УДК 681.142

В.А. Краснобаев[1], А.С. Янко[1], С.А. Кошман[2]

[1] *Полтавский национальный технический университет имени Юрия Кондратюка, Полтава*
[2] *Харьковский национальный технический университет сельского хозяйства имени Петра Василенко, Харьков*

МЕТОД ТАБЛИЧНОЙ РЕАЛИЗАЦИИ ОПЕРАЦИИ УМНОЖЕНИЯ В КЛАССЕ ВЫЧЕТОВ

В статье предлагается математическая модель и метод процесса табличной реализации операции умножения двух чисел, представленных в искусственной форме класса вычетов.

Ключевые слова: *класс вычетов, искусственная форма, компьютерная система обработки целочисленных данных, табличная реализация модульной операции умножения.*

Введение

Поиски путей повышения производительности позиционной компьютерной системы обработки целочисленных данных (КСОЦД) реального времени привел к необходимости проведения исследований возможности использования в позиционной двоичной системе счисления (ПСС) табличного метода (табличной машинной арифметики) реализации арифметических операций [1 – 3].

В общем случае табличное операционное устройство (ТОУ) КСОЦД, предназначенное для реализации арифметических операций, которые реализуется в унитарном коде, представляет собой двухвходовое постоянное запоминающее устройство (ПЗУ). Для каждого из входов ПЗУ количество входных шин для l-байтового ($8l$ двоичных разряда) равно 2^{8l}. При этом общее количество логических схем совпадения “И” в узлах ПЗУ (которое в основном и определяет общее количество оборудования табличного ОУ) равно $N_{l\text{ПСС}} = 2^{8l} \times 2^{8l} = 2^{16l}$.

Тенденция развития КСОЦД направлена на увеличение длины разрядной сетки вычислителя. В настоящее время для практических целей используется КСОЦД с длиной разрядной сетки равной l=4 и l=8. В этом случае $N_{4\text{ПСС}}=2^{32}\times2^{32}=2^{64}$ и $N_{8\text{ПСС}}=2^{64}\times2^{64}=2^{128}$. Если учитывать, что, $2^{32}=4294967296$, $2^{64}=18446744073709551616$, а $2^{128}\approx3{,}4\times10^{38}$, то очевидно, что табличный метод реализации арифметических операций в ПСС не применим. Исходя из этого, очевидно, что табличная реализация целочисленных модульных арифметических операций в ПСС практически может быть целесообразна только для значения l=1. Действительно, в этом случае $N_{1\text{ПСС}} = 2^{16} = 65536$, что является приемлемым количеством оборудования ПЗУ для современного развития элементной базы.

Известно, что применение машинной арифметики в непозиционной системе счисления класса вычетов (КВ) позволяет эффективно использовать табличные методы реализации арифметических операций [3]. Это объясняется тем, что КВ, кроме уникального свойства независимости друг от друга остатков по принятой системе оснований, обладает свойством малоразрядности остатков, совокупность которых определяет число. Использование последнего свойства КВ открывает широкие возможности не только в создании табличной машинной арифметики, но и в создании принципиально новой схемной реализации КСОЦД, которая в свою очередь заметно расширяет применение машинной арифметики [4].

При реализации алгоритмов модульной обработки данных, для l-байтовых машинных слов, ПЗУ ТОУ КСОЦД в КВ содержит $N_{1\text{КВ}} = \sum_{i=1}^{n} m_i^2$ схем совпадения И, а для разрядной сетки с l=4 и l=8 соответственно необходимо иметь $N_{4\text{КВ}}$=2397 и $N_{8\text{КВ}}$=13275, что вполне приемлемо при реализации арифметических операций сложения, вычитания и умножения для современной элементной микроэлектронной базы, например ПЛИС.

Результаты ранее проведенных исследований подтверждают важность разработки эффективных методов, моделей и алгоритмов табличной реализации целочисленных модульных операций в КВ.

Цель данной статьи состоит в совершенствовании метода табличной реализации арифметической операции умножения в КВ двух чисел, представленных в целочисленном виде, как для положительного, так и для отрицательного числовых диапазонов обработки данных.

Кратко охарактеризуем основные достоинства метода табличной реализации арифметических операций в КВ.

Во-первых. Использование табличного метода обеспечивает высокое быстродействие выполнения арифметических модульных операций сложения, вычитания и умножения. Результат арифметической операции может быть получен в момент поступле-

ния входных операндов на ТОУ, т.е. практически за один такт работы КСОЦД. Таким образом, время выполнения арифметических операций в КВ сравнимо с тактовой частотой вычислителя, что принципиально невозможно для позиционных КСОЦД, созданных на существующей компьютерной элементной базе.

Во-вторых. Табличное ОУ обеспечивает высокую надежность функционирования КСОЦД. Оно реализуются в виде набора, по числу n модулей m_i КВ, отдельных, независимо функционирующих компьютерных вычислительных трактов в виде компактных ПЗУ. В этом случае весь вычислительный тракт ТОУ, состоящий из совокупности самостоятельно функционирующих ПЗУ, строится по блочному принципу, что улучшает техническое обслуживание КСОЦД.

В-третьих. Простота структуры КСОЦД, функционирующей в КВ. Модульность структуры ТОУ в КВ обуславливает блочную структуру построения всей КСОЦД. Кроме этого, ТОУ в КВ состоит в из однотипных регистров, табличных сумматоров, шифраторов, дешифраторов и однотипных логических элементов И, ИЛИ и НЕ. Это обуславливает унификацию оборудования компьютерного вычислительного тракта ОУ КСОЦД для произвольного модуля $\{m_i\}$, $i = \overline{1,n}$ КВ [2, 5].

Анализ литературных источников. В литературе описаны методы реализации арифметических операций в КВ, основанные на табличном принципе [2, 3].

Поиски путей упрощения структуры табличного ТОУ КСОЦД обусловили необходимость совершенствования метода реализации одной из наиболее трудоемкой в вычислительной техники арифметической операции – умножения. Так, в [3] представлена математическая модель (ММ) процесса табличной реализации операции арифметического модульного умножения двух целых чисел в КВ. Особенностью метода, основанного на реализации данной ММ, является возможность уменьшения количества оборудования КСОЦД счет сокращения на (50-70)% логических элементов “И” в узлах таблицы ПЗУ ТОУ, непосредственно реализующего операцию модульного умножения по произвольному m_i модулю КВ. Уменьшение оборудования ТОУ возможно за счет использования свойств симметрии таблицы реализации $a_i b_i (\mathrm{mod}\, m_i)$ модульной операции арифметического умножения. Покажем это.

В КВ число А представляется в виде совокупности остатков $\{a_i\}$ по n модулям (основаниям) $\{m_i\}$, где: $a_i = A - [A / m_i] \cdot m_i$; $M = \prod_{i=1}^{n} m_i$. В этом случае число А в КВ представляется в виде $A = (a_1, a_2, ..., a_i, ..., a_n)$.

Пусть задана пара чисел

$$A = (a_1, a_2, ..., a_i, ..., a_n) \text{ и}$$

$$B = (b_1, b_2, ..., b_i, ..., b_n)$$

в КВ с попарно взаимно простыми основаниями $m_1, m_2, ..., m_i, ..., m_n)$. В соответствии с правилом $\otimes$ выполнения арифметической операции в КВ каждой паре остатков a_i и b_i ставится в соответствие величина $(a_i \otimes b_i) \bmod m_i$. Таким образом, весь машинный тракт вычислительной операции $(A \otimes B) \bmod M$ в КВ можно представить в виде n независимых однотипных ПЗУ.

Рассмотрим процедуру реализации арифметической операции модульного умножения двух остатков a_i и b_i по модулю m_i соответственно чисел А и В. Таблица значений $a_i b_i (\mathrm{mod}\, m_i)$ результата операции модульного умножения симметрична относительно диагоналей, вертикали и горизонтали, проходящих (для m_i - нечетного числа) между числами $\frac{(m_i - 1)}{2}$ и $\frac{(m_i + 1)}{2}$. Симметричность относительно левой диагонали определяется коммутативностью операции $a_i \cdot b_i = b_i \cdot a_i$ умножения. Симметричность относительно правой диагонали определяется тем, что

$$a_i \cdot b_i \equiv [(m_i - b_i)(m_i - a_i)] \bmod m_i.$$

Симметричность относительно вертикали и горизонтали определяется из условия кратности по модулю m_i суммы симметричных чисел:

$$a_i b_i \equiv [m_i - a_i (m_i - b_i)] \bmod m_i,$$

$$a_i b_i \equiv [m_i - b_i (m_i - a_i)] \bmod m_i.$$

Используя свойства симметрии можно полностью восстановить таблицу значений $a_i b_i (\mathrm{mod}\, m_i)$ модульного умножения только по ее 0,25 части. Отсюда возникает возможность упростить таблицу (уменьшить количество двухвходовых элементов И ПЗУ) модульного умножения. Для решения поставленной задачи необходимо ввести признак, определяющий местоположение входных чисел в каждом из четырех квадрантов таблицы $a_i b_i (\mathrm{mod}\, m_i)$ модульного умножения.

Рассмотрим один из возможных вариантов кодирования входных остатков a_i и b_i таблицы операции модульного умножения по модулю m_i посредством специально введенного кода информационного сжатия данных (КИСД).

В [3] данный код назван кодом табличного умножения. Значения остатков a_i (b_i), лежащие в числовом диапазоне $\left[0, \frac{m_i - 1}{2}\right)$, могут быть закодированы произвольным образом, а значения a_i (b_i),

лежащие в числовом диапазоне $\left[\frac{m_1+1}{2}, m_i\right)$, кодируются, как $m_i - a_i$ ($m_i - b_i$). Для отличия диапазонов нахождения значений остатков a_i и b_i вводится признак γ_a (γ_b) КИСД, определенный следующим образом:

$$\gamma_a\ (\gamma_b) = \begin{cases} 0, \text{если } 0 \le a_i(b_i) \le \dfrac{m_i - 1}{2}, \\ 1, \text{если } \dfrac{m_i + 1}{2} \le a_i(b_i) \le m_i - 1. \end{cases}$$

Метод определения результата операции модульного умножения, посредством введенного КИСД, следующий. Если заданы два остатка чисел А и В в КВ по модулю m_i вида $a_i = (\gamma_a, a_i^*)$, $b_i = (\gamma_b, b_i^*)$, где $0 \le a^*(b^*) \le (m_i - 1)/2$, то для, того чтобы получить произведение этих чисел по модулю m_i, достаточно получить произведение $a_i^* b_i^* (\mathrm{mod}\, m_i)$, и инвертировать его обобщенный признак γ_i в случае, если γ_a отлично от γ_b, т.е. $a_i b_i (\mathrm{mod}\, m_i) = (\gamma_i, a_i^* b_i^* (\mathrm{mod}\, m_i))$, где

$$\gamma_i = \begin{cases} \gamma_i, \text{если } \gamma_a = \gamma_b, \\ \overline{\gamma_i}, \text{если } \gamma_a \ne \gamma_b. \end{cases}$$

Рассмотренный известный метод реализации модульной операций умножения в КВ, основанный на известной ММ [3], позволяют повысить эффективность использования табличной арифметики. Сокращение количества оборудования ПЗУ, составляющих основную часть ТОУ, позволяет улучшить показатели надежности (увеличить вероятность безотказной работы P(t), уменьшить время восстановления $T_в$) и улучшить эксплуатационно-технические показатели (уменьшить массогабаритные характеристика, уменьшить потребляемую мощность и улучшить техническое обслуживание) КСОЦД в КВ.

Процесс табличной реализации двух чисел в КВ в положительном числовом диапазоне представляется в виде:

$$\begin{aligned} &C = A \cdot B (\mathrm{mod} M) = [(a_1, a_2, ..., a_i, ..., a_n) \cdot (b_1, b_2, ..., \\ &, ..., b_i, ..., b_n)] \mathrm{mod} M = [(a_1 \cdot b_1) \mathrm{mod} m_1, (a_2 \cdot b_2) \mathrm{mod} m_2, ..., \\ &, ..., (a_i \cdot b_i) \mathrm{mod} m_i, ..., (a_n \cdot b_n) \mathrm{mod} m_n] = \\ &= \{[(\gamma_{a_1}, a_1^*) \cdot (\gamma_{b_1}, b_1^*)] \mathrm{mod} m_1, [(\gamma_{a_2}, a_2^*) \cdot \\ &\cdot (\gamma_{b_2}, b_2^*)] \mathrm{mod} m_2, ..., [(\gamma_{a_i}, a_i^*) \cdot (\gamma_{b_i}, b_i^*)] \mathrm{mod} m_i, ..., \\ &, ..., [(\gamma_{a_n}, a_n^*) \cdot (\gamma_{b_n}, b_n^*)] \mathrm{mod} m_n\} = \\ &= \{[\gamma_1, (a_1^* \cdot b_1^*) \mathrm{mod} m_1], [\gamma_2, (a_2^* \cdot b_2^*) \mathrm{mod} m_2], ..., \\ &, ..., [\gamma_i, (a_i^* \cdot b_i^*) \mathrm{mod} m_i], ..., [\gamma_n, (a_n^* \cdot b_n^*) \mathrm{mod} m_n]\} = \\ &= (c_1, c_2, ..., c_i, ..., c_n). \end{aligned} \quad (1)$$

При этом признак γ_{a_i} (γ_{b_i}) кода (γ_{a_i}, a_i^*) ((γ_{b_i}, b_i^*)) КИСД остатка $a_i(b_i)$ таблицы модульного умножения для произвольного m_i модуля КВ определяется следующим образом.

Для m_i - четного числа

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

Для m_i - нечетного числа

$$\gamma_{a_i}(\gamma_{b_i}) = \begin{cases} 0, & \text{если } 0 \le a_i(b_i) \le (m_i - 1)/2, \\ 1, & \text{если } (m_i - 1)/2 < a_i\ (b_i) \le m_i - 1. \end{cases} \quad (3)$$

При этом $0 \le a_i(b_i) \le m_i - 1$.

Числовая часть $a_i^*\ (b_i^*)$ КИСД остатка $a_i(b_i)$ определяется следующим образом. Для m_i - четного числа это будет

$$a_i^*\ (b_i^*) = \begin{cases} a_i\ (b_i), & \text{если } 0 \le a_i(b_i) \le m_i/2; \\ \overline{a_i}\ (\overline{b_i}) = m_i - a_i(b_i), & \text{если } m_i/2 < a_i(b_i) \le m_i - 1, \end{cases} \quad (4)$$

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

Для m_i -нечетного числа

$$a_i^*(b_i^*) = \begin{cases} a_i(b_i), & \text{если } 0 \le a_i(b_i) \le (m_i - 1)/2, \\ \overline{a_i}(\overline{b_i}) = m_i - a_i(b_i), & \text{если } (m_i - 1)/2 < a_i(b_i) \le m_i - 1, \end{cases} \quad (5)$$

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

Тогда результат $(a_i \cdot b_i) \mathrm{mod}\, m_i$ модульного умножения определяется в КИСД как $[\gamma_i, (a_i^* \cdot b_i^*) \mathrm{mod}\, m_i]$. В этом случае

$$(a_i \cdot b_i) \mathrm{mod}\, m_i = \begin{cases} (a_i^* \cdot b_i^*) \mathrm{mod}\, m_i, \\ \text{если } (\gamma_{a_i} + \gamma_{b_i}) = 0\ (\mathrm{mod}\, 2); \\ m_i - (a_i^* \cdot b_i^*) \mathrm{mod}\, m_i, \\ \text{если } (\gamma_{a_i} + \gamma_{b_i}) = 1\ (\mathrm{mod}\, 2), \end{cases} \quad (6)$$

при этом $0 \le (a_i^* \cdot b_i^*) \mathrm{mod}\, m_i \le m_i - 1$.

Совокупность выражений (2) – (6) представляет собой ММ процесса табличной реализации модульного арифметического умножения в КВ.

Недостаток рассмотренной ММ состоит в том, что ее использования не дает возможности создать табличный метод реализации операции алгебраического умножения в КВ.

Основная часть

Для создания метода умножения чисел вначале необходимо разработать ММ процесса табличной реализации операции модульного умножения в КВ. Предложенная в [2] ММ не совсем адекватно отображает модель процесса табличной реализации операций алгебраического умножения в КВ. Это обусловлено тем, что данная ММ не учитывает чи-

словой диапазон изменения чисел, представленных в искусственной форме.

Для построения ММ процесса 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 (ИФ) представления чисел в КВ):

$$\begin{cases} A'(B') = \dfrac{M}{2} + |A|\left(|B|\right), \text{ если } A(B) \geq 0, \\ A'(B') = \dfrac{M}{2} - |A|\left(|B|\right), \text{ если } A(B) < 0, \end{cases} \quad (7)$$

т.е. для положительных чисел $A' = \dfrac{M}{2} + |A|$, а для отрицательных – $A' = \dfrac{M}{2} - |A|$.

Для выполнения операции арифметического и алгебраического умножения чисел, представленных в ИФ, необходимо провести синтез ММ реализации этих модульных операций в виде функции

$$(A \cdot B)' = f(A', B'). \quad (8)$$

В общем виде произведение $A' \cdot B'$ двух чисел A' и B' в КВ по модулю M определится как

$$A' \cdot B' = \left[(a_1' \cdot b_1') \bmod m_1, (a_2' \cdot b_2') \bmod m_2, ... \right.$$

$$..., (a_i' \cdot b_i') \bmod m_i, ..., (a_n' \cdot b_n') \bmod m_n, \quad \text{где}$$

$A' = (a_1', a_2', ..., a_i', ..., a_n')$ и $B' = (b_1', b_2', ..., b_i', ..., b_n')$.

В соответствии с определением ИФ чисел в КВ имеем, что

$$\begin{cases} A' = \dfrac{M}{2} + A \\ B' = \dfrac{M}{2} + B \end{cases},$$

а также

$$(AB)' = \frac{M}{2} + A \cdot B. \quad (9)$$

С учётом числовых диапазонов изменения величин A(B) и A′(B′) соотношение (9) можно представить в виде

$$(AB)' = \left(\frac{M}{2} + A \cdot B \right) \bmod M. \quad (10)$$

Проведём следующие числовые преобразования

$$A' \cdot B' = (\frac{M}{2} + A) \cdot (\frac{M}{2} + B) =$$

$$= A \cdot B + \frac{M}{2} \cdot (\frac{M}{2} + A + B). \quad (11)$$

Из выражения (11) следует что $A \cdot B = A' \cdot B' - \dfrac{M}{2} \cdot (\dfrac{M}{2} + A + B)$. Тогда подставляя значение $A \cdot B$ в (10) получим

$$(A \cdot B)' = A' \cdot B' - \frac{M}{2} \cdot (\frac{M}{2} + A + B) + \frac{M}{2}. \quad (12)$$

Для получения ММ (8) в выражении (12) необходимо учесть формулу (7) и то, что $\dfrac{M}{2} = \prod_{i=2}^{n} m_i = (1, 0, ..., 0, ..., 0)$.

Окончательно получим выражение

$$(A \cdot B)' = A' \cdot B' + \frac{M}{2} \cdot (A' + B'). \quad (13)$$

Чтобы получить ММ (8) необходимо рассмотреть два варианта представления выражения (13) [5].

Первый вариант. Числа A' и B' одинаковой чётности (числа A' и B' одновременно чётные ($a_1 = b_1 = 0$) или нечётные ($a_1 = b_1 = 1$)). В этом случае $A' + B' = (0, c_2, ..., c_i, ..., c_n)$. В выражении (13) значение $\dfrac{M}{2} \cdot (A' + B') = (1, 0, ..., 0) \cdot (0, c_1, ..., c_n) = (0, 0, ..., 0)$ будет равно нулю, а аналитическое выражение (13) примет вид

$$(A \cdot B)' = A' \cdot B'. \quad (14)$$

Второй вариант. Числа A' и B' различной чётности (число A' чётное ($a_1' = 0$), а число B' нечётное ($b_1' = 1$) или число A' нечётное ($a_1' = 1$), а число B' чётное ($b_1' = 0$)). В этом случае $A' + B' = (1, c_2, ..., c_i, ..., c_n)$. В выражении (13) значение $\dfrac{M}{2} \cdot (A' + B') = (1, 0, ..., 0) \cdot (1, c_1, ..., c_n) =$ $= (1, 0, ..., 0) = \dfrac{M}{2}$. В этом случае выражение (13) примет вид

$$(A \cdot B)' = A' \cdot B' + \frac{M}{2}. \quad (15)$$

Исходя из вышеизложенного ММ процесса реализации операций арифметического и алгебраического умножения в КВ для произвольного модуля имеет следующий вид

$$(A \cdot B)' = f(A', B') =$$

$$= \begin{cases} A' \cdot B', \text{ если } A' \text{ и } B' \text{ одинаковой четности}, \\ A' \cdot B' + \dfrac{M}{2}, \text{ если } A' \text{ и } B' \text{ различной четности}. \end{cases} \quad (16)$$

Факт наличия в ММ (16) значения $\dfrac{M}{2}$ может быть объяснено следующим образом. В аналитическом выражении (12) действия над числами A' и B' производятся по модулю M, а над числами A и B – по модулю $\dfrac{M}{2}$. В этом случае обрабатываемые числа A и A' лежат в соответствующих числовых интервалах

$$\begin{cases} -\dfrac{M}{2} \leq A \leq \dfrac{(M-1)}{2}, \\ 0 \leq A' \leq M - 1. \end{cases}$$

Значение величины $\frac{M}{2}$ обуславливает числовое различие в реализации ММ (16).

На основании общей ММ (16) реализации операции арифметического и алгебраического умножения чисел, представленных в ИФ, разработаем математическую модель табличной реализации операции арифметического и алгебраического умножения чисел в КВ. В этом случае остатки чисел A и B кодируются следующим образом

$$a'_i = [\gamma'_{a_i}, (a_i')^*], \quad b'_i = [\gamma'_{b_i}, (b_i')^*]. \tag{17}$$

Для m_i - четного числа

$$\gamma'_{a_i}(\gamma'_{b_i}) = \begin{cases} 0, \text{ если } 0 \le a'_i(b'_i) \le m_i/2, \\ 1, \text{ если } m_i/2 < a'_i(b'_i) \le m_i - 1. \end{cases} \tag{18}$$

Для m_i - нечетного числа

$$\gamma'_{a_i}(\gamma'_{b_i}) = \begin{cases} 0, \text{ если } 0 \le a'_i(b'_i) \le (m_i-1)/2, \\ 1, \text{ если } (m_i-1)/2 < a'_i(b'_i) \le m_i - 1. \end{cases} \tag{19}$$

Числовая часть $(a'_i)^*\,[(b'_i)^*]$ КИСД остатка $a_i(b_i)$ соответствующих остатков a_i и b_i определяется следующим образом.

Для m_i – четного числа

$$(a'_i)^*[(b'_i)^*] = \begin{cases} a'_i\,(b'_i), \text{ если } 0 \le a'_i(b'_i) \le m_i/2; \\ \overline{a'_i}\,(\overline{b'_i}) = m_i - a'_i(b'_i), \\ \text{если } m_i/2 < a'_i(b'_i) \le m_i - 1, \end{cases} \tag{20}$$

при этом $0 \le (a'_i)^*\,[(b'_i)^*] \le m_i/2$.

Для m_i – нечетного числа

$$(a'_i)^*[(b'_i)^*] = \begin{cases} a'_i\,(b'_i), \text{ если } 0 \le a'_i(b'_i) \le (m_i-1)/2; \\ \overline{a'_i}\,(\overline{b'_i}) = m_i - a'_i(b'_i), \\ \text{если } (m_i-1)/2 < a'_i(b'_i) \le m_i - 1, \end{cases} \tag{21}$$

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

Результат $(a'_i \cdot b'_i) \bmod m_i$ операции умножения остатков a'_i и b'_i по модулю m_i представляется в КИСД, т.е. в виде $\left\{\gamma'_i, [(a'_i)^*(b'_i)^*] \bmod m_i\right\}$. Тогда

$$(a'_i \cdot b'_i) \bmod m_i = \begin{cases} [(a'_i)^* \cdot (b'_i)^*] \bmod m_i, \\ \text{если } (\gamma'_{a_i} + \gamma'_{b_i}) = 0 \,(\bmod 2); \\ m_i - [(a'_i)^* \cdot (b'_i)^*] \bmod m_i, \\ \text{если } (\gamma'_{a_i} + \gamma'_{b_i}) = 1 \,(\bmod 2), \end{cases} \tag{22}$$

при этом $0 \le [(a'_i)^* \cdot (b'_i)^*] \bmod m_i \le m_i - 1$.

С учётом соотношений (7), (17) ÷ (22), значение $A' \cdot B'$ определяется следующим образом

$$A' \cdot B' = (a'_1, a'_2, ..., a'_i, ..., a'_n) \cdot (b'_1, b'_2, ..., b'_i, ..., b'_n) =$$

$$= \Big[(a'_1 \cdot b'_1) \bmod m_1, (a'_2 \cdot b'_2) \bmod m_2, ..., (a'_i \cdot b'_i) \bmod m_i, ..., (a'_n \cdot b'_n) \bmod m_n \Big] =$$

$$= (\{[\gamma'_{a_1}, (a'_i)^*] \cdot [\gamma'_{b_1}, (b'_1)^*]\} \bmod m_1,$$

$$\{[\gamma'_{a_2}, (a'_2)^*] \cdot [\gamma'_{b_2}, (b'_2)^*]\} \bmod m_2, ...,$$

$$\{[\gamma'_{a_i}, (a'_i)^*] \cdot [\gamma'_{b_i}, (b'_i)^*]\} \bmod m_i, ...,$$

$$\{[\gamma'_{a_n}, (a'_n)^*] \cdot [\gamma'_{b_n}, (b'_n)^*]\} \bmod m_n) =$$

$$= (\{\gamma'_1, [(a'_1)^* \cdot (b'_1)^*] \bmod m_1\},$$

$$\{\gamma'_2, [(a'_2)^* \cdot (b'_2)^*] \bmod m_2\}, ...,$$

$$\{\gamma'_i, [(a'_i)^* \cdot (b'_i)^*] \bmod m_i\}, ...,$$

$$\{\gamma'_n, [(a'_n)^* \cdot (b'_n)^*] \bmod m_n\}). \tag{23}$$

С учетом полученного выражения (23), результат операции $(AB)'$ алгебраического умножения двух чисел в КВ определится в соответствии с выражением (16).

Совокупность соотношений (16), (18)÷(22) представляют собой математическую модель процесса табличной реализации операции алгебраического умножения двух чисел в КВ. На основе этой ММ в статье совершенствован метод табличной реализации арифметической операции умножения за счет возможности выполнения одновременно операций арифметического и алгебраического умножения в классе вычетов (рис. 1).

Рассмотрим в общем виде пример конкретного применения разработанного метода для КВ, заданного основаниями $m_1 = 2$, $m_2 = 3$, $m_3 = 5$, при этом $M = 30$. Объем кодовых слов КВ представлен в табл. 1.

Пусть для чисел $A_{ПСС} = 5$ и $B_{ПСС} = -10$ в ПСС необходимо определить результат операции умножения этих чисел в КВ, представленных в ИФ. Вначале определим ИФ этих чисел в КВ (табл. 1):

$$A'_{КВ} = \frac{M}{2} + A_{КВ} = (1 \,\|\, 0 \,\|\, 0) + (1 \,\|\, 2 \,\|\, 0) = (0 \,\|\, 2 \,\|\, 0),$$

$$B'_{КВ} = \frac{M}{2} - B_{КВ} = (1 \,\|\, 0 \,\|\, 0) - (0 \,\|\, 1 \,\|\, 0) = (1 \,\|\, 2 \,\|\, 0).$$

В результате произведения двух чисел получим, что $C_{КВ} = A'_{КВ} \cdot B'_{КВ} = (0 \,\|\, 2 \,\|\, 0) \cdot (1 \,\|\, 2 \,\|\, 0) = (0 \,\|\, 1 \,\|\, 0)$. Так как числа $A'_{КВ}$ и $B'_{КВ}$ разной чётности ($(a'_1 + b'_1) = 0 + 1 = 1 (\bmod 2)$), то результат C_p операции умножения определится в виде $C_p = C'_{КВ} + \frac{M}{2} = (0 \,\|\, 1 \,\|\, 0) + (1 \,\|\, 0 \,\|\, 0) = (1 \,\|\, 1 \,\|\, 0)$. В ПСС значение C_p равно 25.

Проверка (табл. 1). В соответствии с выражением (7) имеем, что

$$(A_{ПСС} \cdot B_{ПСС})' = \left[\frac{M}{2} + (A_{ПСС} \cdot B_{ПСС})\right] \bmod M =$$

$$= \left[5\cdot(-10)\right] = \left\{15 + \left[5\cdot(-10)\right]\right\} \bmod 30 = (15-50) \bmod 30 =$$

$$= (-35) \bmod 30 = (2\cdot 30 - 35) \bmod 30 = 25 = C_p .$$

Проведенная проверка показала, что применение данного метода позволяет получить достоверный результат операции умножения двух чисел в отрицательном числовом диапазоне.

Для реализации приведенного примера в табличном варианте необходимо дополнительно использовать соотношения (17) – (23).

Таблица 1

Объём кодовых слов в КВ

A(B) в ПСС	A′(B′) в ПСС	A′(B′) в КВ		
		$m_1 = 2$	$m_2 = 3$	$m_3 = 5$
1	*2*	*3*	*4*	*5*
-15	0	0	0	0
-14	1	1	1	1
-13	2	0	2	2
-12	3	1	0	3
-11	4	0	1	4
-10	5	1	2	0
-9	6	0	0	1
-8	7	1	1	2

Окончание табл. 1

1	*2*	*3*	*4*	*5*
-7	8	0	2	3
-6	9	1	0	4
-5	10	0	1	0
-4	11	1	2	1
-3	12	0	0	2
-2	13	1	1	3
-1	14	0	2	4
0	15	1	0	0
1	16	0	1	1
2	17	1	2	2
3	18	0	0	3
4	19	1	1	4
5	20	0	2	0
6	21	1	0	1
7	22	0	1	2
8	23	1	2	3
9	24	0	0	4
10	25	1	1	0
11	26	0	2	1
12	27	1	0	2
13	28	0	1	3
14	29	1	2	4

Задание исходных данных для реализации арифметической операции модульного умножения двух чисел $A_{KB} = (a_1, a_2, ..., a_i, ..., a_n)$ и $B_{KB} = (b_1, b_2, ..., b_i, ..., b_n)$ в КВ.

Кодирование чисел A_{KB} и B_{KB} в виде A'_{KB} и B'_{KB}

$$\begin{cases} A'(B') = \dfrac{M}{2} + |A|\left(|B|\right), \text{ если } A(B) \ge 0, \\ A'(B') = \dfrac{M}{2} - |A|\left(|B|\right), \text{ если } A(B) < 0. \end{cases}$$

$$\begin{cases} -\dfrac{M}{2} \le A \le \dfrac{(M-1)}{2}, \\ 0 \le A' \le M-1. \end{cases}$$

Представление остатков a'_i и b'_i чисел A'_{KB} и B'_{KB} по модулям m_i $(i = \overline{1, n})$ на основе использования КИСД

$$a'_i = [\gamma'_{a_i}, (a_i')^*] \quad b'_i = [\gamma'_{b_i}, (b_i')^*]. \quad \gamma'_{a_i}(\gamma'_{b_i}) = \begin{cases} 0, \text{ если } 0 \le a'_i(b'_i) \le m_i/2, \\ 1, \text{ если } m_i/2 < a'_i(b'_i) \le m_i - 1. \end{cases}$$

$$\gamma'_{a_i}(\gamma'_{b_i}) = \begin{cases} 0, \text{ если } 0 \le a'_i(b'_i) \le (m_i - 1)/2, \\ 1, \text{ если } (m_i - 1)/2 < a'_i(b'_i) \le m_i - 1. \end{cases}$$

Для m_i – четного числа $(a'_i)^*[(b'_i)^*] = \begin{cases} a'_i\ (b'_i), \text{ если } 0 \le a'_i(b'_i) \le m_i/2; \\ \overline{a'_i}\ (\overline{b'_i}) = m_i - a'_i(b'_i), \text{ если } m_i/2 < a'_i(b'_i) \le m_i - 1, \end{cases}$ при этом

$$0 \le (a'_i)^*\ [(b'_i)^*] \le m_i/2.$$

Для m_i – нечетного числа $(a'_i)^*[(b'_i)^*] = \begin{cases} a'_i\ (b'_i), \text{ если } 0 \le a'_i(b'_i) \le (m_i - 1)/2; \\ \overline{a'_i}\ (\overline{b'_i}) = m_i - a'_i(b'_i), \text{ если } (m_i - 1)/2 < a'_i(b'_i) \le m_i - 1. \end{cases}$

Рис. 1. Метод табличной реализации операции умножения двух чисел в КВ (блоки 1 – 3)

Определение результата $(a'_i \cdot b'_i) \bmod m_i \quad (i = \overline{1, n})$ операции модульного умножения в виде

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

Определение результата операции модульного умножения $(A'_{KB} \cdot B'_{KB}) \bmod M$

$$A' \cdot B' = (a'_1, a'_2, ..., a'_i, ..., a'_n) \cdot (b'_1, b'_2, ..., b'_i, ..., b'_n) =$$

$$= \left[(a'_1 \cdot b'_1) \bmod m_1, (a'_2 \cdot b'_2) \bmod m_2, ..., (a'_i \cdot b'_i) \bmod m_i, ..., (a'_n \cdot b'_n) \bmod m_n \right] =$$

$$= (\{[\gamma'_{a_1}, (a'_i)^*] \cdot [\gamma'_{b_1}, (b'_1)^*]\} \bmod m_1, \{[\gamma'_{a_2}, (a'_2)^*] \cdot [\gamma'_{b_2}, (b'_2)^*]\} \bmod m_2, ...,$$

$$\{[\gamma'_{a_i}, (a'_i)^*] \cdot [\gamma'_{b_i}, (b'_i)^*]\} \bmod m_i, ..., \{[\gamma'_{a_n}, (a'_n)^*] \cdot [\gamma'_{b_n}, (b'_n)^*]\} \bmod m_n) =$$

$$= (\{\gamma'_1, [(a'_1)^* \cdot (b'_1)^*] \bmod m_1\}, \{\gamma'_2, [(a'_2)^* \cdot (b'_2)^*] \bmod m_2\}, ...,$$

$$\{\gamma'_i, [(a'_i)^* \cdot (b'_i)^*] \bmod m_i\}, ..., \{\gamma'_n, [(a'_n)^* \cdot (b'_n)^*] \bmod m_n\}).$$

В соответствии с математической моделью $(A \cdot B)' = f(A', B') = \begin{cases} A' \cdot B', \text{ если } A' \text{ и } B' \text{ одинаковой четности,} \\ A' \cdot B' + \dfrac{M}{2}, \text{ если } A' \text{ и } B' \text{ различной четности} \end{cases}$

определение результата операции $(A_{KB} \cdot B_{KB})'$ алгебраического умножения двух чисел A_{KB} и B_{KB} в КВ.

Рис. 1. Метод табличной реализации операции умножения двух чисел в КВ (окончание, блоки 4 – 6)

Выводы

В статье разработана математическая модель операции умножения двух чисел, на основе которой усовершенствован метод процесса табличной обработки данных для выполнения целочисленных модульных операций арифметического и алгебраического умножения двух чисел, представленных в КВ.

В дальнейшем усовершенствованный метод умножения двух чисел может быть положена в основу разработки обобщенного метода быстрой обработки целочисленных операций сложения, вычитания и умножения в КВ.

Список литературы

1. Сиора А.А. Отказоустойчивые системы с версионно-информационной избыточностью в АСУ ТП: Монография / А.А. Сиора, В.А. Краснобаев, В.С. Харченко. – Х.: МОН, НАУ им. Н.Е. Жуковского (ХАИ), 2009. – 320 с.

2. Материалы Международной научно-технической конференции "50 лет модулярной арифметике". МИЭТ, г. Зеленоград. Моск. обл. 23-25 ноября 2005г.

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

4. Krasnobayev V.A. Method for Realization of Transformations in Public-Key Cryptography / V.A. Krasnobayev // Telecommunications and Radio Engineering (USA). – 2007. – Vol. 66, Issue 17. – P. 1559-1572.

5. Кошман С.О. Диверсність табличних методів реалізації арифметичних операцій у системі залишкових класів / С.О. Кошман, В.І. Барсов, В.А. Краснобаєв // Вісник ХНТУСГ. – 2008. – Вип. 73. – Т. 2. – С. 70-72.

Поступила в редколлегию 17.02.2014

Рецензент: д-р техн. наук, с.н.с. Г.А. Кучук, Харьковский университет Воздушных Сил им. И. Кожедуба, Харьков.

МЕТОД ТАБЛИЧНОЇ РЕАЛІЗАЦІЇ ОПЕРАЦІЇ МНОЖЕННЯ У КЛАСУ ЛИШКІВ

В.А. Краснобаєв, А.С. Янко, С.О. Кошман

У статті пропонується математична модель і метод процесу табличної реалізації операції множення двох чисел, що представлені у штучній формі класу лишків.

***Ключові слова**: клас лишків, штучна форма, комп'ютерна система обробки цілочисельних даних, таблична реалізація модульної операції множення.*

METHOD OF THF TABULAR IMPLEMENTATION OPERATION OF MULTIPLICATION IN THE RESIDUE CLASS

V.A. Krasnobaeyv, A.S. Yanko, S.A. Koshman

The paper proposes a mathematical model and method of the process of table implementation of operation of multiplication of two numbers which represented by the simulated form of residue class.

***Keywords**: residue class, simulated form, the computer system processing integer data, tabular implementation of modular operation of multiplication.*