УДК 681.1

АЛГОРИТМ ФАКТОРИЗАЦІЇ НА ОСНОВІ ТЕОРЕМИ ФЕРМА

Якименко І.З.[1)], Івасьєв С.В.[2)], Петрица Н.П.[3)]
Тернопільський національний економічний університет
[1)] к.т.н., доцент, [2)] к.т.н., викладач, [3)]магістрант

І. Постановка проблеми

Факторизація є однією з найважливіших задач теорії чисел та сучасної асиметричної криптографії [1]. Її суть полягає у розкладі деякого цілого числа у добуток простих співмножників [2]. Відомі методи факторизації, в залежності від їх продуктивності, розбиваються на дві групи: експоненціальні та субекспоненціальні [3]. Всі вони досить громіздкі, тому вимагають значних обчислювальних ресурсів для опрацювання багаторозрядних чисел. Крім того, сьогоднішній інтерес до проблеми факторизації продиктований також невизначеністю щодо теоретичного обґрунтування стійкості до розкриття асиметричних криптосистем.

Найбільш розповсюдженими для факторизації є алгоритми що базуються на теоремі Ферма. Обчислювальна складність методу Ферма для великорозрядних чисел досить велика, оскільки кількість ітерацій може становити 2^{300} - 2^{400} і тільки на єдиному кроці можливе однозначне рішення задачі факторизації. Для спрощення цієї задачі доцільно використати систему залишкових класів (СЗК), яка дозволить виконати розпаралелення обчислень.

ІІ. Мета роботи

Мета роботи полягає в розробці алгоритму факторизації багаторозрядних чисел на основі арифметики теоретико - числового базису Радемахера – Крестенсона шляхом представлення цифрових даних у СЗК, застосування модульної арифметики, виключення операції добування кореня квадратного, що, в порівнянні з відомими методами, дає можливість зменшити розрядності операндів, спростити алгоритм пошуку факторизованих чисел та підвищити швидкодію алгоритму обчислень.

ІІІ. Метод факторизації великорозрядних чисел на основі теореми Ферма за допомогою використання властивостей квадратичності лишків

Метод Ферма описується наступним виразом:

$$\Delta_n = \sqrt{n^2 - P_0}\ , \tag{1}$$

де $n = \left\lfloor \sqrt{P_0} \right\rfloor + k$, k=1, 2, 3, … .

Відомо, що квадрати цілих чисел можна представити у вигляді суми непарних чисел, кількість яких дорівнює даному числу [2]:

$$n^2 = \sum_{i=1}^{n} (2i-1). \tag{2}$$

Тому, знайшовши Δ_n за формулою (1) при k=1, наступні ітерації виконуються згідно виразу

$$S_k = \sqrt{(\Delta_0)^2 + (2n-1)}.$$

Ітерації продовжуються до тих пір, поки параметр S_k не буде цілим числом, причому кількість ітерацій в обох методах однакова.

В таблиці 1 представлено приклад факторизації за допомогою класичного та удосконаленого методів Ферма для P_0=3811.

Таблиця1.

Приклад факторизації за допомогою класичного та удосконаленого методів Ферма для P_0=3811.

k	N	$(\Delta_n)^2$, класичний метод	$(\Delta_n)^2$, вдосконалений метод
1	62	62^2-3811=33	62^2-3811=33
2	63	63^2-3811=158	33+125=158
3	64	64^2-3811=285	158+127=285
4	65	65^2-3811=414	285+129=414
5	66	66^2-3811=545	414+131=545
6	67	67^2-3811=678	545+133=678

7	68	68^2-3811=813	678+135=813
8	69	69^2-3811=950	813+137=950
9	70	70^2-3811=1089=33^2	950+139=1089=33^2

Таким чином, отримано розклад числа 3811 на прості множники:

$3811 = 70^2 - 33^2 = (70 + 33)(70 - 33) = 103*37$.

З таблиці 1 видно, що у вдосконаленому методі виключається операція піднесення до квадрату. Крім того, арифметичні дії виконуються над числами, розмірність яких на декілька порядків менша, ніж у класичному методі. Однак слід зазначити, що кількість ітерацій в обох випадках буде однаковою, а найскладнішою залишається операція перевірки квадратичності лишку. Для зменшення її обчислювальної складності можна використати СЗК.

Розглянемо залишки квадратів цілих чисел по декількох простих модулях p_j, тобто $a_1(p_1, p_2, ..., p_m) = b_1^1, b_2^1, \ldots, b_m^1$, $a_2(p_1, p_2, ..., p_m) = b_1^2, b_2^2, \ldots, b_m^2$, $a_n(p_1, p_2, ..., p_m) = b_1^n, b_2^n, \ldots, b_m^n$, де $a_i = i^2$, $b_j^i = a_i (mod\ p_j), 1 \le i \le n,\ 1 \le j \le m$, m – кількість модулів.

Використовуючи властивість (3), шукані залишки можна отримувати за допомогою рекурентної формули $b_j^i = \left(b_j^{i-1} + z_i^j\right) mod\ p_j$, де $z_j^i = z_i\ mod\ p_j$, z_i=2i-1.

Відповідні результати по модулях 3, 5, 7, 11 представлені в таблиці 2.

Таблиця 2

Пошук залишків квадратів по простих модулях

n	z_i	a_n	p_1=3		p_2=5		p_3=7		p_4=11	
			z_1^i	b_1^i	z_2^i	b_2^i	z_3^i	b_3^i	z_4^i	b_4^i
1	1	1	1	1	1	1	1	1	1	1
2	3	4	0	1	3	4	3	4	3	4
3	5	9	2	0	0	4	5	2	5	9
4	7	16	1	1	2	1	0	2	7	5
5	9	25	0	1	4	0	2	4	9	3
6	11	36	2	0	1	1	4	1	0	3
7	13	49	1	1	3	4	6	0	2	5
8	15	64	0	1	0	4	1	1	4	9
9	17	81	2	0	2	1	3	4	6	4
10	19	100	1	1	4	0	5	2	8	1
11	21	121	0	1	1	1	0	2	10	0

З таблиці 2 видно, що кількість квадратичних лишків для кожного модуля становить (p_j+1)/2 (включаючи 0). Це випливає з рівності $n^2 mod\ p_j = (-n^2)\ mod\ p_j = (p_j - n)^2\ mod\ p_j$.

Отриманий з ознак квадратичності лишку вектор $Y(Y_1, Y_2, \ldots, Y_n)$, в якому Y_i=0 або 1, утворює ключ факторизації. В даному випадку Y(000000001). Це означає, що на дев'ятій ітерації можливий випадок, коли Δ_n буде цілим числом, що і підтверджують обчислення: $\sqrt{1089} = 33$.

Висновок

Дослідження показали, що вдосконалений алгоритм факторизації на основі використання елементарних операцій характеризується високою швидкодією та ефективністю.

Розроблений алгоритм факторизації на основі проведених досліджень, дозволяє змінити зону розрядностей обчислювальних ресурсів на декілька порядків нижче по шкалі квадратів та замінити операцію знаходження кореня квадратного, операції на якій базується обчислювальна складність алгоритму Ферма, на операцію порівняння.

Список використаних джерел

1. Kasianchuk M. Rabin's modified method of encryption using various forms of system of residual classes/ M. Kasianchuk,I. Yakymenko, I. Pazdriy, A. Melnyk, S.Ivasiev// XIV International Conference "The Experience of Designing and Application of CAD Systems in Microelectronics (CADSM-2017)", 21-25 February, 2017, Polyana-Svalyava (Zakarpattya), Ukraine. – P.222-224.
2. Karpinski M. Advanced method of factorization of multi-bit numbers based on Fermat's theorem in the system of residual classes / M. Karpiński, S. Ivasiev, I. Yakymenko, M. Kasianchuk ,T. Gancarczyk// Proc. of 16th International Conference on Control, Automation and Systems (ICCAS–2016) – Gyeongju, Korea. – V.1. – October, 2016. – P.1484–1486.
3. Ишмухаметов. Ш.Т. Методы факторизации натуральных чисел: учебное пособие / Ш.Т. Ишмухаметов.– Казань: Казан. ун. 2011.– 190 с.