УДК 519.7

Я.Н. НИКОЛАЙЧУК, М.Н. КАСЯНЧУК, И.З. ЯКИМЕНКО

ТЕОРЕТИЧЕСКИЕ ОСНОВЫ МОДИФИЦИРОВАННОЙ СОВЕРШЕННОЙ ФОРМЫ СИСТЕМЫ ОСТАТОЧНЫХ КЛАССОВ

Аннотация. Представлены теоретические основы модифицированной совершенной формы системы остаточных классов. Разработан метод подбора системы из трех модулей, которые образуют модифицированную совершенную форму системы остаточных классов, что исключает поиск обратного элемента по модулю и существенно упрощает процесс перевода чисел из системы остаточных классов в десятичную систему счисления.

Ключевые слова: система остаточных классов, система модулей, модифицированная совершенная форма, диапазон вычислений, обратный элемент по модулю, китайская теорема об остатках.

ВВЕДЕНИЕ

В настоящее время основным требованием к устройствам вычислительной техники, обеспечивающим выполнение математических операций над многоразрядными числами [1], является их высокое быстродействие [2]. В современных вычислительных системах наиболее распространенной является двоичная система счисления. Однако ее использование исчерпывает свои возможности и не может привести к скачкообразному повышению быстродействия [3]. Это обусловлено ее большой разрядностью, наличием межразрядных переносов и строго последовательной структурой [4]. Известно, что наиболее перспективным методом повышения быстродействия является распараллеливание процесса обработки информации [5]. Этим свойством обладают некоторые непозиционные системы счисления, в частности система остаточных классов (СОК) [6]. Хотя она имеет определенные недостатки (отсутствие операций деления и сравнения чисел, трудности при определении переполнения разрядной сетки, сложность перевода чисел в десятичную систему счисления и т.п.), однако свойство малоразрядности модулей СОК позволяет эффективно выполнять операции сложения, вычитания, умножения, возведения в степень над большими числами [7], что является важным, в частности относительно задач асимметричной криптографии [8].

ТЕОРЕТИЧЕСКИЕ ОСНОВЫ СИСТЕМЫ ОСТАТОЧНЫХ КЛАССОВ

Десятичному числу N в СОК соответствуют наименьшие неотрицательные остатки b_i этого числа в системе взаимно простых модулей p_i, т.е. $b_i = N \bmod p_i$ [7]. При этом диапазон вычислений должен находиться в пределах $0 \le N \le P-1$, где $P = \prod_{i=1}^{n} p_i$.

Обратное преобразование в десятичную систему счисления происходит согласно китайской теореме об остатках [9]:

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

где $B_i = M_i m_i$, $M_i = P / p_i$, базисные числа m_i находятся из выражения $(M_i m_i) \bmod p_i = 1$.

Необходимость вычисления базисных чисел $m_i = M_i^{-1} \bmod p_i$ существенно увеличивает сложность перевода чисел из СОК в десятичную систему. Упрощение этой задачи происходит в совершенной форме СОК (СФ СОК) [6], когда модули p_i подбираются таким образом, чтобы все m_i стали равны единице за счет исключения операций поиска обратного элемента по модулю и умножения на базисные числа m_i. В работах [10, 11] была развита теория СФ СОК и предложен метод для определения соответствующей системы модулей. В [12] описаны условия для аналитического вычисления базисных чисел. Однако в случае ограниченного количества модулей или необходимости использования модулей, которые мало отличаются один от другого, эти методы неприменимы. В работе [13] предложена модифицированная СФ СОК (МСФ СОК), в которой $m_i = \pm 1$, что также исключает необходимость поиска обратного элемента по модулю и умножения на базисные числа. Однако теоретические методы расчета системы модулей, которые удовлетворяют условиям МСФ СОК, отсутствуют.

Исходя из вышесказанного, цель настоящей статьи — развитие теории и методов нахождения системы модулей для МСФ СОК.

РАЗРАБОТКА ТЕОРЕТИЧЕСКИХ ОСНОВ ПОИСКА МОДУЛЕЙ МСФ СОК

Для упрощения ограничимся рассмотрением трех взаимно простых модулей: p_1, p_2, p_3. Согласно свойствам МСФ СОК запишем систему конгруэнций:

$$\begin{cases} p_2 p_3 \bmod p_1 = \pm 1, \\ p_1 p_3 \bmod p_2 = \pm 1, \\ p_1 p_2 \bmod p_3 = \pm 1. \end{cases} \tag{2}$$

Обозначим разность $p_2 - p_1 = a$ и представим модули в виде $p_1 = an - b$, $p_2 = a(n+1) - b$, где $n = 1, 2, 3$, ... ; числа a и b являются взаимно простыми.

Итак, необходимо отыскать модуль p_3, который будет удовлетворять системе (2). Решение системы (2) в общем случае является достаточно громоздким, поэтому в целях упрощения раскрытия сути предложенного метода используем численные расчеты.

Пусть $a = 5$, $b = 2$. Тогда $p_1 = 5n - 2$, $p_2 = 5n + 3$. Первые два уравнения системы (2) имеют вид

$$\begin{cases} 5p_3 \bmod (5n-2) = \pm 1, \\ 5p_3 \bmod (5n+3) = \pm 1. \end{cases} \tag{3}$$

Обратные элементы $\pm 5^{-1} \bmod (5n-2)$ и $\pm 5^{-1} \bmod (5n+3)$ можно найти из алгоритма Евклида [14] :

$$5n - 2 = 5(n-1) + 3,$$

$$5 = 3 \cdot 1 + 2,$$

$$3 = 2 \cdot 1 + 1$$

и его следствия

$$1 = 3 - 1 \cdot 2 = 3 - 1 \cdot (5 - 1 \cdot 3) = -1 \cdot 5 + 2 \cdot 3 = -1 \cdot 5 + 2 \cdot ((5n-2) -$$

$$-5(n-1)) = 2 \cdot (5n-2) - 5 \cdot (2n-1) = 1.$$

(Приводится пример расчета только для одного из уравнений системы (3).)

Итак, $5^{-1} \bmod (5n-2) = -(2n-1) \bmod (5n-2) = 3n-1$. Аналогично можно показать, что $5^{-1} \bmod (5n+3) = -(2n+1) \bmod (5n+3) = 3n+2$.

Следует отметить, что в данном случае обратный элемент более удобно находить способом, описанным в [15]. К единице следует добавлять модуль, пока

результат ни станет кратным 5, т.е. добавив к единице три модуля $(5n-2)$, получим $(15n-6)+1$. После его деления на 5 имеем обратный элемент: $(3n-1)$. Аналогичная процедура для второго модуля: $1+3\cdot(5n+3)=15n+10$, обратный элемент будет равен $(3n+2)$.

В соответствии с этим система (3) трансформируется в систему, удобную для использования китайской теоремы об остатках, причем необходимо рассмотреть четыре разных случая, которые соответствуют каждому остатку из каждого уравнения:

$$\begin{cases} p_3 \bmod (5n-2) = 3n-1 \text{ или } 2n-1, \\ p_3 \bmod (5n+3) = 3n+2 \text{ или } 2n+1. \end{cases} \tag{4}$$

Исходя из (4), необходимо найти число, которое при делении на $(5n-2)$ дает остаток $(3n-1)$ или $(2n-1)$, а при делении на $(5n+3)$ — остаток $(3n+2)$ либо $(2n+1)$. Для использования китайской теоремы об остатках снова необходимо рассмотреть алгоритм Евклида:

$$5n+3=(5n-2)+5,$$

$$5n-2=5\cdot(n-1)+3,$$

$$5=3\cdot 1+2,$$

$$3=2\cdot 1+1$$

и его следствия:

$$1=3-1\cdot 2=3-1\cdot(5-1\cdot 3)=-1\cdot 5+2\cdot 3=-1\cdot 5+2\cdot((5n-2)-5(n-1))=$$

$$=2\cdot(5n-2)-5\cdot(2n-1)=2\cdot(5n-2)-(2n-1)((5n+3)-(5n-2))=$$

$$=2\cdot(5n-2)-(2n-1)(5n+3)+(2n-1)(5n-2)=-(2n-1)(5n+3)+(2n+1)(5n-2).$$

Для нахождения возможного значения модуля p_3 необходимо проанализировать каждый из четырех случаев:

1) $(-(2n-1)(5n+3)(3n-1)+(2n+1)(5n-2)(3n+2)) \bmod ((5n+3)(5n-2))=$
$=(30n^2+6n-7) \bmod (25n^2+5n-6)=5n^2+n-1$;

2) $(-(2n-1)^2(5n+3)+(2n+1)^2(5n-2)) \bmod ((5n+3)(5n-2))=$
$=(20n^2+4n-5) \bmod (25n^2+5n-6)=20n^2+4n-5$;

3) $(-(2n-1)(5n+3)(2n-1)+(2n+1)(5n-2)(3n+2)) \bmod ((5n+3)(5n-2))=$
$=(10n^3+31n^2+3n-7) \bmod (25n^2+5n-6)=10n^3+6n^2-2n-1$;

4) $(-(2n-1)(5n+3)(3n-1)+(2n+1)(5n-2)(2n+1)) \bmod ((5n+3)(5n-2))=$
$=(-10n^3+19n^2+7n-5) \bmod (25n^2+5n-6)=(-10n^3-6n^2+2n+1)$.

Таблица 1

b	Выражение для нахождения системы модулей p_n и диапазона P			
	p_1	p_2	p_3	P
1	$5n-1$	$5n+4$	$5n^2+3n-1$	$125n^4+150n^3-27n+4$
2	$5n-2$	$5n+3$	$5n^2+n-1$	$125n^4+50n^3-50n^2-11n+6$
3	$5n-3$	$5n+2$	$5n^2-n-1$	$125n^4-50n^3-50n^2+11n+6$
4	$5n-4$	$5n+1$	$5n^2-3n-1$	$125n^4-150n^3+27n+4$

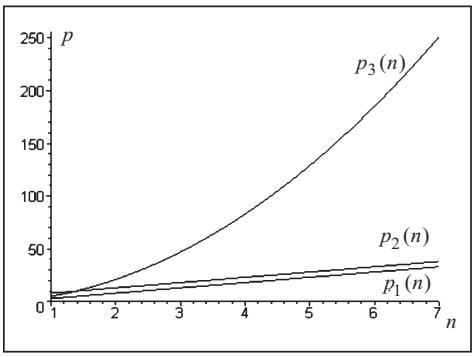

Рис. 1. Графики зависимости модулей p_1, p_2, p_3 от n при $b = 2$

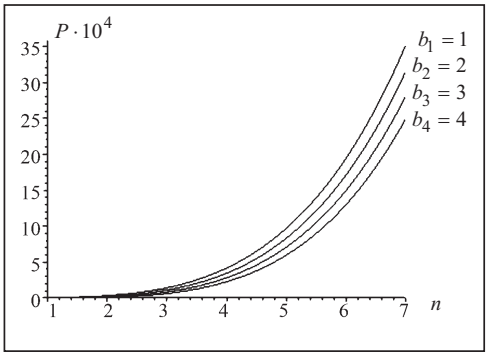

Рис. 2. Графики зависимости диапазона вычислений P от параметра n при разных значениях b

Таблица 2

Значение параметра		Численные значения модулей p_n и диапазона P			
n	b	p_1	p_2	p_3	P
1	3	2	7	3	42
	2	3	8	5	120
	1	4	9	7	252
2	4	6	11	13	858
	3	7	12	17	1428
	2	8	13	21	2184
	1	9	14	25	3150
3	4	11	16	35	6160
	3	12	17	41	8364
	2	13	18	47	10998
	1	14	19	53	14098
4	4	16	21	67	22512
	3	17	22	75	28050
	2	18	23	83	34362
	1	19	24	91	41496

Далее необходимо проверить выполнение третьего уравнения системы (2). Непосредственной подстановкой можно убедиться, что данное условие удовлетворяет результату, полученному только в первом случае:

$$(25n^2 + 5n - 6) \bmod (5n^2 + n - 1) = -1.$$

Аналогично можно рассчитать модуль p_3 для любого значения b. В табл. 1 представлены аналитические выражения для нахождения системы модулей МСФ СОК и диапазона возможных вычислений при разных b и n.

На рис. 1 приведены графики зависимости модулей p_1, p_2, p_3 от n при $b = 2$. Отсюда следует, что согласно табл. 1 графики для p_1 и p_2 параллельны и возрастают линейно, а для p_3 возрастает параболически. Следует отметить, что при остальных значениях b характер графиков не изменяется.

На рис. 2 показан график зависимости диапазона вычислений P от n при разных возможных значениях параметра b. Диапазон вычислений согласно табл. 1 возрастает пропорционально n^4, причем тем интенсивнее, чем меньше b.

В табл. 2 даны численные значения модулей p_1, p_2, p_3 и P при $a = 5$ для разных величин параметров n и b.

Из рис. 1 и табл. 2 видно, что при $n = 1$ между модулями справедливо соотношение $p_1 < p_3 < p_2$, в остальных случаях модуль p_3 является наибольшим. Кроме того, при постоянной n и изменении b на единицу значение модуля p_3 изменяется на величину $2n$, что следует также из данных табл. 1.

ЗАКЛЮЧЕНИЕ

Исходя из вышесказанного можно сделать вывод, что МСФ СОК является перспективной для использования в современных вычислительных системах, особенно при выполнении арифметических операций над многоразрядными числами. Впервые разработан метод подбора системы из трех модулей, кото-

рые образуют МСФ СОК, что исключает поиск обратного элемента и существенно уменьшить количество операций, необходимых для перевода чисел из СОК в десятичную систему исчисления.

СПИСОК ЛИТЕРАТУРЫ

1. Задірака В.К., Олексюк О.С. Комп'ютерна арифметика багаторозрядных чисел. — К.: [б.в.], 2003. — 264 с.
2. Николайчук Я.Н., Шевчук Б.М., Воронич А.Р., Заведюк Т.А., Гладюк В.Н. Теория надежной и защищенной передачи данных в сенсорных и локально-региональных сетях // Кибернетика и системный анализ. — 2014. — **50**, № 2. — С. 161–174.
3. Kasyanchuk M., Yakymenko I., Nykolaychuk Ya. Matrix algorithms of processing of the information flow in computer systems based on theoretical and numerical Krestenson's basis // Proceedings of the X International Conference "Modern Problems of Radio Engineering, Telecommunications and Computer Science" (TCSET-2010). — L'viv–Slavske, 2010. — P. 241.
4. Рабинович З.Л., Раманаускас В.А. Типовые операции в вычислительных машинах. — К.: Техніка, 1980. — 264 с.
5. Yatskiv V., Yatskiv N., Su Jun, Sachenko A., Hu Zhengbing. The use of modified correction code based on residue number system in WSN // Proceedings of the 7-th 2013 IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems (IDAACS'2013). — Berlin, Germany. — 2013. — **1.** — P. 513–516.
6. Николайчук Я.Н. Теория источников информации. — Тернополь: ООО «Терно–граф», 2010. — 536 с.
7. Акушский И.Я., Юдицкий Д.И. Машинная арифметика в остаточных классах. — М.: Сов. радио, 1968. — 440 с.
8. Задірака В.К, Олексюк О.С. Комп'ютерна криптологія. — К.: [б.в.], 2002. — 504 с.
9. Бухштаб А.А. Теория чисел. — М.: Просвещение, 1966. — 384 с.
10. Kasianchuk M. Conception of theoretical bases of the accomplished form of Krestenson's transformation and its practical application // Proceedings of the 4-th International Conference "Advanced Computer Systems and Networks: Design and Application" (ACSN–2009). — L'viv, 2009. — P. 299–301.
11. Касянчук М. Концепция теоретических положений совершенной формы преобразования Крестенсона и его практическое применение // Оптико-электронные информационно-энергетические технологии. — 2010. — № 2 (20). — С. 43–48.
12. Николайчук Я.Н., Касянчук М.Н., Якименко И.З. Теоретические основы аналитического вычисления коэффициентов базисных чисел преобразования Крестенсона // Кибернетика и системный анализ. — 2014. — **50**, № 5. — С. 3–8.
13. Касянчук М.Н. Теория и математические закономерности совершенной формы системы остаточных классов // Труды Международного симпозиума «Вопросы оптимизации вычислений (ПОО–XXXV)». Т.1. — Киев–Кацивели, 2009. — С. 306–310.
14. Вербицкий О.В. Вступление в криптологию. — Львов: Науково-технічна література, 1998. — 248 с.
15. Касянчук М.Н., Николайчук Я.Н., Якименко И.З. Теория алгоритмов превращений китайской теоремы об остатках в матрично-разграниченном базисе Радемахера-Крестенсона. — Вестник Национального университета «Львовская политехника». Семинар «Компьютерные системы и сети». — 2010. — № 688. — С. 118–125.

Поступила 30.01.2015