УДК 004.056.5

Олександр ДРОЖАК

Західноукраїнський національний університет

АНАЛІЗ ТЕСТІВ ПРОСТОТИ ФЕРМА ТА МІЛЛЕРА-РАБІНА

Вступ. Аналіз тестів простоти числа є важливим аспектом у теорії чисел та криптографії, оскільки ефективне визначення простоти числа має ключове значення для безпеки сучасних криптографічних алгоритмів. Розвиток швидких і точних методів тестування простоти чисел дозволяє знижувати обчислювальні витрати при роботі з великими числами, що є критичним для практичних застосувань, таких як генерація ключів у криптографії.

Актуальність таких тестів також зростає з урахуванням потреб у безпечному зберіганні даних та захисті інформації в цифрову епоху.

Метою аналізу тестів простоти Ферма та Тесту Міллера-Рабіна є оцінка їх ефективності, точності та надійності при визначенні простоти великих чисел.

1. Тест Ферма

Тест Ферма дозволяє швидко виявити складні числа, але може давати хибнопозитивні результати, що робить його менш надійним для великих чисел.

За теоремою Ферма, якщо n – просте число, тоді будь-якого a справедливо така рівність

$$a^{n-1}=1 \pmod{n}.$$

Звідси ми можемо вивести правило тесту Ферма на перевірку простоти числа: візьмемо випадкове

$$a \in \{1, ..., n-1\}$$

і перевіримо чи дотримуватиметься рівність

$$a^{n-1}=1 \pmod{n}.$$

Якщо рівність недотримується, отже швидше за все n – складове.

Проте умова рівності може бути дотримано, навіть якщо n – не просте. Наприклад, візьмемо $n = 561 = 3 \times 11 \times 17$. Відповідно до Китайської теореми про залишки:

$$Q_{561} = Q_3 \times Q_{11} \times Q_{17},$$

де кожне $a \in Q*_{561}$ відповідає наступному:

$$(x,y,z) \in Q*_3 \times Q*_{11}11 \times Q*_{17}.$$

По теоремі Ферма

$$x^2=1,\ y^{10}=1 \text{ і } z^{16}=1.$$

Оскільки 2, 10 і 16 всі є дільниками 560, це означає, що $(x, y, z)^{560} = (1, 1, 1)$, тобто $a^{560} = 1$ для будь-якого $a \in Q*_{561}$.

Не має значення яке ми виберемо, 561 завжди буде проходити тест Ферма незважаючи на те, що воно складене, доки a є взаємно простим з n. Такі числа називаються числами Кармайкла і встановлено, що їх існує безліч.

Якщо a не взаємно просте з n, воно тест Ферма не проходить, але в цьому випадку ми можемо відмовитися від тестів і продовжити шукати дільники n,

обчислюючи НСД(a,n).

2. Тест Міллера-Рабіна

Тест Міллера-Рабіна, у свою чергу, є більш точним і менш схильний до помилок, що робить його одним з найбільш використовуваних методів для перевірки простоти в криптографії. Аналіз цих тестів сприяє вибору оптимального алгоритму для застосувань, де важлива швидкість та точність перевірки простоти чисел.

Можна вдосконалити тест, сказавши, що n - просте тоді і тільки тоді, коли рішеннями

$$x^2 = 1 \pmod{n} \text{ є } x = \pm 1.$$

Таким чином, якщо n проходить тест Ферма, тобто

$$a^n - 1 = 1,$$

тоді ми ще перевіряємо щоб

$$a^{(n-1)/2} = \pm 1,$$

оскільки

$$a^{(n-1)/2}$$

це квадратний корінь 1.

На жаль, такі числа, як, наприклад 1729 - третє число Кармайкла, досі можуть обдурити цей покращений тест. Можливим вдосконаленням буде проведення ітерацій. Тобто поки це буде можливо, зменшуватимемо експоненту вдвічі, доки не дійдемо до якогось числа, крім 1. Якщо ми отримаємо в результаті щось, крім -1, тоді n буде складним. Якщо говорити формальніше, то нехай 2^S буде найбільшим ступенем 2, що ділиться на n-1, тобто

$$n - 1 = 2^S q$$

для якогось непарного числа q.

Кожне число із послідовності

$$a^{n-1} = a^{(2\text{^}S)q}, a^{(2\text{^}S\text{-}1)q}, \ldots, aq.$$

Це квадратний корінь попереднього члена послідовності.

Тоді якщо n – просте число, то послідовність повинна починатися з 1 і кожне наступне число теж має бути 1, або перший член послідовність може бути не дорівнює 1, але тоді він дорівнює -1.

Тест Міллера-Рабін бере випадкове $a \in Z_n$. Якщо вищезазначена послідовність не починається з 1, або перший член послідовності не дорівнює 1 або -1, тоді n - не просте.

Виявляється, що для будь-якого складеного n, включаючи числа Кармайкла, можливість пройти тест Міллера-Рабіна дорівнює приблизно 1/4. (У середньому значно менше.) Таким чином, ймовірність того, що n пройде декілька прогонів тесту, зменшується експонентно.

Якщо n не проходить тест Міллера-Рабіна з послідовністю, що починається з 1, тоді у нас з'являється нетривіальний квадратний корінь з 1 по модулю n, і ми можемо ефективно знаходити дільники n. Тому числа Кармайкла завжди зручно розкладати на множники.

Коли тест застосовується до чисел виду pq, де p і q - великі прості числа,

вони не проходять тест Міллера-Рабіна практично у всіх випадках, оскільки послідовність не починається з 1.

На практиці тест Міллера-Рабіна реалізується так:

Дано n, потрібно знайти s, що

$$n - 1 = 2^S q$$

для деякого непарного q.

Візьмемо випадкове

$$a \in \{1,...,n-1\}$$

Якщо $a^q = 1$, n проходить тест і припиняємо виконання. Для $i = 0, \ldots, s-1$ перевірити рівність

$$a^{(2\wedge i)q} = -1.$$

Якщо рівність виконується, то n проходить тест (припиняємо виконання).Якщо жодна з вищенаведених умов не виконана, то n – складене.

Перед виконанням тесту Міллера-Рабін варто провести ще кілька тривіальних поділів на маленькі прості числа. Строго кажучи ці тести є тестами на те чи вважається число складеним, оскільки вони не доводять по суті, що число просте, що перевіряється, але точно доводять, що воно може виявитися складовим.

Існують ще детерміновані алгоритми, які працюють за поліноміальний час для визначення простоти (Agrawal, Kayal і Saxena), проте на сьогоднішній день вони вважаються непрактичними.

Висновок. Аналіз тестів простоти Ферма та Міллера-Рабіна показує, що кожен з них має свої переваги та обмеження. Тест Ферма є швидким, але може давати хибнопозитивні результати для псевдопростих чисел, що обмежує його надійність при перевірці великих чисел. Тест Міллера-Рабіна, в свою чергу, є більш точним і менш схильним до помилок, тому його часто використовують як основний метод у криптографії. Враховуючи це, оптимальним є використання тесту Міллера-Рабіна в поєднанні з іншими методами для досягнення високої точності при визначенні простоти чисел.

Перелік використаних джерел.

1. J.P. Buhler Algorithmic Number Theory: Proc. ANTS-III – Portland, OR, v.1423, Lect.Not.Comp.Sci. Springer–Verlag, 1998, 640 p.

2. D. Venturi Lecture Notes on Algorithmic Number Theory. – Springer-Verlag, New-York, Berlin, 2009, 217 p.

3. Sh.T. Ishmukhametov Methods of factorization of natural numbers: a tutorial.– Kazan, Kazan University, 2011, 190 p.

4. Ya.M.Nikolaichuk, Kasianchuk M.M., Yakymenko I.Z., Ivasiev S.V Vector and modular method of multiplication of multidigit numbers in RademacherKrestenson basis. Herald of the National University "Lviv Polytechnic" "Computer systems and networks", no. 694, 2014, pp. 118–125.

5. M.Kasyanchuk, I. Yakymenko, Y.Nykolajchuk. Matrix Algorithm of Processing of the Information Flow in Computer Systems Based on Theoretical and Numerical Krestenson's Based. Proceedings of the Integrational Conference TCSET'2010, February 23-27, 2010, p. – C: 241