УДК 004.75

Н.Г.Яцків канд. техн. наук, доц., О.О. Левценюк
Тернопільський національний економічний університет, Україна

АЛГОРИТМ МОДУЛЯРНОГО МНОЖЕННЯ НА ОСНОВІ СКОРОЧЕНИХ ТАБЛИЦЬ

N.G. Yatskiv Ph.D Assoc. Prof., O.O. Levtsenyuk

MODULAR MULTIPLICATION ALGORITHM BASED ON INCOMPLETE TABLES

Операція модулярного множення широко застосовується в криптографії (асиметричні алгоритми), в модулярних корегуючих кодах, в алгоритмах обробки даних в системі залишкових класів [1, 2]. Ефективність вказаних алгоритмів залежить від швидкодії виконання модулярного множення.

В залежності від апаратних засобів та розрядності чисел для виконання модулярного множення розроблені різні методи та алгоритми, зокрема, метод індексного множення, метод різниці квадратів, табличний метод, метод Шенхаге – Штрасена та алгоритм Фюрера [2, 3]. Алгоритм Шенхаге – Штрасена використовується для множення великих чисел за модулем чисел Ферма.

Табличний метод модулярного множення характеризується високою швидкодією, однак при великих значеннях модулів ($\log_2 p > 10$) потребує значних обсягів пам'яті для зберіганні таблиць.

Для вирішення даної задачі в роботі запропоновано алгоритм модулярного множення на основі неповних таблиць.

В більшості застосувань системи залишкових класів використовуються модулі розрядності $\log_2 p < 10$. Наприклад, множення двох 32 – х бітних двійкових чисел в системі залишкових класів замінюється паралельним множенням 8-ми 5-ти бітних чисел за модулями: 7, 11, 13, 17, 19, 23, 29, 31.

Нехай необхідно виконати множення виду $c = (a \times b) \bmod p$, де $0 \le a < p$, $0 \le b < p$, p – просте число, $\bmod p$ – операція обчислення залишку за модулем.

Табличний метод представимо у вигляді двовимірної таблиці розміром p на p. (табл.1).

Таблиця 1 – Множення чисел за модулем 11

	a									
b	1	2	3	4	5	6	7	8	9	10
	2	**4**	6	8	10	1	3	5	7	9
	3	6	**9**	1	4	7	10	2	5	8
	4	8	1	**5**	9	2	6	10	3	7
	5	10	4	9	**3**	8	2	7	1	6
	6	1	7	2	8	**3**	9	4	10	5
	7	3	10	6	2	9	**5**	1	8	4
	8	5	2	10	7	4	1	**9**	6	3
	9	7	5	3	1	10	8	6	**4**	2
	10	9	8	7	6	5	4	3	2	**1**

Оскільки дана таблиця є симетричною відносно діагоналі, то для виконання множення за модулем $p = 11$ достатньо зберігати 1 / 2 таблиці (табл. 2). Якщо $a > b$ то

для виконання множення $(a \times b) \bmod 11$, потрібно присвоїти a значення b, b значення a, і за таблицею знайти результат множення.

Алгоритм отримання результату множення при використанні 1 / 4 таблиці наступний: 1) $e = a + b$, якщо $e > p$, тоді $k = e - p$, отримуємо нові значення $a_1 = a - k$, $b_1 = b - k$ за якими знаходимо результат модулярного множення (табл.3).

Таблиця 2 – 1 / 2 таблиці множення чисел за модулем 11

	a									
b		2	3	4	5	6	7	8	9	10
	2	4								
	3	6	9							
	4	8	1	5						
	5	10	4	9	3					
	6	1	7	2	8	3				
	7	3	10	6	2	9	5			
	8	5	2	10	7	4	1	9		
	9	7	5	3	1	10	8	6	4	
	10	9	8	7	6	5	4	3	2	1

Таблиця 3 – 1 / 4 таблиці множення чисел за модулем 11

	a_1									
b_1		2	3	4	5	6	7	8	9	10
	2	4								
	3	6	9							
	4	8	1	5						
	5	10	4	9	3					
	6	1	7	2	8					
	7	3	10	6						
	8	5	2							
	9	7								
	10									

Наприклад: $a = 7$, $b = 8$, тоді $e = a + b = 7 + 8 = 15$, так як $15 > p$, то $k = 15 - 11 = 4$, $a_1 = 7 - 4 = 3$, $b_1 = 8 - 4 = 4$. Тоді, за таблицею 3, знаходимо правильний результат множення, який дорівнює 1; 2) якщо $e \le p$ і $a \le b$ - результат множення знаходимо за таблицею; 3) якщо $e \le p$ і $a > b$, то значення a, b міняємо місцями і результат множення знаходимо за таблицею 3.

Запропонований метод модулярного множення на основі скорочених таблиць дозволяє зменшити обсяг пам'яті для зберігання таблиць в 2 або 4 рази, при цьому зберігає високу швидкодію табличних методів.

Література

1. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. – М.: Триумф, 2002. – 816 с.

2. Яцків В. В. Методи виконання модулярних операцій та їх реалізація на ПЛІС / В. В. Яцків // Вісник Хмельницького національного університету. Технічні науки . - 2014. - № 6. - С. 218-224.

3. Николайчук Я.М. Теоретичні основи виконання модулярних операцій множення та експоненціювання в теоретико-числовому базисі Крестенсона-Радемахера/ Я.М. Николайчук, М.М. Касянчук, І.З. Якименко, Т.М. Долинюк // Інформатика та математичні методи в моделюванні. – 2011. – Том 1, № 2. – С. 123–130.

4. Модулярные параллельные вычислительные структуры нейропроцессорных систем /Н. И. Червяков, П. А. Сахнюк, А. В. Шапошников, С. А. Ряднов. Под редакцией Н.И. Червякова. – М.: Физматлит, 2003. – 288 с.