УДК 681.142

В. А. КРАСНОБАЕВ[1], А. С. ЯНКО[1], С. А. КОШМАН[2]

[1] *Полтавский национальный технический университет им. Юрия Кондратюка, Украина*

[2] *Харьковский национальный технический университет сельского хозяйства им. Петра Василенка, Украина*

МЕТОД ВОЗВЕДЕНИЯ ОСТАТКОВ ЦЕЛЫХ ЧИСЕЛ ПО ПРОИЗВОЛЬНОМУ МОДУЛЮ СИСТЕМЫ ОСТАТОЧНЫХ КЛАССОВ В СТЕПЕНЬ НАТУРАЛЬНОГО ЧИСЛА

На основе существующей математической модели возведения в квадрат остатков целых чисел по модулю класса вычетов в статье разработаны математическая модель и метод возведения остатков целых чисел по произвольному модулю системы остаточных классов (СОК) в степень натурального числа. Приведены примеры конкретной реализации представленного метода возведения остатков целых чисел в степень. Предложенный метод возведения остатков целых чисел в степень натурального числа может быть использован в компьютерной системе быстрой обработки целочисленных данных, функционирующей в СОК, а также в компьютерных вычислительных устройствах, функционирующих в обычной позиционной двоичной системе счисления.

Ключевые слова: *непозиционная система счисления в остаточных классах, позиционная двоичная система счисления, компьютерная система быстрой обработки целочисленных данных, возведения остатков целых чисел в степень натурального числа.*

Введение

Характерной чертой современного информационного общества является смещение вектора значимости интересов государства в сторону разработки и использования новых прогрессивных информационных технологий, которые в последние годы являются составляющими стратегических ресурсов любой страны. Достижение высоких экономических и социальных результатов, повышение доли Украины в мировой экономической системе в значительной мере зависит от масштабов и темпов проведения глобальной информатизации всего общества. Одним из наиболее важных направлений развития научно-технического прогресса в сфере создания и использования новых информационных технологий является развитие и внедрение эффективных компьютерных систем и компонентов вычислительной техники [1, 2].

Возрастающая сложность существующих задач обработки целочисленных данных опережает темпы повышения вычислительной мощности существующих универсальных позиционных ЭВМ. В этом аспекте основным направлением совершенствования вычислительных устройств в позиционных системах счисления (ПСС) является удовлетворение требования неуклонного роста производительности реализации целочисленных вычислений. Проводимые теоретические, экспериментальные и промышленные исследования и разработки в этом направлении позволили обосновать перспективное направление роста производительности реализации целочисленных вычислений в ПСС, основанное на принципе распараллеливания вычислений.

Применение основных методов повышения производительности в ПСС не во всех случаях позволяет повысить производительность вычислений. Сфера применения их ограничивается классом решаемых задач. Кроме этого, сам процесс искусственного расчленения алгоритма, определение и выделение независимых вычислительных ветвей требует больших трудозатрат, причем, не всегда возможно распараллеливание произвольных алгоритмов вообще. Отметим, что все существующие методы повышения производительности в ПСС обладают общим недостатком: невозможность максимально распараллелить решаемые алгоритмы на уровне элементарных операций сложения, вычитания и умножения.

Одним из возможных направлений в решении задачи повышения производительности целочисленных вычислений является переход к машинной арифметике с нетрадиционным представлением операндов. В настоящее время из множества нетрадиционных машинных арифметик для практического применения в компьютерных системах предлагаются следующие: модулярная арифметика в системе остаточных классов (СОК) или как ее еще называют класс вычетов (КВ); коды Фибоначчи; биноминальная система счисления; модулярная комплексная

арифметика Гаусса; арифметика в кольце полиномов.

Из перечисленных нетрадиционных машинных арифметик, для реализации целочисленных арифметических операций в действительной числовой области вычислений, наибольшее практическое применение получила непозиционная система счисления в СОК.

Обзор литературных источников

Существует ряд реальных технических разработок компьютерных систем обработки целочисленных данных (КСОЦД) в СОК. В 60-х годах прошлого столетия коллектив ученых и инженеров, возглавляемый доктором технических наук, профессором Д. И. Юдицким, создал первую в мире ЭВМ Т-340А, функционирующую в СОК, для штатного полигонного варианта радиолокационной станции "Дунай-3УП" системы А-35 противоракетной обороны СССР.

В семидесятых годах прошлого столетия, в связи с научными разработками таких ЭВМ в СОК, как А-340А, К-340А, Т-340А, "Алмаз", система 5Э53 и ЭВМ "Вычет" и их массовым производством на предприятиях промышленности СССР, в мире интенсивно проводились серьезные научные исследования в области модулярной арифметики. Появилось много публикаций на эту тему в открытой печати, в том числе и фундаментальных монографий [1, 3].

Кроме этого за последние годы в СОК были разработаны следующие КСОЦД: бортовой компьютер управления авиационным двигателем, разработанный Б. С. Гаспаром (СССР); модулярные цифровые фильтры, разработанные Е. К. Лебедевым (СССР); бортовой компьютер Star (США); специализированные процессоры ДПФ (США, Южная Корея); ряд военных специализированных бортовых компьютеров (США, Япония); специализированные процессоры цифровой обработки сигналов (США); компьютеры Sprint для робототехники (США, Япония); в 2011 году, в рамках программы "Университетский кластер" АН РФ, в Вятском государственном университете для решения проблемы высокоточных и быстрых целочисленных матричных вычислений, на основе табличного метода выполнения арифметических операций, был создан, прошел испытание и функционирует вычислительный кластер в КВ; в 2013 году в китайской компании "Tpv Display Technology (Wuhan, China) Co., Ltd" при разработке и внедрении беспроводной сенсорной сети системы контроля состояния промышленного оборудования при изготовлении мониторов; на предприятии ТОВ "Релком-Поділля" при разработке системы видеонаблюдения на основе беспроводных мультимедийных сенсорных сетей; в корпорации "Cypress Semiconductors" при разработке аппаратно-программного обеспечения для модулей CY8CKIT-050 PsoC 5 и CyFi (CYRF7936), которые могут быть использованы в беспроводных сенсорных сетях.

Результаты исследований в области создания КСОЦД известных авторов показали, что использование СОК в качестве системы счисления компьютерных вычислительных средств может существенно повысить производительность решения задач определенного класса.

Однако необходимо отметить, что существует многочисленный класс алгоритмов и задач (задачи маршрутизации, оптимизационные задачи, вычислительные задачи и пр.), где кроме выполнения целочисленных арифметических операций в СОК существует операция возведения остатков целых чисел в степень натурального числа. Значительное время выполнения этой операций в отрицательном числовом диапазоне существенно снижает общую эффективность использования КВ в качестве системы счисления КСОЦД.

Таким образом, актуальны и практически важны исследования, посвященные разработке метода быстрой реализации операции возведения остатков целых чисел по произвольному модулю СОК в степень натурального числа.

Результаты анализа последних исследований и публикаций, в которых начато решение данной задачи, показал следующее.

В [5] разработаны методы и алгоритмы возведения целых чисел, представленных в СОК, в степень натурального числа. Однако они не всегда применимы для их реализации в отрицательном числовом диапазоне на основе табличного принципа обработки данных в СОК.

В [6] представлен метод возведения чисел в квадрат по модулю СОК. Недостаток метода - невозможность возведения целых чисел, представленных в СОК, в произвольную степень натурального числа на основе табличного принципа обработки данных.

Недостатком метода, описанного в [8], является невозможность возведения целых чисел в СОК в произвольную степень натурального числа на основе табличного принципа обработки данных в классе вычетов.

Цель статьи – разработка метода быстрой реализации операции возведения остатков целых чисел по произвольному модулю СОК в степень натурального числа, как в положительном, так и отрицательном числовых диапазонах на основе табличного принципа обработки данных.

Основная часть

Известно, что по виду исходного числа $A_{СОК} = (a_1 \| a_2 \| ... \| a_{i-1} \| a_i \| a_{i+1} \| ... \| a_n)$, представленного в СОК, нельзя определить его принадлежность к положительному или отрицательному числовым диапазонам. Существует два варианта представления чисел в СОК, как в положительном, так и в отрицательном числовых диапазонах.

Первый вариант. Исходное число в СОК $A_{СОК} = (a_1 \| a_2 \| ... \| a_{i-1} \| a_i \| a_{i+1} \| ... \| a_n)$ имеет дополнительно по два (или по одному) знаковых разряда Ω_{+A} и Ω_{-A}, где

$$\Omega_{+A_{СОК}} = \begin{cases} 1, \text{если } A_{СОК} > 0, \\ 0, \text{если } A_{СОК} < 0; \end{cases}$$

$$\Omega_{-A_{СОК}} = \begin{cases} 0, \text{если } A_{СОК} > 0, \\ 1, \text{если } A_{СОК} < 0. \end{cases}$$

В этом случае исходное число в СОК представится в виде $A_{СОК} = [\Omega_{+A_{СОК}}; \Omega_{-A_{СОК}}; (a_1 \| \| a_2 \| ... \| a_{i-1} \| a_i \| a_{i+1} \| ... \| a_n)]$. В случае если $A_{СОК} = 0$, знаковые разряды равны $\Omega_{+A} = \Omega_{-A} = 0$.

При данном варианте введения знака числа имеется существенный недостаток: техническая и временная сложность формирования знака результата позиционных и непозиционных операций в СОК [5].

Второй вариант. Для реализации процесса выполнения операции возведения остатков целых чисел по произвольному модулю СОК в степень натурального числа, как в положительном, так и в отрицательном числовых диапазонах, предполагается представить исходное число $A_{СОК} = (a_1 \| a_2 \| ... \| ... \| a_{i-1} \| a_i \| a_{i+1} \| ... \| a_n)$ в искусственной A' форме (ИФ) [3]:

$$\begin{cases} A'_{СОК} = \frac{M}{2} + |A_{СОК}|, \text{если } A \geq 0, \\ A'_{СОК} = \frac{M}{2} - |A_{СОК}|, \text{если } A < 0, \end{cases}$$

т. е. для положительных чисел имеем $A'_{СОК} = \frac{M}{2} + |A_{СОК}|$, а для отрицательных – $A'_{СОК} = \frac{M}{2} - |A_{СОК}|$, где $M = \prod_{i=1}^{n} m_i$.

В настоящее время отсутствует эффективный метод быстрого возведения остатков целых чисел, представленных в СОК, по произвольному модулю в степень натурального числа, как в положительном, так и отрицательном числовых диапазонах на основе их представления в ИФ. Таким образом, актуальны исследования в области создания методов и алгоритмов быстрого возведения остатков целых чисел, представленных в СОК, по произвольному модулю в степень натурального числа, как в положительном, так и отрицательном числовых диапазонах на основе их представления в ИФ.

Чтобы разработать данный метод вначале необходимо синтезировать математическую модель (ММ) $(A^k_{СОК})' = f(A'_{СОК})$ процесса возведения остатков целых чисел $A_{СОК}$, представленных в СОК, по произвольному модулю в степень k натурального числа. Т. е. надо получить аналитическое выражение, которое определяет зависимость результата $A^k_{СОК}$ операции возведения числа $A_{СОК}$ в СОК в степень k, и представленного в ИФ, от значения числа $A'_{СОК}$, непосредственно представленного в ИФ.

В начале, в качестве примера, определим ММ $(A^k_{СОК})' = f(A'_{СОК})$ для значений $k = 2$ и $m_1 = 2$. В этом случае в СОК имеем, что

$$M = \prod_{i=1}^{n} m_i = (0 \| 0 \| ... \| 0 \| 0 \| 0 \| ... \| 0) \quad (1)$$

и

$$\frac{M}{2} = \prod_{i=2}^{n} m_i = (1 \| 0 \| ... \| 0 \| ... \| 0), \quad (2)$$

где n - количество оснований СОК.

В соответствии с определением ИФ чисел в СОК имеем, что

$$\begin{cases} A'_{СОК} = \frac{M}{2} + A_{СОК}, \end{cases}$$

а также

$$(A^k_{СОК})' = \frac{M}{2} + A^k_{СОК}. \quad (3)$$

С учётом числовых диапазонов изменения величин $A_{СОК}$ и $A'_{СОК}$ соотношение (3) можно представить в виде

$$(A^k_{СОК})' = \left(\frac{M}{2} + A^k_{СОК} \right) \bmod M. \quad (4)$$

Проведём следующие числовые преобразования

$$(A'_{СОК})^2 = A'_{СОК} \cdot A'_{СОК} = (\frac{M}{2} + A_{СОК}) \cdot (\frac{M}{2} + A_{СОК}) = \frac{M}{2} \cdot \frac{M}{2} + M \cdot \frac{M}{2} + M \cdot \frac{M}{2} + A^2_{СОК} = A^2_{СОК} + A_{СОК} \cdot M + \frac{M}{2} \cdot \frac{M}{2}. \quad (5)$$

Учитывая выражение (1) и (2) получим, что

$$A_{СОК} \cdot M = (a_1 \| a_2 \| ... \| a_{i-1} \| a_i \| a_{i+1} \| ... \| a_n) \times \times (0 \| 0 \| ... \| 0 \| 0 \| 0 \| ... \| 0) = (0 \| 0 \| ... \| 0 \| 0 \| 0 \| ... \| 0) = 0$$

и $$\frac{M}{2}\cdot\frac{M}{2}=(1\,\|\,0\,\|\,...\,\|\,0\,\|\,0\,\|\,0\,\|\,...\,\|\,0)\times$$
$$\times(1\,\|\,0\,\|\,...\,\|\,0\,\|\,0\,\|\,0\,\|\,...\,\|\,0)=$$
$$=(1\,\|\,0\,\|\,...\,\|\,0\,\|\,0\,\|\,0\,\|\,...\,\|\,0)=\frac{M}{2}.$$

В этом случае выражение (5) представится в виде

$$(A'_{COK})^2=A^2_{COK}+\frac{M}{2}. \qquad (6)$$

С другой стороны

$$(A'_{COK})^2=\frac{M}{2}+A^2_{COK},$$

$$A^2_{COK}=(A'_{COK})^2-\frac{M}{2}. \qquad (7)$$

Подставляя значение A^2_{COK} (7) в соотношение (6) получим, что

$$(A'_{COK})^2=(A^2_{COK})'-\frac{M}{2}+\frac{M}{2}, \text{ или}$$

$$(A'_{COK})^2=(A^2_{COK})'. \qquad (8)$$

Аналитическое соотношение (8) является ММ процесса возведения целых чисел в квадрат по модулю СОК. Аналогичным образом можно получить ММ для общего случая, когда $k>2$ в виде

$$(A^k_{COK})'=(A'_{COK})^k. \qquad (9)$$

В этом случае, очевидно, что $(A^k_{COK})'=$ $=(A^{k-1}_{COK})'\cdot A'_{COK}$.

Формулу (9) можно представить в виде

$$[a_1^k(\bmod m_1)\,\|\,a_2^k(\bmod m_2)\,\|\,...$$
$$...\,\|\,a_i^k(\bmod m_i)\,\|\,...\,\|\,a_n^k(\bmod m_1)]'=$$
$$=(a_1'\,\|\,a_2'\,\|\,...\,\|\,a'_{i-1}\,\|\,a'_i\,\|\,a'_{i+1}\,\|\,...\,\|\,a'_n)^k. \qquad (10)$$

Обрабатываемые числа A^k_{COK} и $(A'_{COK})^k$ лежат в соответствующих числовых интервалах

$$\begin{cases}-\frac{M}{2}\le A^k_{COK}\le\frac{(M-1)}{2},\\ 0\le(A'_{COK})^k\le M-1.\end{cases}$$

На основании ММ (10) реализации операции возведения в степень остатков целых чисел, рассмотрим метод табличной реализации операции возведения остатков целых чисел по произвольному модулю СОК в степень натурального числа, как в положительном, так и отрицательном числовых диапазонах.

В случае табличной реализации операции возведения остатков целых чисел по произвольному модулю остатки числа A'_{COK} кодируются кодом табличного умножения (КТУ) следующим образом [3, 7-12]

$$a'_i=[\gamma'_{a_i},(a'_i)^*].$$

Признак γ'_{a_i} КТУ определяется следующим образом.

Для m_i - четного числа

$$\gamma'_{a_i}=\begin{cases}0, \text{ если } 0\le a'_i\le m_i/2,\\ 1, \text{ если } m_i/2<a'_i\le m_i-1.\end{cases} \qquad (11)$$

Для m_i - нечетного числа

$$\gamma'_{a_i}=\begin{cases}0, \text{ если } 0\le a'_i\le (m_i-1)/2,\\ 1, \text{ если } (m_i-1)/2<a'_i\le m_i-1.\end{cases} \qquad (12)$$

Числовая часть $(a'_i)^*$ КТУ остатка a'_i определяется следующим образом.

Для m_i- четного числа

$$(a'_i)^*=\begin{cases}a'_i, \text{ если } 0\le a'_i\le m_i/2;\\ \overline{a'_i}=m_i-a'_i, \text{ если } m_i/2<a'_i\le m_i-1,\end{cases} \qquad (13)$$

при этом $0\le(a'_i)^*\le m_i/2$.

Для m_i- нечетного числа

$$(a'_i)^*=\begin{cases}a'_i, \text{ если } 0\le a'_i\le (m_i-1)/2;\\ \overline{a'_i}=m_i-a'_i, \text{ если } (m_i-1)/2<a'_i\le m_i-1,\end{cases} \qquad (14)$$

при этом $0\le(a'_i)^*\le(m_i-1)/2$.

Результат $(a'_i\cdot a'_i)\bmod m_i$ операции умножения остатка a'_i сам на себя по модулю m_i представляется в КТУ, т.е. в виде $\left\{\gamma'_i,[(a'_i)^*(a'_i)^*]\bmod m_i\right\}$. Тогда выполняется условие $(\gamma'_{a_i}+\gamma'_{a_i})=0\,(\bmod 2)$. В этом случае

$$(a'_i\cdot a'_i)\bmod m_i=[(a'_i)^*\cdot(a'_i)^*]\bmod m_i, \qquad (15)$$

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

С учётом соотношений (8), $(11)\div(15)$, значение $(A'_{COK})^2=A'_{COK}\cdot A'_{COK}$ определяется следующим образом:

$$(A'_{COK})^2=A'_{COK}\cdot A'_{COK}=(a_1\,\|\,a_2\,\|\,...\,\|\,a_{i-1}\,\|\,a_i\,\|$$
$$\|\,a_{i+1}\,\|\,...\,\|\,a_n)\times(a_1\,\|\,a_2\,\|\,...\,\|\,a_{i-1}\,\|\,a_i\,\|\,a_{i+1}\,\|\,...\,\|\,a_n)=$$
$$=\left[(a'_1\cdot a'_1)\bmod m_1\,\|\,(a'_2\cdot a'_2)\bmod m_2\,\|\,...\right.$$
$$\left.\|\,(a'_i\cdot a'_i)\bmod m_i\,\|\,...\,\|\,(a'_n\cdot a'_n)\bmod m_n\right]=$$
$$=(\,\{[\,\gamma'_{a_1},(a'_i)^*]\cdot[\gamma'_{a_1},(a'_i)^*]\}\bmod m_1\,\|$$
$$\|\,\{[\,\gamma'_{a_2},(a'_2)^*]\cdot[\,\gamma'_{a_2},(a'_2)^*]\}\bmod m_2\,\|\,...$$
$$...\,\|\,\{[\gamma'_{a_i},(a'_i)^*]\cdot[\gamma'_{a_i},(a'_i)^*]\}\bmod m_i\,\|\,...$$
$$...\,\|\,\{[\gamma'_{a_n},(a'_n)^*]\cdot[\gamma'_{a_n},(a'_n)^*]\}\bmod m_n)=$$
$$=(\,\{\gamma'_1,[\,(a'_1)^*\cdot(a'_1)^*]\bmod m_1\}\,\|$$

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

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

$$\ldots \| \{\gamma'_n, [(a'_n)^* \cdot (a'_n)^*] \bmod m_n\}). \quad (16)$$

С учетом полученного выражения (16), результат операции $(A'_{COK})^k$ возведения остатков целых чисел по произвольному модулю КВ в степень натурального числа определяется путем умножения предыдущего результата $(A'_{COK})^{k-1}$ операции возведения чисел на значение A'_{COK}.

На основании разработанной ММ (9), (10) и на основе использования табличного принципа реализации модульной операции умножения, в статье разработан метод быстрого возведения остатков целых чисел по произвольному модулю СОК в степень натурального числа, как в положительном, так и отрицательном числовых диапазонах. На рис. 1 приведён метод быстрого возведения остатков целых чисел по произвольному модулю СОК для случая $k = 2$.

Рассмотрим пример конкретного применения разработанного метода для СОК, заданной основаниями $m_1 = 2$, $m_2 = 5$, $m_3 = 7$, при этом $M = 70$. Объем кодовых слов A_{COK} в СОК представлен в таблице 1. В таблице 2 представлен объем кодовых слов A' в ИФ.

Таблица 1

Объем кодовых слов A_{COK} в СОК

A в ПСС	A_{COK} в СОК			A в ПСС	A_{COK} в СОК		
	$m_1 = 2$	$m_1 = 5$	$m_1 = 7$		$m_1 = 2$	$m_1 = 5$	$m_1 = 7$
0	0	0	0	35	1	0	0
1	1	1	1	36	0	1	1
2	0	2	2	37	1	2	2
3	1	3	3	38	0	3	3
4	0	4	4	39	1	4	4
5	1	0	5	40	0	0	5
6	0	1	6	41	1	1	6
7	1	2	0	42	0	2	0
8	0	3	1	43	1	3	1
9	1	4	2	44	0	4	2
10	0	0	3	45	1	0	3
11	1	1	4	46	0	1	4
12	0	2	5	47	1	2	5
13	1	3	6	48	0	3	6
14	0	4	0	49	1	4	0
15	1	0	1	50	0	0	1
16	0	1	2	51	1	1	2
17	1	2	3	52	0	2	3
18	0	3	4	53	1	3	4
19	1	4	5	54	0	4	5
20	0	0	6	55	1	0	6
21	1	1	0	56	0	1	0
22	0	2	1	57	1	2	1
23	1	3	2	58	0	3	2
24	0	4	3	59	1	4	3
25	1	0	4	60	0	0	4
26	0	1	5	61	1	1	5
27	1	2	6	62	0	2	6
28	0	3	0	63	1	3	0
29	1	4	1	64	0	4	1
30	0	0	2	65	1	0	2
31	1	1	3	66	0	1	3
32	0	2	4	67	1	2	4
33	1	3	5	68	0	3	5
34	0	4	6	69	1	4	6

Задание исходных данных для реализации метода возведения остатков a_i целого числа $A_{COK} = (a_1 \| a_2 \| \ldots \| a_{i-1} \| a_i \| a_{i+1} \| \ldots \| a_n)$ по произвольному модулю m_i $(i = \overline{1, n})$ СОК в степень k.

Кодирование исходных чисел A_{COK} в кодовые слова, представленные в искусственной форме вида A'_{COK}

$$\begin{cases} A'_{COK} = \dfrac{M}{2} + |A_{COK}|, \text{если } A_{COK} \geq 0, \\ A'_{COK} = \dfrac{M}{2} - |A_{COK}|, \text{если } A_{COK} < 0. \end{cases} \quad \begin{cases} -\dfrac{M}{2} \leq A_{COK} \leq \dfrac{(M-1)}{2}, \\ 0 \leq A'_{COK} \leq M-1. \end{cases} \quad \begin{cases} (A^k_{COK})' = \dfrac{M}{2} + \left|A^k_{COK}\right|, \text{если } A^k_{COK} \geq 0, \\ (A^k_{COK})' = \dfrac{M}{2} - \left|A^k_{COK}\right|, \text{если } A^k_{COK} < 0. \end{cases}$$

Представление остатков a'_i числа $A'_{COK} = (a_1' \| a_2' \| \ldots \| a'_{i-1} \| a'_i \| a'_{i+1} \| \ldots \| a'_n)$ в искусственной форме по модулям m_i $(i = \overline{1, n})$ на основе использования кода табличного умножения

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

$$\text{Для } m_i - \text{ четного числа } (a'_i)^* = \begin{cases} a'_i, \text{ если } 0 \leq a'_i \leq m_i / 2; \\ \overline{a'_i} = m_i - a'_i, \text{если } m_i / 2 < a'_i \leq m_i - 1, \end{cases}$$

$$\text{Для } m_i - \text{ нечетного числа } (a'_i)^* = \begin{cases} a'_i, \text{ если } 0 \leq a'_i \leq (m_i - 1)/2; \\ \overline{a'_i} = m_i - a'_i, \text{если } (m_i - 1)/2 < a'_i \leq m_i - 1. \end{cases} \quad \text{При этом } 0 \leq (a'_i)^* \leq m_i / 2.$$

Определение результата $(a'_i)^2 = (a'_i \cdot a'_i) \bmod m_i$ $(i = \overline{1, n})$ операции модульного умножения в виде $\gamma'_i, [(a'_i) \cdot (a'_i)] \bmod m_i$, при этом

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

Определение результата операции $\left[(A'_{COK})^{k-1} \cdot A'_{COK}\right] \bmod M = \left\{\left[(a'_1)^{k-1}\right] \bmod m_1 \| \left[(a'_2)^{k-1}\right] \bmod m_2 \| \ldots \right.$

$\left. \ldots \| \left[(a'_2)^{k-1}\right] \bmod m_i \| \ldots \| \left[(a'_n)^{k-1}\right] \bmod m_n \right\} \cdot (a_1' \| a_2' \| \ldots \| a'_{i-1} \| a'_i \| a'_{i+1} \| \ldots \| a'_n)$ возведения остатков a_i целого числа $A_{COK} = (a_1 \| a_2 \| \ldots \| a_{i-1} \| a_i \| a_{i+1} \| \ldots \| a_n)$ по произвольному модулю m_i $(i = \overline{1, n})$ СОК в степень k натурального числа

$$(A')^2 = (A'_{COK} \cdot A'_{COK}) \bmod M = A'_{COK} \cdot A'_{COK} = (a_1' \| a_2' \| \ldots \| a'_{i-1} \| a'_i \| a'_{i+1} \| \ldots \| a'_n) \cdot (a_1' \| a_2' \| \ldots \| a'_{i-1} \| \| a'_i \| a'_{i+1} \| \ldots \| a'_n) == \left[(a'_1 \cdot a'_1) \bmod m_1 \| (a'_2 \cdot a'_2) \bmod m_2 \| \ldots \| (a'_i \cdot a'_i) \bmod m_i \| \ldots \| (a'_n \cdot a'_n) \bmod m_n\right] =$$

$$= (\{[\gamma'_{a_1}, (a'_1)^*] \cdot [\gamma'_{a_1}, (a'_1)^*]\} \bmod m_1 \| \{[\gamma'_{a_2}, (a'_2)^*] \cdot [\gamma'_{a_2}, (a'_2)^*]\} \bmod m_2 \| \ldots$$

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

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

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

В соответствии с математической моделью имеем

$$\left[a_1^k (\bmod m_1) \| a_2^k (\bmod m_2) \| \ldots \| a_i^k (\bmod m_i) \| \ldots \| a_n^k (\bmod m_1)\right]' = (a_1' \| a_2' \| \ldots \| a'_{i-1} \| a'_i \| a'_{i+1} \| \ldots \| a'_n)^k$$

процесса возведения остатков целых чисел по произвольному модулю, реализуется операция

$$\left[(A'_{COK})^{k-1} \cdot A'_{COK}\right] \bmod M = \left\{\left[(a'_1)^{k-1}\right] \bmod m_1 \| \left[(a'_2)^{k-1}\right] \bmod m_2 \| \ldots \right.$$

$$\left. \ldots \| \left[(a'_2)^{k-1}\right] \bmod m_i \| \ldots \| \left[(a'_n)^{k-1}\right] \bmod m_n \right\} \cdot (a_1' \| a_2' \| \ldots \| a'_{i-1} \| a'_i \| a'_{i+1} \| \ldots \| a'_n).$$

Рис. 1. Метод быстрого возведения остатков целого числа по произвольному модулю СОК в степень натурального числа

Таблица 2

Объем кодовых слов A′ в ИФ

A	A′	A	A′	A	A′	A	A′	A	A′
-35	0	-21	14	-7	28	7	42	21	56
-34	1	-20	15	-6	29	8	43	22	57
-33	2	-19	16	-5	30	9	44	23	58
-32	3	-18	17	-4	31	10	45	24	59
-31	4	-17	18	-3	32	11	46	25	60
-30	5	-16	19	-2	33	12	47	26	61
-29	6	-15	20	-1	34	13	48	27	62
-28	7	-14	21	0	35	14	49	28	63
-27	8	-13	22	1	36	15	50	29	64
-26	9	-12	23	2	37	16	51	30	65
-25	10	-11	24	3	38	17	52	31	66
-24	11	-10	25	4	39	18	53	32	67
-23	12	-9	26	5	40	19	54	33	68
-22	13	-8	27	6	41	20	55	34	69

Приведем примеры определения величины значения A^{k}_{COK} (табл. 1).

Пример 1. Пусть $A_{COK} = 2 = (0 \| 2 \| 2)$ и $k = 2$. Определим значение $A^{k}_{COK} = 2^2$. Так, как $A = 2 > 0$, тогда получим, что $A'_{COK} = \frac{M}{2} + A_{COK} = 35 + 2 = (1 \| 0 \| 0) + (0 \| 2 \| 2) = (1 \| 2 \| \| 2) = 37$. В результате умножения значения $A'_{COK} = (1 \| 2 \| 2)$ само на себя $((1 \cdot 1) \bmod 2$, $(2 \cdot 2) \bmod 5$ и $(2 \cdot 2) \bmod 7)$ получим, что $(A'_{COK})^2 = (1 \| 4 \| 4)$.

Проверка:

$$(A'_{COK})^2 = 37^2 = 37 \times 37 = 1369 = 39 (\bmod 70) = (1 \| 2 \| 2) \times (1 \| 2 \| 2) = (1 \| 4 \| 4) = 39.$$

$$(A^2_{COK})' = \frac{M}{2} + A^2_{COK},$$

$$A^2_{COK} = (A^2_{COK})' - \frac{M}{2},$$

$$2^2 = 39 - 35,$$

$$2^2 = 4.$$

Пример 2. Пусть $A_{COK} = -2$ $(2 = (0 \| 2 \| 2))$ и $k = 2$. Так как $A_{COK} = -2 < 0$, тогда $A'_{COK} = \frac{M}{2} - A_{COK} = 35 - 2 = (1 \| 0 \| 0) - (0 \| 2 \| 2) = (1 \| 3 \| 5) = 33$. Так как $k = 2$ $(1 \cdot 1 = 1 (\bmod 2)$, $3 \cdot 3 = 4 (\bmod 5)$ та $5 \cdot 5 = 4 (\bmod 7))$, то получим, что $(A'_{COK})^2 = (1 \| 4 \| 4)$.

Проверка:

$$(A'_{COK})^2 = 33^2 = 33 \times 33 = 1089 = 39 (\bmod 70) = (1 \| 3 \| 5) \times (1 \| 3 \| 5) = (1 \| 4 \| 4) = 39.$$

$$A^2_{COK} = (A^2_{COK})' - \frac{M}{2},$$

$$(-2)^2 = 39 - 35,$$

$$(-2)^2 = 4.$$

Пример 3. Пусть $A_{COK} = 2$ $(0 \| 2 \| 2)$ и $k = 3$. Так как $A_{COK} = 2 > 0$, тогда $A'_{COK} = \frac{M}{2} + A_{COK} = 35 + 2 = 37 = (1 \| 0 \| 0) + (0 \| 2 \| 2) = (1 \| 2 \| 2) = 37$. В этом случае $(A')^2 = (1 \| 4 \| 4)$, так как $1 \cdot 1 = 1 (\bmod 2)$, $2 \cdot 2 = 4 (\bmod 5)$ та $2 \cdot 2 = 4 (\bmod 7)$. После третьего $(k = 3)$ умножения $(A'_{COK}) \times (A'_{COK}) \times (A'_{COK})$ числа A'_{COK} имеем, что $(A'_{COK})^3 = (1 \| 3 \| 1)$ $(A^k_{COK} = 2^3)$.

Проверка:

$$(A'_{COK})^3 = 37^3 = 50653 = 43 (\bmod 70) = (1 \| 2 \| 2) \times (1 \| 2 \| 2) \times (1 \| 2 \| 2) = (1 \| 3 \| 1) = 43.$$

$$A^3_{COK} = (A^3_{COK})' - \frac{M}{2},$$

$$2^3 = 43 - 35,$$

$$2^3 = 8.$$

Пример 4. Пусть $A_{COK} = -2$ $(2 = (0 \| 2 \| 2))$, $k = 3$. Если $A_{COK} = -2 < 0$, то имеем, что $A'_{COK} = \frac{M}{2} - A = 35 - 2 = (1 \| 0 \| 0) - (0 \| 2 \| 2) = (1 \| 3 \| 5) = 33$. После первой итерации умножения имеем $A'_{COK} \times A'_{COK} = (A'_{COK})^2$ $(1 \cdot 1 = 1 (\mathrm{mod}\, 2)$, $3 \cdot 3 = 4 (\mathrm{mod}\, 5)$ та $5 \cdot 5 = 4 (\mathrm{mod}\, 7))$. Так, як $k = 3$, тогда проведем вторую итерацию операцию умножения $(A'_{COK})^2 \times A'_{COK}$. В этом случае имеем $(A'_{COK})^3 = (A'_{COK})^2 \times A'_{COK} = (1 \| 4 \| 4) \times (1 \| 3 \| 5) = (1 \| 2 \| 6) = 27$.

Проверка:

$$(A'_{COK})^3 = 33^3 = 35937 = 27 (\mathrm{mod}\, 70) = A'_{COK} \times A'_{COK} \times A'_{COK} = (1 \| 3 \| 5) \times (1 \| 3 \| 5) \times (1 \| 3 \| 5) = (1 \| 2 \| 6) = 27.$$

$$A^3_{COK} = (A^3_{COK})' - \frac{M}{2},$$

$$(-2)^3 = 27 - 35,$$

$$(-2)^3 = -8.$$

Пример 5. Пусть $A_{COK} = -3$ $(3 = (1 \| 3 \| 3))$, $k = 3$. Если $A_{COK} = -3 < 0$, тогда $A'_{COK} = \frac{M}{2} - A_{COK} = 35 - 3 = (1 \| 0 \| 0) - (1 \| 3 \| 3) = (0 \| 2 \| 4) = 32$. После первой итерации умножения получим $A'_{COK} \times A'_{COK} = (A'_{COK})^2 = (0 \| 2 \| 4) \times (0 \| 2 \| 4) = (0 \| 4 \| 2)$. Так как $k = 3$ проводим вторую итерацию операции умножения $(A'_{COK})^2 \times A'_{COK} = (A'_{COK})^3 = (0 \| 4 \| 2) \times (0 \| 2 \| 4) = (0 \| 3 \| 1)$. Таким образом получим, что $A^k_{COK} = (-3)^3 = (0 \| 3 \| 1)$.

Проверка:

$$(A'_{COK})^3 = 32^3 = 32768 = 8 (\mathrm{mod}\, 70) = A' \times A' \times A' = (0 \| 2 \| 4) \times (0 \| 2 \| 4) \times (0 \| 2 \| 4) = (0 \| 2 \| 4) = (0 \| 3 \| 1) = 8.$$

$$A^3_{COK} = (A^3_{COK})' - \frac{M}{2},$$

$$(-3)^3 = 8 - 35,$$

$$(-3)^3 = -27.$$

На основе предложенного метода рассмотрим алгоритм возведения остатков a'_i целых чисел по одному произвольному модулю m_i СОК в квадрат.

Пусть необходимо определить значение $a_i^2 (\mathrm{mod}\, m)$, где: a_i, m_i – натуральные числа и $0 \le a_i \le m_i - 1$. Вначале покажем, что выполняется следующее математическое соотношение

$$a_i^2 (\mathrm{mod}\, m_i) = (m_i - a_i)^2 \bmod m_i. \qquad (17)$$

Действительно, число a_i^2 представим в виде $a_i^2 = k \cdot m_i + \alpha$ $(0 \le \alpha \le m_i - 1; k = 0, 1, 2, ...)$, т. е. $a_i^2 \equiv \alpha \bmod m_i$. Тогда $(m_i - a_i)^2 = m_i^2 - 2 \cdot m_i \cdot a_i + a_i^2 = m_i^2 - 2 \cdot m_i \cdot a_i + k \cdot m_i + \alpha$. В этом случае $(m_i^2 - 2 \cdot m_i \cdot a_i + k \cdot m_i + \alpha) \equiv \alpha \bmod m_i$. Равенство (17) справедливо как для четного, так и для нечетного значения модулю m_i.

Аналитическое соотношение (17) является алгоритмом возведения остатков целых чисел по произвольному модулю СОК в квадрат. Целесообразно рассмотреть три возможных варианта практической реализации этого алгоритма.

Первый вариант. Значение величины модуля $m_i = 2 \cdot z + 1$ СОК есть нечетное $(z = 0, 1, 2, ...)$ число. Для этого случая схема процесса реализации операции $A^2 (\mathrm{mod}\, m)$ непосредственно основывается на соотношении (17).

Второй вариант. Значение величины модуля $m_i = 2z$ СОК есть четное число, а значение величины $\frac{m_i}{2}$ есть также четное число. В этом случае значение $\frac{m_i}{2}$ является целым числом и, следовательно, $\left(\frac{m_i}{2}\right)^2 = \frac{m_i}{4} \cdot m_i \equiv 0 (\mathrm{mod}\, m_i)$. В этом случае алгоритм реализации операции возведения остатков целых чисел по произвольному модулю СОК в квадрат определяется следующим выражением (18)

$$\left(\frac{m_i}{2}\right)^2 = 0 \,(\mathrm{mod}\ m_i). \qquad (18)$$

Третий вариант. Значение величины модуля СОК $m_i = 2 \cdot z$ является четным числом, и значение величины $\frac{m_i}{2}$ также есть нечетное число. Предлагаемый алгоритм реализации возведения остатков целых чисел по произвольному модулю СОК в квадрат основывается на использовании следующего соотношения (19)

$$\left(\frac{m_i}{2}\right)^2 \equiv \frac{m_i}{2} (\mathrm{mod}\, m_i). \qquad (19)$$

Действительно выражение (19) легко представить в виде

$$\frac{m_i}{2}\cdot\left(\frac{m_i}{2}-1\right)=0\,(\mathrm{mod}\,\frac{m_i}{2}\cdot 2). \qquad (20)$$

Из теории чисел известно, что сравнимость $A\equiv B(\mathrm{mod}\,m_i)$ двух чисел A и B по модулю m_i равносильна делимости числа $A-B$ на модуль m_i. Из выражения (20) следует, что число $\frac{m_i}{2}\cdot\left(\frac{m_i}{2}-1\right)$ делится на модуль $m_i=\frac{m_i}{2}\cdot 2$. Действительно, первый сомножитель $\frac{m_i}{2}$ произведения (20) делится на $\frac{m_i}{2}$, а второй $\frac{m_i}{2}-1$ сомножитель – делится на два, так как по условию $\frac{m_i}{2}$ нечетное число. Таким образом, показана справедливость сравнения (19).

Заключение

На основании ММ процесса возведения целых чисел в квадрат по модулю и на основе использования табличного принципа реализации модульной операции умножения, в данной статье разработан метод быстрого возведения остатков целых чисел по произвольному модулю СОК в степень натурального числа, как в положительном, так и отрицательном числовых диапазонах. Полученные результаты важны и могут быть использованы для технической реализации модульной операции возведения остатков целых чисел по произвольному модулю в степень натурального числа в компьютерных вычислительных устройствах, функционирующих как в непозиционной системе счисления СОК, так и в обычной позиционной двоичной системе счисления.

Литература

1. Материалы Международной научно-технической конференции "50 лет модулярной арифметике" [Текст] // МИЭТ, г. Зеленоград, Моск. обл. 23-25 ноября 2005. – С. 101-130.

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

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

4. Краснобаев, В. А. Методы повышения надежности специализированных ЭВМ систем и средств связи [Текст] / В. А. Краснобаев. – Харьков : МО СССР, 1990. – 173 с.

5. Краснобаев, В. А. Методы и алгоритмы возведения чисел в произвольную степень по модулю системы остаточных классов [Текст] / В. А. Краснобаев // АСУ и приборы автоматики. – 1986. – Вып. 80. – С. 101-103.

6. Мартыненко, С. О. Метод возведения чисел в квадрат по модулю М модулярной системы счисления [Текст] / С. О. Мартыненко, В. А. Краснобаев // Радіоелектронні і комп'ютерні системи. – 2010. – № 5 (46). – С. 165-171.

7. Краснобаев, В. А. Метод табличной реализации операции умножения в классе вычетов [Текст] / В. А. Краснобаев, А. С. Янко, С. А. Кошман // Системи обробки інформації : зб. наук. пр. / Харк. ун-т Повітр. Сил ім. Івана Кожедуба. – Вип. 4 (120). – Харків : НАНУ, ПАНМ, ХУПС, 2014. – С. 121-127.

8. Краснобаев, В. А. Математические модели и алгоритмы возведения целых чисел в квадрат по произвольному модулю класса вычетов [Текст] / В. А. Краснобаев, А. С. Янко, С. А. Кошман // Збірник наукових праць Харківського університету Повітряних Сил. – Харків : НАНУ, ПАНМ, ХУПС. – 2014. – Вип. 1 (38). – С. 132-137.

9. Dimauro, G. A. New Technique for Fast Number Comparison in the Residue Number System [Text] / G. Dimauro, S. Impedovo, G. Pirlo // IEEE transactions on computers. – 1993. – Vol. 42, № 5. – P. 608–612.

10. Kaucher, E. Interval analysis in the extended interval space IR [Текст] / E. Kaucher // Computing Supplement. – 1989 – Vol. 2. – P. 33–49.

11. Omondi, A. Residue Number Systems: Theory and Implementation (Advances in Computer Science and Engineering Texts) [Text] / A. Omondi, B. Premkumar. – London : Imperial College Press, 2007. – 312 p.

12. Morgado, Matthew. Modular Arithmetic [Electronic resource] / Matthew Morgado. – Access mode: http://www.math.uchicago.edu/~may/REU2014/REUPapers/Morgado.pdf. – 25.11.2015.

Поступила в редколлегию 25.11.2014, рассмотрена на редколлегии 20.03.2015

МЕТОД ПІДНЕСЕННЯ ОСТАЧ ЦІЛИХ ЧИСЕЛ ЗА ДОВІЛЬНИМ МОДУЛЕМ СИСТЕМИ ЗАЛИШКОВИХ КЛАСІВ ДО СТУПЕНЯ НАТУРАЛЬНОГО ЧИСЛА

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

На основі існуючої математичної моделі піднесення до квадрату остач цілих чисел за модулем класу лишків у статті розроблено математичну модель і метод піднесення остач цілих чисел за довільним модулем системи залишкових класів (СЗК) до ступеня натурального числа. Наведено приклади конкретної реалізації представленого методу піднесення остач цілих чисел до ступеня. Запропонований метод зведення остач цілих чисел до ступеня натурального числа може бути використаний у комп'ютерній системі швидкої обробки цілочисельних даних, що функціонує у СЗК, а також у комп'ютерних обчислювальних пристроях, які функціонують у звичайній позиційній двійковій системі числення.

Ключові слова: непозиційна система числення у залишкових класах, позиційна двійкова система числення, комп'ютерна система швидкої обробки цілочисельних даних, піднесення остач цілих чисел до ступеня натурального числа.

THE METHOD OF INVOLUTION OF RESIDUES OF INTEGERS TO ARBITRARY MODULUS OF SYSTEM OF RESIDUAL CLASSES TO THE POWER OF A NATURAL NUMBER

V. A. Krasnobayev, A. S. Yanko, S. A. Koshman

On the basis of the existing mathematical models squaring residues of integers to residue class modulus in the article developed the mathematical model and the method of involution of residues of integers to arbitrary modulus of system of residual classes (SRC) to the power of a natural number. The examples of the specific implementation of the presented method by involution of residues of integers to the power were made. Proposed method of involution of residues of integers to the power of a natural number can be used in a computer system fast integer data processing which functioning in SRC, and machine computing devices which functioning in a normal positional binary system.

Keywords: non-positional number system of residue class, positional binary number system, computer system fast integer data processing, involution of residues of integers to the power of a natural number.

Краснобаев Виктор Анатольевич – д-р техн. наук, проф., зав. кафедрой компьютерной инженерии, Полтавский национальный технический университет им. Юрия Кондратюка, Полтава, Украина, e-mail: krasnobaev_va@rambler.ru.

Янко Алина Сергеевна – аспирант каф. компьютерной инженерии, Полтавский национальный технический университет им. Юрия Кондратюка, Полтава, Украина, e-mail: al9_yanko@ukr.net.

Кошман Сергей Александрович – канд. техн. наук, доцент, доцент каф. автоматизации и компьютерно-интегрированных технологий, Харьковский национальный технический университет сельского хозяйства им. Петра Василенка, Харьков, Украина, e-mail: s_koshman@ukr.net.