4. Вимірювач дисперсності порошків AccuSizer 780 / DPF, Santa Barbara.
5. Laven Ph. Simulation of Rainbows, Coronas and Glories by use Mie Theory. Applied Optics, 2003, v.42, № 3, pp. 435-444.
6. Woo K.S., Romey F.J., Dick W.D., Liu Y.H. Measurement of Atmospheric Aerosols using the Wide-Range Particle Spectrometer (WPSTM).

Якименко І.З.
кандидат технічних наук, доцент;
Мачуляк М.В.
студент,
Тернопільський національний економічний університет

АЛГОРИТМ ВИЗНАЧЕННЯ ПРОСТИХ ТА ВЗАЄМНО ПРОСТИХ ЧИСЕЛ ВИДУ $2^N + K$

Визначення простих і взаємно простих чисел є однією з найважливіших задач теорії чисел [1] і сучасної асиметричної криптографії [2]. Існуючі підходи щодо вирішення задач даного класу базуються на використанні решета Еретосфена, ймовірносного тесту на простоту та алгоритмі Евкліда [3]. Функціональними обмеженнями даних алгоритмів є використання для обчислень багаторівневого базису Радемахера, який характеризуються часово складними операціями модульного ділення, множення та сумування з наскрізними переносами.

Крім того, актуальність проблеми визначення простих і взаємно простих чисел продиктована також невизначеністю щодо теоретичного обґрунтування стійкості асиметричних криптосистем [4].

Алгоритм визначення простих та взаємнопростих чисел

Запропонований алгоритм базується на рекурентному обчисленні залишків по заданому модулю шляхом отримання значення (табл. 1):

$$b_{i+1} = 2 \cdot b_i \,(\mathrm{mod}\, p). \qquad (1)$$

При цьому, стартова позиція рекурентної перевірки подільності числа на прості множники визначається згідно виразу:

$$res\, 2^i \,(\mathrm{mod}\, p) + res \sum_{j=0}^{n} 2^j \,(\mathrm{mod}\, p) \equiv 0 (\mathrm{mod}\, p). \qquad (2)$$

Результати реалізації пошуку простих чисел виду 2^n+3 представлено в таблиці 2.

Отримана аналітика простих чисел, які не задовольняють умову (2) ні по одному з простих модулів, які менші половини розрядності шуканого p, приведена в таблиці 2.

Таблиця 1

Пошук простих чисел виду 2^n+3, розклад на прості множники

131072		65536		32768		16384		8192		4096		2048		1024		512		256		128		64		32		16		8		4		2		1	
18		17		16		15		14		13		12		11		10		9		8		7		6		5		4		3		**2**		**1**	
5,7	1	107	1		1	7	1	5,11, 146	1		1	7	1	13, 79	1	5, 103	1	7, 37	1	131	1	67	1	5,7	1	19	1	11	1	7	1		**2**		**1**
7	1	13, 109	1	5,11	1	7, 131	1	83	1		1	5,7	1		1		1	7	1	5	1		1	7,11	1	13, 19	1	5	1	7, 59	1	29, 101	1		1
5,7, 11	1		1		1	7	1	79,5	1		1	7, 29	1	13	1	5	1	7, 37	1	11, 53	1		1	5,7	1	19, 97	1		1	7	1	5	1	61	1
7	1	13	1	5, 109	1	7	1		1		1	5,7	1		1	11	1	7, 137	1	5	1	103	1	7	1	13, 19	1	5, 131	1	7	1		1		1
5,7	1	79	1		1	7,	1	5	1		1	7, 11, 139	1	13, 131	1	5	1	7, 37	1	59	1		1	5,7,	1	19	1	29	1	7	1	5,11	1	67	1
7, 131	1	13	1	5	1	7, 109	1	11,29 53,97	1		1	5,7	1		1		1	7	1	5,83	1	61	1	7	1	13, 19	1	5,11	1	7	1		1		1
5,7	1	79	1	11	1	7	1	5	1		1	7, 101	1	13	1	5	1	7, 37	1		1		1	5,7, 11	1	19	1	103	1	7	1	5	1		1
7,11	1	13	1	5	1	7	1	109	1	67	1	5,7, 59	1		1		1	7	1	5, 11, 107	1	131	1	7,29	1	13, 19	1	5	1	7	1	79	1		1
5,7	1		1	29	1	7	1	5, 131	1	61	1	7	1	13	1	5,11	1	7, 37	1		1		1	5,7	1	19, 97	1		1	7	1	5	1		1
7	1	13	1	5	1	7	1		1	109	1	5,7, 11	1		1		1	7	1	5	1		1	7,53	1	13, 19, 79	1	5	1	7	1	11, 83	1	103	1
5,7, 139	1		1	59	1	7	1	5,11	1		1	7	1	13	1	5	1	7, 37	1	29	1		1	5,7	1	19	1	11	1	7, 131	1	5	1		1
7,29	1	13, 107	1	5,11, 103	1	7	1	97	1		1	5,7, 109, 137	1		1	131	1	7, 37	1	5, 79	1	67	1	7,11	1	13, 19	1	5	1	7	1		1		1
5,7, 11	1	131	1		1	7	1	5,83	1		1	7	1	13	1	5, 53	1	7	1	11	1		1	5,7	1	19	1	101	1	7	1	5	1	61	1
7	1	13	1	5	1	7	1		1		1	5,7	1	79, 109	1	11,29	1	7, 37	1	5	1		1	7	1	13, 19	1	5	1	7	1		1		1

Слід зазначити, що в результаті заповнення табличних даних комірки, які залишилися незаповненими, відповідають простим числам виду 2^n+3, а всі інші числа є складеними.

Слід зазначити, що на основі використання таблиці 1 було побудовано таблицю 2, яка дозволяє знаходити взаємно прості числа та вирішувати задачу факторизації чисел виду 2^n+3.

Таблиця 2

Аналітика простих та взаємно простих чисел

Прості числа	Вирази виду 2^n+1, які діляться на прості числа	Вирази виду 2^n+3, які діляться на прості числа	Вирази виду 2^n+5, які діляться на прості числа	Вирази виду 2^n+11, які діляться на прості числа	Вирази виду 2^n+13, які діляться на прості числа
3	$2^{2n+1}+1$	-	-	-	-
5	$2^{4n+2}+1$	$2^{4n+1}+3$	-	-	-
7	-	$2^{3n+2}+3$	-	-	-
11	$2^{10n+5}+1$	$2^{10n+3}+3$	$2^{10n+9}+5$	-	-
13	$2^{12n+6}+1$	$2^{12n+10}+3$	$2^{12n+3}+5$	$2^{12n+2}+11$	-
17	$2^{8n+4}+1$	-	-	-	$2^{8n+3}+13$
19	$2^{18n+9}+1$	$2^{18n+4}+3$	$2^{18n+7}+5$	$2^{18n+4}+11$	$2^{18n+15}+13$
23	-	-	$2^{11n+6}+5$	$2^{11(n+1)}+11$	-
29	$2^{28n+14}+1$	$2^{28n+19}+3$	$2^{28n+8}+5$	$2^{28n+12}+11$	$2^{28n+5}+13$
31	-	-	-	-	-
37	$2^{36n+18}+1$	$2^{36n+8}+3$	$2^{36n+5}+5$	$2^{36n+13}+11$	$2^{36n+30}+13$
41	$2^{20n+10}+1$	-	$2^{20n+17}+5$	-	-
43	$2^{14n+7}+1$	-	-	$2^{14n+6}+11$	-
47	-	-	$2^{23n+9}+5$	$2^{46n+18}+11$	$2^{23n+8}+13$
53	$2^{52n+26}+1$	$2^{52n+43}+3$	$2^{52n+21}+5$	$2^{52n+32}+11$	$2^{52n+51}+13$
59	$2^{58n+29}+1$	$2^{58n+21}+3$	$2^{58n+35}+5$	$2^{58n+55}+11$	$2^{58n+17}+13$
61	$2^{60n+30}+1$	$2^{60n+36}+3$	$2^{60n+52}+5$	$2^{60n+46}+11$	$2^{60n+11}+13$
67	$2^{66n+33}+1$	$2^{66n+6}+3$	$2^{66n+48}+5$	$2^{66n+27}+11$	$2^{66n+53}+13$
71	-	-	-	$2^{35n+12}+11$	-
73	-	-	-	-	-
79	-	$2^{39n+10}+3$	-	-	-
83	-	$2^{82n+31}+3$	$2^{82n+51}+5$	$2^{82n+49}+11$-	-
89	-	-	-	$2^{11n+9}+11$	-
97	$2^{45n+24}+1$	$2^{45n+40}+3$	-	-	-
101	$2^{100n+50}+1$	$2^{100n+19}+3$	$2^{100n+74}+5$	$2^{100n+65}+11$	$2^{100n+17}+13$

Запропонований підхід дозволяє визначати аналітичні вирази вигляду 2^n+k, які є складеними, тобто їх можна факторизувати.

В роботі пропонується алгоритм визначення простих і взаємно простих чисел виду $2^n + k$, який на відміну від існуючих, шляхом рекурентного обчислення залишків по заданому модулю та з врахуванням стартової позиції рекурентної перевірки подільності числа на прості множники дозволяє вирішувати задачі даного класу. Отримані аналітичні вирази вказують на те, які з чисел є взаємно прості та складені.

Список використаних джерел:

1. Omondi A. Residue Number System: Theory and Implementation / A. Omondi, B. Premkumar. – Imperial College Press, 2007,Vol. 2, 296 p.

2. Романец Ю. В. Защита информации в компьютерных системах и сетях / Ю.В. Романец, П.А. Тимофеев, В.Ф. Шаньгин. – М.: Радио и связь, 2001. – 376 с.

3. Menezes A. Handbook of Applied Cryptography. // A. Menezes, P. van Oorschot, S. Vanstone / CRC Press., 2003. – Pp. 780.

4. Задірака В. Комп'ютерна криптологія: підручник / В. Задірака, О. Олексюк – К.: 2002. – 504 с.