УДК 581.3
М.В. Мачуляк, В.Р. Слободян, В.В. Пекельна, І.А. Фольварков
Тернопільський національний економічний університет, Україна

АЛГОРИТМ ПЕРЕВІРКИ ЧИСЕЛ НА ПРОСТОТУ В СИСТЕМІ ЗАЛИШКОВИХ КЛАСІВ

M.V. Machulyak, V.R. Slobodyan, V.V. Pekelna, I.A. Folvarkov

ALGORITHM FOR PRIME VERIFICATION NUMBERS IN THE RESIDUAL CLASSES BASED

Відрізнити просте число від складеного, а також розкласти останнє на прості множники є однією з найважливіших задач арифметики. Пошук великих простих чисел необхідний, наприклад, для забезпечення надійності систем захисту інформації з відкритим ключем. Безпека останніх базується на твердженні, що операція множення двох великих простих чисел є односторонньою функцією.

На сьогоднішній час перевірка простоти числа здійснюється на основі ймовірнісних тестів Ферма, Соловей – Штрасена, Мілера – Рабіна, які відзначаються значною обчислювальною складністю.

Основною ідеєю тесту Ферма перевірки на простоту є використання теореми Ферма згідно якої, якщо n – просте, то для довільного a, $1 \leq a \leq n - 1$ має місце рівність $a^{n-1} \equiv 1 (\mathrm{mod}\ n)$ в іншому n не є простим [1].

У тесті на простоту Соловай – Штрасена використовується критерій Ейлера: якщо n – просте, то $a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right) (\mathrm{mod}\ n)$ для всіх значень a, для яких НСД(a, n) = 1. Слід зазначити, що в даному підході потрібно перевіряти чи $\left(\frac{a}{n}\right)$ буде квадратичним лишком, тобто обчислювати символ Якобі [2].

Тест Мілера – Рабіна найбільш часто використовується на практиці та називається сильним тестом на простоту. Він базується на наступному факті: нехай n – непарне просте число, при чому $n - 1 = 2^s * r$, де r – непарне, a –натуральне число, яке взаємнопросте з n, тобто НСД(a, n) = 1. Тоді має місце одна із рівностей: $a^r \equiv 1 (\mathrm{mod}\ n)$, або $a^{2^j r} \equiv -1 (\mathrm{mod}\ n)$ для деякого j, $0 \leq j \leq s - 1$[1]. Враховуючи те, що в даному методі є операції модулярного експоненціювання, що призводить до значної обчислювальної складності $O(nLog_2{}^2 n)$.

Функціональними обмеженнями даних алгоритмів є використання для обчислень багаторівневого базису Радемахера, які характеризуються складними операціями модульного ділення, множення та сумування з наскрізними переносами. Використання системи числення залишкових класів призведе до зменшення часових затрат та дозволить аналітично встановити подільність чисел типу Мерсена [3]. Запропонований алгоритм в системі числення залишкових класів базується на рекурентному обчисленні залишків по заданому модулю згідно співвідношення:

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

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

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

Результати реалізації даного алгоритму представлено в таблиці 1.

Таблиця 1. Аналітика простих та взаємно простих чисел виду $2^n + \kappa$.

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	-	$2^{39n+10}+3$	-	-	-

Незаповнені дані в таблиці1 свідчать про те, що не існує чисел виду $2^n + \kappa$ які б ділилися на відповідні прості числа. Отже, відповідна запропонований алгоритм дозволяє суттєво скоротити час перевірки простоти чисел та на основі розробленої аналітики вказати прості дільники.

Література

1. Бородін О.І. Теорія чисел / О.І.Бородін. – К.: Вища школа, 1970. – 275 с.
2. Карпінський М.П., Якименко І.З., Хомінчук А.В. Використання символів Якобі в криптографії ЕК. III Міжнародна науково-технічна конференція "Світ інформації та телекомунікацій-2006" Київ, ДУІКТ 26-27 квітня 2006 р. – С.208.
3. Kasianchuk M. Algorithms of findings of perfect shape modules of remaining classes system / M.Kasianchuk, I.Yakymenko, I.Pazdriy, O.Zastavnyy // Proceedings of the XIII-th International Conference “The Experience of Designing and Application of CAD Systems in Microelectronics (CADSM-2015)”. - Polyana-Svalyava (Zakarpattya), Ukraine.- 2015. - P.168-171.
4. Николайчук Я.М., Якименко І.З., Долинюк Т.М. Теоретичні основи виконання модулярних операцій множення та експоненціювання в теоретико–числовому базисі Крестенсона–Радемахера. Інформатика та математичні методи в моделюванні. – №2. – 2011. – с. 123–130.