УДК 519.7

Касянчук М. Н.

Канд. физ.-мат. наук, доцент, доцент кафедры компьютерной инженерии Тернопольского национального экономического университета, Тернополь, Украина

ПОСТРОЕНИЕ МОДИФИЦИРОВАННОЙ СОВЕРШЕННОЙ ФОРМЫ СИСТЕМЫ ОСТАТОЧНЫХ КЛАССОВ С ИСПОЛЬЗОВАНИЕМ ФАКТОРИЗАЦИИ

Актуальность. Решена актуальная задача нахождения модулей системы остаточных классов, в которой повышается скорость перевода чисел из системы остаточных классов в десятичную систему исчисления.

Цель работы – разработка метода построения четырехмодульной модифицированной совершенной формы системы остаточных классов, в которой отсутствует процедура поиска обратного элемента по модулю при переводе чисел из системы остаточных классов в десятичную систему исчисления.

Метод. Предложен метод определения набора модулей модифицированной совершенной формы системы остаточных классов на основе факторизации произведения чисел. Использование данного метода позволяет существенно уменьшить вычислительную сложность при выполнении арифметических операций над многоразрядными числами путем распараллеливания процесса вычислений и переводе чисел из системы остаточных классов в десятичную систему исчисления за счет исключения процедуры поиска обратного элемента по модулю и умножения на базисные числа. Определены условия для нахождения любого количества модулей модифицированной совершенной формы системы остаточных классов, два из которых являются неизвестными. Приведен пример использования предложенного метода для четырехмодульной модифицированной совершенной формы системы остаточных классов, в котором получены все возможные наборы модулей при заданном наименьшем модуле. Представлены табличные значения и проанализированы графические зависимости полученных модулей.

Результаты. Использование предложенного метода подбора модулей, которые образуют модифицированную совершенную форму, позволит увеличить быстродействие вычислительных систем, работающих в системе остаточных классов.

Выводы. Впервые предложен метод построения четырехмодульной модифицированной совершенной формы системы остаточных классов на основе факторизации, в которой отсутствует сложная процедура поиска обратного элемента по модулю. Это позволяет упростить процессы вычислений над многоразрядными числами и перевода чисел из системы остаточных классов в десятичную систему исчисления.

Ключевые слова: система остаточных классов, базисные числа, система модулей, модифицированная совершенная форма, разрядность чисел, факторизация.

НОМЕНКЛАТУРА

МСФ – модифицированная совершенная форма;

СОК – система остаточных классов;

СФ – совершенная форма;

$b_1, b_2, \ldots, b_n$ – запись числа в системе остаточных классов;

k_1 – ряд натуральных чисел;

k_2 – ряд целых чисел;

n – количество модулей;

N – запись числа в десятичной системе исчисления;

$p_1, p_2, \ldots, p_n$ – модули;

P – произведение модулей.

ВВЕДЕНИЕ

В последнее время непозиционные системы исчисления привлекают все больше внимания с целью использования их в современных вычислительных системах [1]. Это объясняется тем, что в связи со значительным ростом объемов вычислений и увеличением разрядности используемых чисел [2] существенно проявляются недостатки двоичной системы (например, ее многоразрядность, последовательная структура, наличие междуразрядных переносов [3]), которые в большой степени замедляют быстродействие вычислительных систем. Перечисленные недостатки отсутствуют в некоторых непозиционных системах исчислений, например, в системе остаточных классов (СОК) [4], что делает ее использование весьма перспективным. В частности, СОК можно эффективно использовать при выполнении целочисленных операций модулярной арифметики над многоразрядными числами: сложения, вычитания, умножения, возведения в степень [5] и т.д. Это особенно актуально для современной асимметричной криптографии (алгоритмы RSA, Эль-Гамаля, Рабина, электронной цифровой подписи [6]), больших матричных вычислений, разработки методов помехозащищенного кодирования [7], других задач дискретной и прикладной математики [8]. Кроме того, очень важным положительным свойством СОК является возможность распараллеливания процесса вычислений согласно модульной арифметике с низкой разрядностью модулей [4].

К отрицательным сторонам СОК относятся целочисленность операндов, трудности выполнения арифметических операций деления и сравнения [9], а также определения переполнения разрядной сетки. Еще одним недостатком, который существенно замедлил развитие СОК, является сложность перевода в позиционные системы исчислений [4], что связано с необходимостью поиска обратного элемента по модулю.

Объект исследования – процесс перевода чисел из СОК в десятичную систему исчисления. Предметом исследования выступают модули СОК, для которых отсутствует процедура поиска обратного элемента по модулю.

Целью данной работы являлась разработка метода построения четырехмодульной модифицированной со-

DOI 10.15588/1607-3274-2017-3-6

вершенной формы системы остаточных классов, в которой отсутствует процедура поиска обратного элемента по модулю при переводе чисел из системы остаточных классов в десятичную систему исчисления.

1 ПОСТАНОВКА ЗАДАЧИ

Теоретической основой СОК является теория чисел [10]. Любое целое десятичное число N представляется в СОК в виде набора $(b_1, b_2, \ldots, b_n)$ наименьших положительных остатков от деления этого числа на фиксированные натуральные попарно взаимно простые числа $p_1, p_2, \ldots, p_n$ ($b_i=N \bmod p_i$), которые называются модулями (n – количество модулей). При этом должно выполняться неравенство $0 \le N<P-1$, где $P=\prod_{i=1}^{n} p_i$ – число, которое определяет условие переполнения разрядности вычислений.

При обратном преобразовании из СОК в десятичную систему исчисления используется китайская теорема об остатках:

$$N=\left(\sum_{i=1}^{n} b_i B_i\right) \bmod P, \qquad (1)$$

где $B_i=M_i m_i$, $M_i=\frac{P}{p_i}$, $m_i=M_i^{-1} \bmod p_i$ – базисные числа.

Нахождение обратных элементов по модулю характеризуется значительной вычислительной сложностью и в теории чисел реализуется полным перебором возможных вариантов, с помощью алгоритма Евклида или теоремы Эйлера [11]. Поэтому разработка метода построения СОК, в которой отсутствует данная процедура, является актуальной задачей.

2 ОБЗОР ЛИТЕРАТУРЫ

В работе [12] описана совершенная форма (СФ) СОК, в которой выполняется условие $M_i \bmod p_i = 1$, что позволяет избежать процедуры поиска обратного элемента и умножения в (1) на базисные числа m_i. Выражение (1) в этом случае упрощается:

$$N=\left(\sum_{i=1}^{n} b_i M_i\right) \bmod P. \qquad (2)$$

В [13], [14] путем решения систем конгруэнций получено выражение для поиска набора модулей СФ СОК:

$$\sum_{i=1}^{n} \frac{1}{p_i} = k_1 + \frac{1}{\prod_{i=1}^{n} p_i}, \qquad (3)$$

где $k_1=1, 2, 3, \ldots$.

В [15] решена задача и определены условия для аналитического нахождения m_i. Однако у всех этих случаях значения p_i быстро увеличиваются, что неприемлемо при необходимости использования модулей одинаковой разрядности.

В [12] предложена модифицированная совершенная форма (МСФ) СОК, в которой $M_i \bmod p_i = \pm 1$, что также исключает выполнение операции поиска обратного элемента. Вычисления (1) происходят согласно формулы

$$N=\left(\sum_{i=1}^{n} b_i m_i M_i\right) \bmod P, m_i=\pm 1. \qquad (4)$$

В [16] разработан метод построения МСФ СОК из трех модулей на примере p_2–p_1=5. В [17] представлены теоретические основы построения трехмодульной МСФ СОК в общем случае. Однако в настоящее время отсутствуют универсальные методы нахождения любого количества модулей, которые удовлетворяют условиям МСФ СОК.

3 МАТЕРИАЛЫ И МЕТОДЫ

Рассуждения, аналогичные представленным в [13], [14] для СФ СОК (выражение (3)), приводят к условию, которое должно выполняться для МСФ СОК:

$$\sum_{i=1}^{n} \frac{1}{p_i} = k_2 \pm \frac{1}{\prod_{i=1}^{n} p_i}, \qquad (5)$$

где $k_2=0, \pm 1, \pm 2, \pm 3, \ldots$.

В отличие от СФ СОК, где все модули положительные и поэтому $k_1>0$, в МСФ СОК модули имеют разные знаки и для упрощения задачи можно принять $k_2=0$, что соответствует наибольшему диапазону вычислений при заданном количестве модулей. Таким образом, уравнение (5) представим следующим выражением:

$$\frac{1}{p_1}+\frac{1}{p_2}+\frac{1}{p_3}+\ldots+\frac{1}{p_{n-1}}+\frac{1}{p_n}=\pm\frac{1}{p_1 p_2 p_3 \cdots p_{n-1} p_n}. \qquad (6)$$

Следует отметить, что условию $m_i=1$ отвечают положительные значения модулей p_i, а условию $m_i=-1$ – отрицательные. Кроме того, если в СФ СОК наименьшие модули строго определены ($p_1=2$, $p_2=3$) [14], то в МСФ СОК они могут изменяться произвольным образом.

Пусть неизвестными будут два последних модуля p_{n-1} и p_n. Тогда (6) представим в виде диофантового уравнения второй степени:

$$p_{n-1}p_n\left(p_2 p_3 \cdots p_{n-2} + p_1 p_3 \cdots p_{n-2} + \ldots + p_1 p_2 \cdots p_{n-3}\right) + \\ + p_1 p_2 \cdots p_{n-2}\left(p_{n-1}+p_{n-2}\right)=\pm 1. \qquad (7)$$

Введем обозначение:

$$p_{n-1,n}=\frac{a,b-p_1 p_2 \cdots p_{n-2}}{p_2 p_3 \cdots p_{n-2} + p_1 p_3 \cdots p_{n-2} + \ldots + p_1 p_2 \cdots p_{n-3}}. \qquad (8)$$

После подстановки (8) в (7) и соответствующих математических преобразований получаем выражение для целочисленного решения (7):

$$\pm\left(p_2 p_3 \cdots p_{n-2} + p_1 p_3 \cdots p_{n-2} + \ldots + p_1 p_2 \cdots p_{n-3}\right) + \\ + \left(p_1 p_2 p_{n-2}\right)^2 = ab. \qquad (9)$$

Это означает, что левую часть (9) надо факторизировать, на основании чего определяются параметры a и b. Кроме этого, модули p_n и p_{n-1} должны быть целыми числами. Поэтому из (8) следует:

$$\left(a,b-p_1 p_2 \cdots p_{n-2}\right) \bmod \left(p_2 p_3 \cdots p_{n-2} + p_1 p_3 \cdots p_{n-2} + \right. \\ \left. + \ldots + p_1 p_2 \cdots p_{n-3}\right) = 0. \qquad (10)$$

Выражения (9) и (10) определяют условия для нахождения любого количества модулей МСФ СОК, два из которых неизвестны.

4 ЭКСПЕРИМЕНТЫ

В качестве примера предложенного метода рассмотрим МСФ СОК, состоящую из четырех модулей. Условия (8)–(10) трансформируются таким образом:

$$p_{3,4}=\frac{a,b-p_1p_2}{p_1+p_2};\ \pm(p_1+p_2)+(p_1p_2)^2=ab;$$

$$(a,b-p_1p_2)\bmod(|p_1+p_2|)=0. \qquad (11)$$

Из (6) видно, что при n=4 значения p_1 и p_2 должны иметь разные знаки. Считая модуль p_1 положительным, наибольшее количество вариантов будет при условии p_2=–(p_1+1), так как в этом случае третье условие (11) выполняется всегда. Первые два приобретут такой вид:

$$p_{3,4}=-(a,b+p_1^2+p_1);\ \pm1+(p_1(p_1+1))^2=ab. \qquad (12)$$

Примем p_1=7, тогда p_2=–8 и из (12) получаем:

$$p_{3,4}=-(a,b+56) \text{ и } ab=\pm1+3136=\begin{cases}3135=3\cdot5\cdot11\cdot19\\3137\end{cases}.$$

Численные расчеты показывают, что для p_1=7 в других случаях, кроме p_2= –8, наибольшее количество вариантов наборов модулей будет при p_2= –9 и p_2= –11. Тогда уравнения (11) приобретут соответственно такой вид:

$$p_{3,4}=-\frac{a,b+63}{2};\ \pm2+63^2=ab;\ (a,b-63)\bmod2=0. \qquad (13)$$

$$p_{3,4}=-\frac{a,b+77}{4};\ \pm4+77^2=ab;\ (a,b-77)\bmod4=0. \qquad (14)$$

Отсюда следует, что

$$ab=\pm2+3969=\begin{cases}3967\\3971=11\cdot19\cdot19\end{cases} \text{ для } p_2=-9 \text{ и}$$

$$ab=\pm4+5929=\begin{cases}5925=3\cdot5\cdot5\cdot79\\5933=17\cdot349\end{cases} \text{ для } p_2=-11.$$

5 РЕЗУЛЬТАТЫ

В таблице 1 представлены всевозможные варианты систем из четырех модулей для МСФ СОК при p_1=7, p_2= –8 согласно (10) (в скобках указана разрядность модулей и диапазона вычислений в двоичной системе исчисления).

Для построения графика зависимости модулей их необходимо перенумеровать в порядке увеличения абсолютной величины p_3, что представлено в таблице 2.

На рисунке 1 показан характер изменения значений модулей p_3 и p_4 в зависимости от номера модуля согласно таблицы 2 в логарифмической шкале с основанием 2.

В таблице 3 приведены упорядоченные значения абсолютных величин модулей, полученные из (12) аналогично таблице 2, при p_2=–9 и p_2=–11, а также граница диапазона вычислений P (в скобках указана разрядность представленных чисел).

На рисунке 2 показаны графики зависимости значений модулей p_3 и p_4 (сплошной линией – для p_2= –9, пунктирной – для p_2=–11) в зависимости от номера модуля согласно таблицы 3 в логарифмической шкале с основанием 2.

Таблица 1 – Возможные варианты систем из четырех модулей для МСФ СОК при p_1=7, p_2= –8 (в скобках – разрядность модулей и диапазона вычислений)

№	p_1, p_2	ab	a	b	p_3	p_4	P
1	7 (3), –8 (4)	3135	1	3135	–57 (6)	–3191 (12)	10185672 (24)
2			–1	–3135	–55 (6)	3079 (12)	9483320 (24)
3			3	1045	–59 (6)	–1101 (11)	3637704 (22)
4			–3	–1045	–53 (6)	989 (10)	2935352 (22)
5			5	627	–61 (6)	–683 (10)	2333128 (22)
6			–5	–627	–51 (6)	571 (10)	1630776 (21)
7			11	285	–67 (7)	–341 (9)	1279432 (21)
8			–11	–285	–45 (6)	229 (8)	577080 (20)
9			15	209	–71 (7)	–265 (9)	1053640 (21)
10			–15	–209	–41 (6)	153 (8)	351288 (19)
11			19	165	–75 (7)	–221 (8)	928200 (20)
12			–19	–165	–37 (6)	109 (7)	225848 (18)
13			33	95	–89 (7)	–151 (8)	752584 (20)
14			–33	–95	–23 (5)	39 (6)	50232 (16)
15			55	57	–111 (7)	–113 (7)	702408 (20)
16			–55	–57	–1 (1)	1 (1)	56 (6)
17		3137	1	3137	–57 (6)	–3193 (12)	10192056 (24)
18			–1	–3137	–55 (6)	3081 (12)	9489480 (24)

Таблица 2 – Упорядочение модулей

№	1	2	3	4	5	6	7	8	9
p_3	1	23	37	41	45	51	53	55	55
p_4	1	39	109	153	229	571	989	3079	3081
№	10	11	12	13	14	15	16	17	18
p_3	57	57	59	61	67	71	75	89	111
p_4	3191	3193	1101	683	341	265	221	151	113

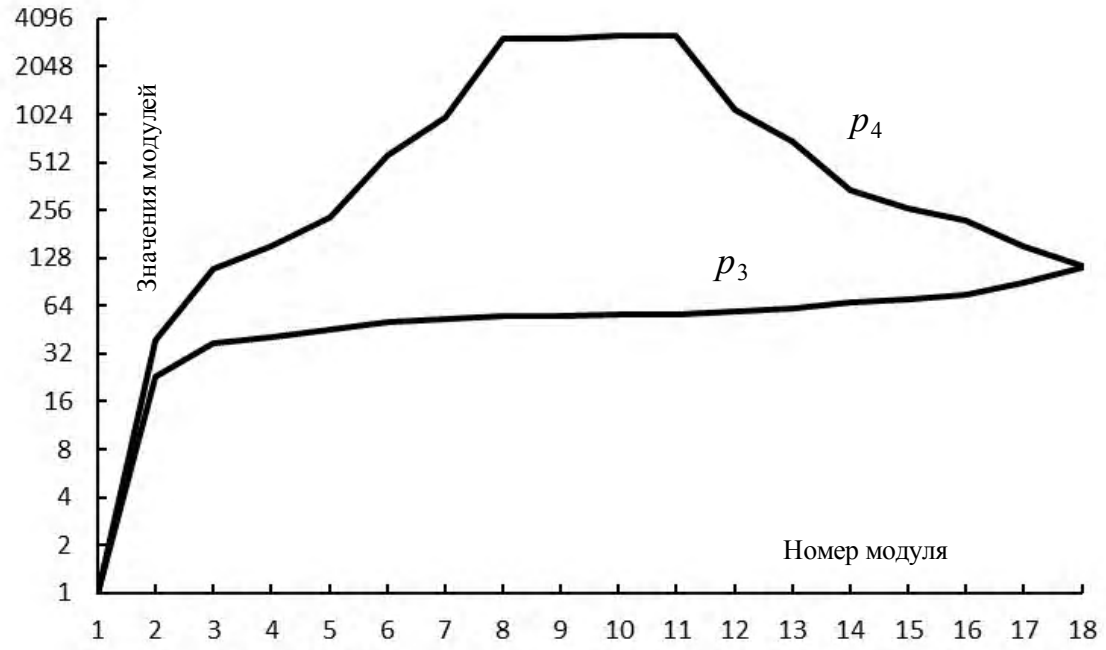

Рисунок 1 – Характер изменения значений модулей p_3 и p_4 при p_1=7, p_2= –8 в зависимости от номера модуля согласно таблицы 2

Таблица 3 – Упорядоченные значения абсолютных величин модулей p_3 и p_4 при p_2= –9 и p_2= –11 (в скобках – разрядность модулей и диапазона вычислений)

p_2	p_3, p_4	1	2	3	4	5	6	7	8
9 (4)	p_3	22(5)	26(5)	31(5)	31(5)	32(6)	32(6)	37(6)	41(6)
	p_4	73(7)	149(8)	1952(11)	1954(11)	2015(11)	2017(11)	212(8)	136(8)
	P	101178 (17)	244062 (18)	3812256 (22)	3816162 (22))	4062240 (22)	4066272 (22)	494172 (19)	351288 (19)
11 (4)	p_3	13(4)	15(4)	18(5)	19(5)	19(5)	20(5)	23(5)	38(6)
	p_4	40(6)	68(7)	277(9)	1462(11)	1464(11)	513(10)	118(7)	39(6)
	P	40040 (16)	78540 (17)	383922 (19)	2138906 (22)	2141832 (22)	790020 (20)	208978 (18)	114114 (17)

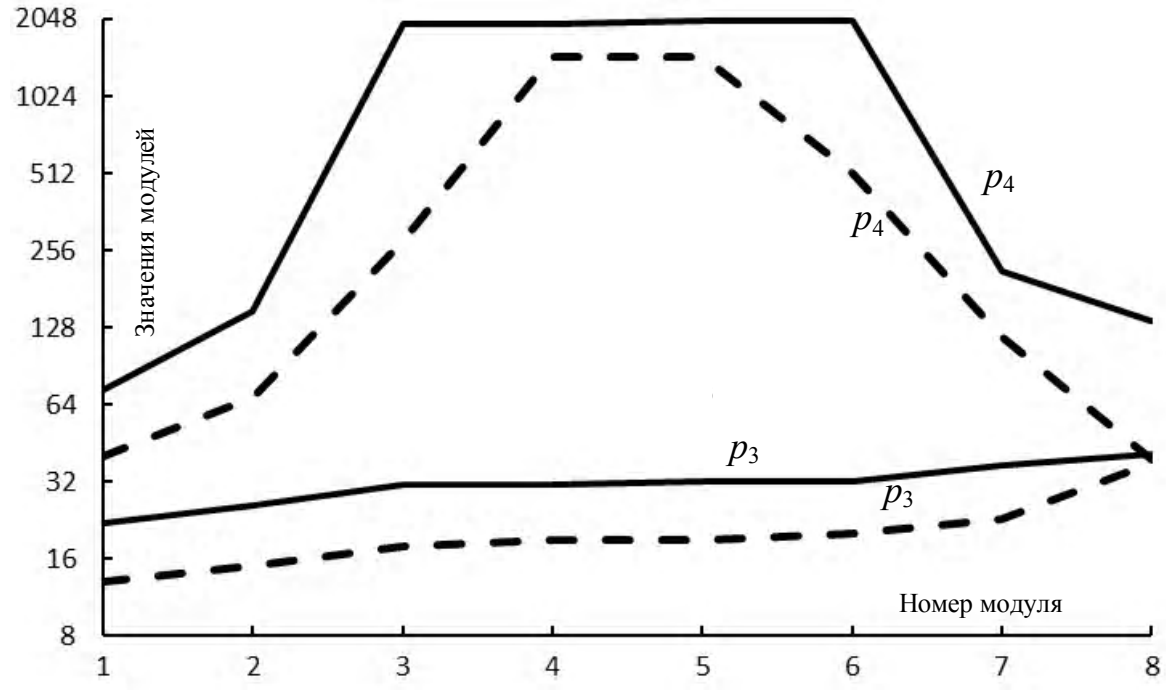

Рисунок 2 – Характер изменения значений модулей p_3 и p_4 при p_1=7, p_2=–9 (сплошная линия) и p_2=–11 (пунктирная линия) в зависимости от номера модуля согласно таблицы 3

В таблице 4 представлены остальные возможные варианты наборов модулей МСФ СОК при p_1=7, полученные согласно условиям (11).

Таблица 4 – Возможные варианты систем из четырех модулей для МСФ СОК при p_1=7, p_2=–10, –12, –13, –15 (в скобках – разрядность модулей и диапазона вычислений)

p_2	p_3	p_4	P
–10 (4)	–23 (5)	1609 (11)	2590490 (22)
	–23 (5)	1611 (11)	2593710 (22)
	–43 (6)	–51 (6)	153510 (18)
–12 (4)	–17 (5)	–1427 (11)	2037756 (22)
	–17 (5)	–1429 (11)	2040612 (22)
	–19 (5)	–145 (8)	231420 (18)
–13 (4)	–15 (4)	1364 (11)	1861860 (21)
	–15 (4)	1366 (11)	1864590 (21)
	–16 (5)	–291 (9)	423696 (19)
–15 (4)	–16 (5)	–73 (7)	122640 (17)

6 ОБСУЖДЕНИЕ

Из таблицы 1 следует, что наибольший диапазон вычислений будет в том случае, когда каждый следующий модуль на единицу больше от произведения абсолютных величин предыдущих. Строка 16 таблицы 1 показывает, что числа 7 и –8 образуют МСФ СОК, поскольку 7 mod 8=–1 mod 8 и 8 mod 7 =1. Модулям p_3=–55 и p_3=–57 ($p_3=p_1 \cdot p_2 \pm 1$) соответствуют по два разных значения p_4.

Из рисунка 1 видно, что модуль p_3 относительно медленно увеличивается. В то же время, график для модуля p_4 увеличивается интенсивнее, приходит к плоскому максимуму посредине номерного диапазона модулей, а потом убывает к значению модуля p_3.

При p_2= –9 и p_2= –11 из (13) и (14) следует, что параметры a и b есть нечетными числами, поэтому третье условие из (13) выполняется при всех возможных значениях a и b, а третье условие (12) – только для половины возможных вариантов параметров a и b.

Графики на рисунке 2 ведут себя аналогично рисунку 1, но при p_2= –9 максимум становится шире.

Из таблицы 4 видно, что большинство вариантов получены при $a=\pm 1$, когда четвертый модуль на единицу отличается от произведения трех предыдущих, что соответствует наибольшей границе диапазона вычислений.

ВЫВОДЫ

В работе решена задача построения четырехмодульной модифицированной совершенной формы системы остаточных классов, в которой отсутствует процедура поиска обратного элемента по модулю.

Научная новизна результатов, полученных в статье, состоит в том, что впервые предложен метод построения четырехмодульной модифицированной совершенной формы системы остаточных классов на основе факторизации, в которой отсутствуют обладающие большой вычислительной сложностью процедуры поиска обратного элемента по модулю и умножения на базисные числа, что позволяет упростить выполнение арифметических операций над многоразрядными числами путем распараллеливания процесса вычислений и перевод чисел из системы остаточных классов в десятичную систему исчисления.

Практическая значимость полученных результатов заключается в том, что использование предложенного метода подбора модулей, которые образуют модифицированную совершенную форму, позволит увеличить быстродействие вычислительных систем, работающих в системе остаточных классов.

Перспективы дальнейших исследований состоят в том, чтобы определить условия для нахождения модулей модифицированной совершенной формы системы остаточных классов, три и больше из которых являются неизвестными, а также программная и аппаратная реализация предложенного и запланированных методов.

БЛАГОДАРНОСТИ

Работа выполнена в рамках научно-исследовательской работы «Обработка многоразрядных чисел в системе остаточных классов» кафедры компьютерной инженерии Тернопольского национального экономического университета, государственный регистрационный номер 0115U001607.

Автор выражает благодарность кандидатам технических наук, доцентам кафедры компьютерной инженерии Тернопольского национального экономического университета Якименко Игорю Зиновьевичу и Ивасьеву Степану Владимировичу за моральную поддержку при написании работы и полезное обсуждение полученных результатов.

СПИСОК ЛИТЕРАТУРЫ

1. Николайчук Я. М. Теорія джерел інформації / Я. М. Николайчук. – Тернопіль : ТзОВ «Терно-граф», 2010. – 536 с.
2. Advanced method of factorization of multi-bit numbers based on Fermat's theorem in the system of residual classes / [M. Karpinski, S. Ivasiev, I. Yakymenko et al.] // Control, Automation and Systems : 16th International Conference, Gyeongju, 16–19 October 2016 : proccedings. – Los Alamitos: IEEE, 2016. – P. 1484–1486. DOI: 10.1109/ICCAS.2016.7832500.
3. Рабинович З. Л. Типовые операции в вычислительных машинах / З. Л. Рабинович, В. А. Раманаускас. – К. : Техника, 1980. –264 с.
4. Акушский И. Я. Машинная арифметика в остаточных классах / И. Я. Акушский, Д. И. Юдицкий. – М. : Сов. радио, 1968. – 440 с.
5. Vector Module Exponential in the Remaining Classes System / [Kozaczko D., Ivasiev S., Yakymenko I. et al.] // Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications : IEEE 8th International Conference, Warsaw, 24–26 September 2015 : proceedings. – Los Alamitos : IEEE, 2015. – P. 161–163.
6. Теорія алгоритмів RSA та Ель-Гамаля в розмежованій системі числення Радемахера-Крестенсона / [М. М. Касянчук, І. З. Якименко, О. І. Волинський та ін.] // Вісник Хмельницького національного університету: технічні науки. – 2011. – № 3. – С. 265–273.
7. Jun S. Method and Device for Image Coding & Transferring Based on Residue Number System / S. Jun, V. Yatskiv // Journal Sensors & Transducers. – 2013. – Vol.148, №1. – P. 60–65.
8. Krasnobayev V. Method of Increasing the Reliability of Verification of Data Represented in a Residue Number System / V. Krasnobayev, S. Koshman, M. Mavrina // Cybernetics and Systems Analysis. – 2014. – Vol. 50, № 6. – P. 969–976. DOI: 10.1007/s10559-014-9688-3.

9. Krasnobayev V. A. A Method for Arithmetic Comparison of Data Represented in a Residue Number System / V. A. Krasnobayev, A. S. Yanko, S. A. Koshman // Cybernetics and Systems Analysis. – 2016. – Vol. 52, № 1. – P. 145–150. DOI: 10.1007/s10559-016-9809-2.
10. Бухштаб А. А. Теория чисел / А. А. Бухштаб. – М. : Просвещение, 1966. – 384 с.
11. Вербіцький О. В. Вступ до криптології / О. В. Вербіцький. – Львів : ВНТЛ, 1998. – 248 с.
12. Касянчук М. М. Теорія та математичні закономірності досконалої форми системи залишкових класів / М. М. Касянчук // Питання оптимізації обчислень: XXXV Міжнародний симпозіум, Кацивелі, 24–29 вересня 2009 р. : тези доповідей. – Київ : Інститут кібернетики ім. В. М. Глушкова, 2009.– С. 306–310.
13. Algorithms of findings of perfect shape modules of remaining classes system / [M. Kasianchuk, I. Yakymenko, I. Pazdriy et al.] // The Experience of Designing and Application of CAD Systems in Microelectronics : XIII International Conference, Polyana-Svalyava, 23–25 February 2015 : Proceedings. – L'viv : Lviv Polytechnic National University, 2015. – P. 168–171.
14. Аналітичний пошук модулів досконалої форми системи залишкових класів та їх використання в китайській теоремі про залишки / [М. М. Касянчук, І. З. Якименко, І. Р. Паздрій та ін.] // Вісник Хмельницького національного університету : технічні науки. – 2015. - №1. – С. 170–176.
15. Nykolaychuk Ya. M. Theoretical Foundations for the Analytical Computation of Coefficients of Basic Numbers of Krestenson's Transformation / Ya. M. Nykolaychuk, M. M. Kasianchuk, I. Z. Yakymenko // Cybernetics and Systems Analysis. – 2014. – Vol. 50, № 5. – P. 649–654. DOI: 10.1007/s10559-014-9654-0.
16. Nykolaychuk Ya. M. Theoretical Foundations of the Modified Perfect Form of Residue Number System / Ya. M. Nykolaychuk, M. M. Kasianchuk, I. Z. Yakymenko // Cybernetics and Systems Analysis. – 2016. – Vol. 52, № 2. – P. 219–223. DOI: 10.1007/s10559-016-9817-2.
17. Kasianchuk M. N. Theory and Methods of Constructing of Modules System of the Perfect Modified Form of the System of Residual Classes / M. N. Kasianchuk, Y. N. Nykolaychuk, I. Z. Yakymenko // Journal of Automation and Information Sciences. – 2016. – Vol.48, № 8. – P. 56–63. DOI: 10.1615/JAutomatInfScien.v48.i8.60.

Статья поступила в редакцию 22.12.2016.
После доработки 13.03.2017.

Касянчук М. М.
Канд. фіз.-мат. наук, доцент, доцент кафедри комп'ютерної інженерії Тернопільського національного економічного університету, Тернопіль, Україна

ПОБУДОВА МОДИФІКОВАНОЇ ДОСКОНАЛОЇ ФОРМИ СИСТЕМИ ЗАЛИШКОВИХ КЛАСІВ З ВИКОРИСТАННЯМ ФАКТОРИЗАЦІЇ

Актуальність. Вирішено актуальне завдання знаходження модулів системи залишкових класів, в якій підвищується швидкість переведення чисел із системи залишкових класів у десяткову систему числення.

Мета роботи – розробка методу побудови чотирьохмодульної модифікованої досконалої форми системи залишкових класів, в якій відсутня процедура пошуку оберненого елемента за модулем при переведенні чисел із системи залишкових класів у десяткову систему числення.

Метод. Запропоновано метод визначення набору модулів модифікованої досконалої форми системи залишкових класів на основі факторизації добутку чисел. Використання даного методу дозволяє істотно зменшити обчислювальну складність при виконанні арифметичних операцій над багаторозрядними числами шляхом розпаралелювання процесу обчислень та переведенні чисел із системи залишкових класів у десяткову систему числення за рахунок уникнення процедури пошуку оберненого елемента за модулем і множення на базисні числа. Визначено умови для знаходження будь-якої кількості модулів модифікованої досконалої форми системи залишкових класів, два з яких є невідомими. Наведено приклад використання запропонованого методу для чотирьохмодульної модифікованої досконалої форми системи залишкових класів, в якому отримані всі можливі набори модулів при заданому найменшому модулі. Представлено табличні значення та проаналізовані графічні залежності отриманих модулів.

Результати. Використання запропонованого методу підбору модулів, що утворюють модифіковану досконалу форму, дозволить збільшити швидкодію обчислювальних систем, які працюють у системі залишкових класів.

Висновки. Вперше запропоновано метод побудови чотирьохмодульної модифікованої досконалої форми системи залишкових класів на основі факторизації, в якій відсутня складна процедура пошуку оберненого елемента за модулем. Це дозволяє спростити процеси обчислень над багаторозрядними числами і переведення чисел із системи залишкових класів у десяткову систему числення.

Ключові слова: система залишкових класів, базисні числа, система модулів, модифікована досконала форма, розрядність чисел, факторизація.

Kasianchuk M. M.
PhD, Associate Professor, Associate Professor of Department of Computer Engineering, Ternopil National Economic University, Ternopil, Ukraine

THE CONSTRUCTION OF THE MODIFIED PERFECT FORM OF RESIDUAL CLASSES SYSTEM USING FACTORIZATION

Context. The urgent task of finding modules of the system of residue classes, which characterize by increasing the speed of transition of numbers from the system of residue classes into decimal number system.

Objective is to develop a method of constructing modified fourth-module perfect form of the system of residue classes without procedure of finding of the absolute value for inverse element under number transition from residue number system to decimal number system.

Method. The method of determining a set of modules if modified perfect form of system's of residue number was proposed which was based on factorization of numbers product. Usage of this form significantly reduced the computational complexity when arithmetic operations were performing on multi-digital numbers and transferring of numbers from the system of residual classes in the decimal system of calculation by eliminating of the searching procedure of the inverse element in absolute value and multiplying by the basic numbers. The conditions of discovering of any absolute number of modified perfect form of system of residual classes and two of them are unknown. An example of the proposed method for forth-module with modified perfect form system, which received all possible sets of modules with given smallest module. Tabular amounts are presented and analyzed according to the received image of modules.

Results. Utilization of the proposed method of modules selection which has constructed modified perfect form allows to increase the performance of computing systems operating in the system residual classes.

Conclusions. It's the first time of discover of the method which allows to construct modified fourth-module perfect form of the system of residue classes based on factorization without complicated procedure of finding of the absolute value for inverse element. Present work helps to simplify the process of calculating digit number and transfer numbers from the system of residual classes into decimal system.

Keywords: system of residual classes, basic number, system of modules, modified perfect form, bit numbers, factorization.

REFERENCES

1. Nykolajchuk Ja. M. Teorija dzherel informacii'. Ternopil', TzOV „Terno-graf", 2010, 536 p.
2. Karpinski M., Ivasiev S., Yakymenko I. et al.] Advanced method of factorization of multi-bit numbers based on Fermat's theorem in the system of residual classes, *Control, Automation and Systems : 16th International Conference, Gyeongju, 16–19 October 2016* : proccedings. Los Alamitos, IEEE, 2016, pp. 1484–1486. DOI: 10.1109/ICCAS.2016.7832500.
3. Rabinovich Z. L., Ramanauskas V. A. Tipovye operacii v vychislitel'nyh mashinah. Kiev, Tehnika, 1980, 264 p.
4. Akushskij I. Ja., Judickij D. I. Mashinnaja arifmetika v ostatochnyh klassah. Moscow, Sov.radio, 1968, 440 p.
5. Kozaczko D., Ivasiev S., Yakymenko I. et al. Vector Module Exponential in the Remaining Classes System, *Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications : IEEE 8th International Conference, Warsaw, 24–26 September 2015 : proceedings*. Los Alamitos, IEEE, 2015, pp. 161–163.
6. Kasjanchuk M. M., Jakymenko I. Z., Volyns'kyj O. I. ta in. Teorija algorytmiv RSA ta El'– Gamalja v rozmezhovanij systemi chyslennja Rademahera-Krestensona, *Visnyk Hmel'nyc'kogo nacional'nogo universytetu. Tehnichni nauky*, 2011, No. 3, pp. 265–273.
7. Jun S., Yatskiv V. Method and Device for Image Coding & Transferring Based on Residue Number System, *Journal Sensors & Transducers,* 2013, Vol. 148, No. 1, pp. 60–65.
8. Krasnobayev V., Koshman S., Mavrina M. Method of Increasing the Reliability of Verification of Data Represented in a Residue Number System, *Cybernetics and Systems Analysis*, 2014, Vol. 50, No. 6, pp. 969–976. DOI:10.1007/s10559-014-9688-3.
9. Krasnobayev V. A., Yanko A. S., Koshman S. A. A Method for Arithmetic Comparison of Data Represented in a Residue Number System, *Cybernetics and Systems Analysis*, 2016, Vol. 52, No. 1, pp. 145–150. DOI: 10.1007/s10559-016-9809-2.
10. Buhshtab A. A. Teorija chisel. Moscow, Prosveshhenie, 1966, 384 p.
11. Verbic'kyj O. V. Vstup do kryptologii'. L'viv, VNTL, 1998, 248 p.
12. Kasjanchuk M. M. Teorija ta matematychni zakonomirnosti doskonaloi' formy systemy zalyshkovyh klasiv, *Pytannja optymizacii' obchyslen': HHHV Mizhnarodnyj sympozium, Kacyveli, 24–29 veresnja 2009 r. : tezy dopovidej*. Kyi'v, Instytut kibernetyky im. V. M. Glushkova, 2009, pp. 306–310.
13. Kasianchuk M., Yakymenko I., Pazdriy I. et al. Algorithms of findings of perfect shape modules of remaining classes system, *The Experience of Designing and Application of CAD Systems in Microelectronics : XIII International Conference, Polyana-Svalyava, 23–25 February 2015 : Proceedings*. L'viv, Lviv Polytechnic National University, 2015, pp. 168–171.
14. Kasjanchuk M. M., Jakymenko I. Z., Pazdrij I. R. ta in. Analitychnyj poshuk moduliv doskonaloi' formy systemy zalyshkovyh klasiv ta i'h vykorystannja v kytajs'kij teoremi pro zalyshky, *Visnyk Hmel'nyc'kogo nacional'nogo universytetu : tehnichni nauky*, 2015, No. 1, pp. 170-176.
15. Nykolaychuk Ya. M., Kasianchuk M. M., Yakymenko I. Z. Theoretical Foundations for the Analytical Computation of Coefficients of Basic Numbers of Krestenson's Transformation, *Cybernetics and Systems Analysis,* 2014, Vol. 50, No. 5, pp. 649–654. DOI: 10.1007/s10559-014-9654-0.
16. Nykolaychuk Ya. M., Kasianchuk M. M., Yakymenko I. Z. Theoretical Foundations of the Modified Perfect Form of Residue Number System, *Cybernetics and Systems Analysis,* 2016, Vol. 52, No. 2, pp. 219–223. DOI: 10.1007/s10559-016-9817-2.
17. Kasianchuk M. N., Nykolaychuk Y. N., Yakymenko I. Z. Theory and Methods of Constructing of Modules System of the Perfect Modified Form of the System of Residual Classes, *Journal of Automation and Information Sciences*, 2016, Vol. 48, No. 8, pp. 56–63. DOI: 10.1615/JAutomatInfScien.v48.i8.60.