_i \cdot b_i) \bmod [(m_i - 1)/2]\}^{'} = \\ = \{[(\gamma_{a_i}, a_i) \cdot (\gamma_{b_i}, b_i)] \bmod [(m_i - 1)/2]\}^{'} = (a_i^{'} \cdot b_i^{'}) \bmod m_i = \{[\gamma_{a_i}^{'}, (a_i^{'})^*] \cdot [\gamma_{b_i}^{'}, (b_i^{'})^*]\} \bmod m_i = \\ = \{\gamma_i^{'}, [(a_i^{'})^* \cdot (b_i^{'})^*] \bmod m_i\}. \end{cases} \quad (18)$$

для $m_i -$ четного числа получим

$$\begin{cases} (a_i \cdot b_i) \bmod [m_i / 2]\}' = \{[\,(\gamma_{a_i}, a_i) \cdot \\ .(\gamma_{b_i}, b_i)\,] \bmod [m_i / 2]\}' = (a_i' \cdot b_i') \bmod m_i + m_i / 2 = \{[\,\gamma_{a_i}', (a_i')^*] \cdot [\gamma_{b_i}', (b_i')^*]\} \bmod m_i \cdot \\ m_i / 2 = \{\gamma_i', (a_i')^* \cdot (b_i')^*]\} \bmod m_i + m_i / 2; \\ \{(a_i \cdot b_i) \bmod [m_i / 2]\}' = \{[\,(\gamma_{a_i}, a_i) \cdot (\gamma_{b_i}, b_i)] \bmod [m_i / 2]\}' = (a_i' \cdot b_i') \bmod m_i = \\ = \{[\gamma_{a_i}', (a_i')^*] \cdot [\gamma_{b_i}', (b_i')^*]\} \bmod m_i = \{\gamma_i', [\,(a_i')^* \cdot (b_i')^*] \bmod m_i. \end{cases} \quad (19)$$

Выводы. Соотношение (18)÷(19) применяется для модульной реализации операций умножения в КВ, как в положительных, так и в отрицательных числовых диапазонах обработки информации. Полученные соотношения рекомендованы к практическому применению.

Литература

1. *Акушский И. Я.* Машинная арифметика в остаточных классах / *И. Я. Акушский, Д. И. Юдицкий.* – М.: Советское радио, 1968. – 440 с.

2. *Жихарев В. Я.* Методы и средства обработки информации в непозиционной системе счисления в остаточних классах / *В. Я. Жихарев, Я. В. Илюшко, Л. Г. Кравец, В. А. Краснобаев.* – Ж.: Волынь, 2005. – 219 с.

3. *Koshman S. A.* Method of bit-by-bit tabular realization of arithmetic operations in the system of residual classes / *S.A. Koshman, V.I. Barsov, V.A. Krasnobayev, K.V. Yaskova, N.S. Derenko.* – Радіоелектронні і комп'ютерні системи, 2009. – № 5 (39). 44-48 с.

4. *Загуменная К. В.* Математическая модель процесса табличной реализации операций алгебраического умножения в классе вычетов / *С. О Мороз, В. О. Жадан, В. А. Краснобаев В. А.* – Радіоелектронні і комп’ютерні системи, 2012. – № 1(53). – С. 68-74.

МОДУЛЬНЕ МНОЖЕННЯ ЧИСЕЛ В НЕПОЗІЦІЙНІЙ СИСТЕМІ ЧИСЛЕННЯ КЛАССА ЛИШКІВ У ВІД’ЄМНОМУ ЧИСЛОВОМУ ДІАПОЗОНІ

К. В. Загуменна

Анотація **– у даній статті розглянута операція модульного множення у від’ємному числовому діапазоні на основі класу лишків.**

MODULAR MULTIPLICATION OF NUMBERS IN NONPOSITIONAL RADIX RESIDUE CLASS IN A NEGATIV NUMERICAL RANGE

K. Zagymennaya

Summary

In this article the modular multiplication operation in the negative number range based on the residue class.