УДК 511

Медведев М, Г.

ЙМОВІРНІСНІ ТЕСТИ НА ПРОСТОТУ

Проблема визначення простоти числа є однією із найважливіших в теорії чисел та криптографії. В цій статті наведено ймовірнісні тести на простоту - тести Ферма, Соловай-Штрасена та Мілера-Рабіна. Для кожного тесту визначено поняття «брехунців» та наведено твердження про їх властивості.

Проблема визначення належності заданого натурального числа до класу простих чи складених чисел є дуже цікавою не тільки в математиці, а й у комп'ютерних науках. 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 кодування інформації з відкритим ключем. Безпека останніх базується на тому факті, що операція множення двох великих простих чисел є односторонньою функцією.

Для перевірки чисел на простоту користуються ймовірнісними тестами: Ферма, Соловай-Штрасена, Мілера-Рабіна.

Тест на простоту називається *ймовірнісним,* якщо в результаті його застосування не можна дати чіткої відповіді на запитання «чи є задане число простим, чи ні?», але можна виявити часткову інформацію стосовно простоти.

Наведені нижче тести дають таку інформацію про непарне ціле число *n:*

- якщо тест визначає, що *n* є складеним, то це дійсно так;
- якщо тест визначає, що *n* є простим, то зі ймовірністю, близькою до 1, можна вважати, що число є простим.

Тест Ферма

Тест базується на теоремі Ферма, яка стверджує, що якщо n – просте, то для довільного a, $1 \le a \le n-1$, має місце рівність $a^{n-1} \equiv 1 (\mathrm{mod}\ n)$. Якщо для заданого n знайдеться хоча б одне таке a, що $a^{n-1} \neq 1 (\mathrm{mod}\ n)$, то n не є простим.

Означення. Нехай n – непарне складене число. Число a, $1 \le a \le n-1$, таке що $a^{n-1} \neq 1 \pmod n$, називається *свідком Ферма* (свідком складеності) для n.

Означення. Нехай n – непарне складене число, a – ціле число, $1 \le a \le n-1$. Число n називається *псевдопростим* за основою a, якщо $a^{n-1} \equiv 1 \pmod n$. Число a називається *брехунцем Ферма* (брехунцем простоти) для n. Кількість брехунців Ферма для числа n будемо позначати через $\mathrm{fl}(n)$ (Ferma liars).

Наприклад, для довільного складеного n число $a = 1$ завжди буде брехунцем Ферма, оскільки $1^{n-1} \equiv 1 (\mathrm{mod}\ n)$.

АЛГОРИТМ

Вхід: непарне ціле число $n \ge 3$, параметр $t \ge 1$.

Вихід: визначення, чи є число n простим.

1. for $i \leftarrow 1$ to t do
   1.1. Обрати довільне ціле a, $2 \le a \le n-2$.
   1.2. Обчислити $k \leftarrow a^{n-1} \mathrm{mod}\ n$.
   1.3. if $k \neq 1$ then return(«складене»).
2. return(«просте»).

Якщо алгоритм дає відповідь «складене», то дійсно число є складеним. Якщо відповідь буде «просте», то або n є дійсно простим, або n є складеним, але має велику кількість брехунців. Чим більше значення параметра t, тим більше тестів буде зроблено і тим більша ймовірність того, що n є простим.

Приклад. Розглянемо складене число $n = 15$ та знайдемо його свідки та брехунці Ферма. Для цього складемо таку таблицю:

a	1	2	3	4	5	6	7
$a^{14} \mathrm{mod}\ 15$	1	4	9	1	10	6	4

a	8	9	10	11	12	13	14
$a^{14} \mathrm{mod}\ 15$	4	6	10	1	9	4	1

Свідками Ферма є числа 2, 3, 5, 6, 7, 8, 9, 10, 12, 13. Брехунцями Ферма є числа 1, 4, 11, 14.

Тест Ферма зручно використовувати для перевірки числа n на складеність, оскільки для більшості натуральних чисел кількість свідків більша за кількість брехунців. Але існують складені числа, які є псевдопростими за довільною основою (взаємно простою з заданим числом). Такі числа називаються числами Кармайкла, і найменше з них дорівнює $561 = 3 * 11 * 17$.

Означення. Число n називається числом *Кармайкла*, якщо воно складене та для довільного a, $1 \le a \le n-1$, НСД $(a, n) = 1$, має місце рівність

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

Критерій Корсельта. Для того, щоб складене число n було числом Кармайкла, необхідно і достатньо виконання двох умов:

- n не ділиться на квадрат простого числа;
- $n-1$ ділиться на $p-1$ для всякого простого дільника p числа n.

Приклад. Простими дільниками числа 561 є 3, 11, 17. При цьому жоден з них не входить до розкладу навіть двічі, а число 560 ділиться на 2, 10 та 16:

$560 : 2 = 280,\ 560 : 10 = 56,\ 560 : 16 = 35.$

Твердження. Кожне число Кармайкла є добутком хоча б трьох простих чисел.

Приклад. Числа Кармайкла в межах до 100 000:

561, 1105, 1729, 2465, 2821, 6601, 8911,
10 585, 15 841, 29 341, 41 041, 46 657,
52 633, 62 745, 63 973, 75 361.

Теорема (Чернік, 1939). Якщо $p = 6m + 1$, $q = 12m + 1$, $r = 18m + 1$ є простими числами, то число pqr є числом Кармайкла.

Приклад. Якщо покласти $m = 1$, то отримаємо $p = 7$, $q = 13$, $r = 19$ – всі прості числа. Отже, $n = 7 * 13 * 19 = 1729$ – число Кармайкла.

Кількість чисел Кармайкла у натуральному ряді до 10^{12} дорівнює 8241, до 10^{13} – 19279, до 10^{14} – 44706, до 10^{15} – 105212.

Тест Соловай–Штрасена

Тест Соловай–Штрасена базується на критерії 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.

Нехай n – непарне складене число, a – ціле число, $1 \le a \le n-1$.

1. Якщо НСД(a, n) > 1 або $a^{\frac{n-1}{2}} \neq \left(\frac{a}{n}\right) (\mathrm{mod}\, n)$,

то число a називається *свідком Ейлера* (свідком складеності) для n.

2. Якщо НСД(a, n) = 1 та $a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right) (\mathrm{mod}\, n)$,

то число n називається *псевдопростим* за основою a. Число a називається *брехунцем Ейлера* (брехунцем простоти) для n. Кількість брехунців Ейлера для числа n будемо позначати через el(n) (Euler liars).

АЛГОРИТМ
Вхід: непарне ціле число $n \ge 3$, параметр $t \ge 1$.
Вихід: визначення, чи є число n простим.
1. for $i \leftarrow 1$ to t do
  1.1. Обрати довільне ціле a, $2 \le a \le n-2$.
  1.2. Обчислити $k \leftarrow a^{(n-1)/2} \bmod n$.
  1.3. if $k \neq 1$ and $k \neq n-1$ then return(«складене»).
  1.4. Обчислити символ Якобі $j \leftarrow \left(\frac{a}{n}\right)$.
  1.5. if $k \neq j \pmod n$ then return(«складене»).
2. return(«просте»).

Тест Мілера–Рабіна

Тестом Мілера–Рабіна називається ймовірнісний тест перевірки на простоту, який було запропоновано Мілером з використанням ідей Рабіна.

Тест Мілера–Рабіна найбільш часто використовується на практиці і називається сильним тестом на простоту. Він базується на такому факті:

Нехай n – непарне просте число, причому $n-1 = 2^s * r$, де r – непарне. Нехай a – таке натуральне число, що 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, $0 \le j \le s-1$.

Означення. Нехай n – непарне складене число, $n-1 = 2^s * r$, де r – непарне, a – натуральне число, $1 \le a \le n-1$.

1. Якщо $a^r \neq 1 (\mathrm{mod}\, n)$ та $a^{2^j r} \neq -1 (\mathrm{mod}\, n)$ для всіх j, $0 \le j \le s-1$, то a називається *сильним свідком* (свідком складеності) для n.

2. Якщо $a^r \equiv 1 (\mathrm{mod}\, n)$ або $a^{2^j r} \equiv -1 (\mathrm{mod}\, n)$ для деякого j, $0 \le j \le s-1$, то a називається *сильним брехунцем* для n, а само число n – *сильним псевдопростим* за основою a. Кількість сильних брехунців числа n будемо позначати через sl(n) (strong liars).

АЛГОРИТМ
Вхід: непарне ціле число $n \ge 3$, параметр $t \ge 1$.
Вихід: визначення, чи є число n простим.
1. Записати $n - 1 = 2^s * r$, де r – непарне.
2. for $i = 1$ to t do
  2.1. Обрати довільне ціле a, $2 \le a \le n-2$.
  2.2. Обчислити $y \leftarrow a^r \pmod n$.
  2.3. if $y \neq 1$ and $y \neq n-1$ then
    $j \leftarrow 1$
    while $j \le s-1$ and $y \neq n-1$ do
    $y \leftarrow y^2 \bmod n$
    if $y = 1$ then return(«складене»).
    $j \leftarrow j + 1$
    if $y \neq n-1$ then return(«складене»).
3. return(«просте»).

Приклад. $n = 221 = 13 * 17$ – складене число. $n - 1 = 220 = 2^2 * 55$, $s = 2$, $r = 55$.

Нехай $a = 5$, НСД(5, 221) = 1.

$$a^r (\mathrm{mod}\, n) \equiv 5^{55} (\mathrm{mod}\, 221) \equiv 112 \neq 1.$$

Вираз $a^{2^j r}$ будемо обчислювати для $j = 0, 1$ ($0 \le j \le 1$) поки не отримаємо -1.

$j = 0$: $a^r (\mathrm{mod}\, n) \equiv 5^{55} (\mathrm{mod}\, 221) \equiv 112 \neq -1$.
$j = 1$: $a^{2r} (\mathrm{mod}\, n) \equiv 5^{55})^2 (\mathrm{mod}\, 221) \equiv 168 \neq -1$,

що підтверджує складеність 221.

Нехай $a = 21$, НСД(21,221) = 1.

$a^r(\text{mod } n) \equiv 21^{55}(\text{mod } 221) \equiv 200 \neq 1.$

$j = 0$: $a^r(\text{mod } n) \equiv 21^{55}(\text{mod } 221) \equiv 200 \neq -1.$

$j = 1$: $a^{2r}(\text{mod } n) \equiv 21^{55})^2(\text{mod } 221) \equiv -1,$

отже, 221 може бути простим.

Приклад показує, що число 5 є сильним свідком для 221, а 21 є сильним брехунцем для 221.

Якщо перебрати в якості a всі значення від 1 до 220, то можна побачити, що число 221 має 6 таких сильних брехунців: 1, 21, 47, 174, 200, 220, а sl(221) = 6.

Властивості брехунців

Основним показником якості перелічених тестів на простоту є кількість ітерацій, після виконання яких на складеному вхідному числі тест дасть відповідь «складене». Кожен із тестів має брехунців. Чим менша кількість брехунців існує для заданого складеного числа n, тим менша кількість ітерацій необхідна для визначення його складеності.

Приклад. Нехай $n = 221$.

Брехунці Ферма: 1, 18, 21, 38, 47, 64, 86, 103, 118, 135, 157, 174, 183, 200, 203, 220. Кількість брехунців: fl(221) = 16.

Брехунці Ейлера: 1, 18, 21, 38, 47, 64, 86, 103, 118, 135, 157, 174, 183, 200, 203, 220. Кількість брехунців: el(221) = 16.

Сильні брехунці: 1, 21, 47, 174, 200, 220. Кількість брехунців: sl(221) = 6.

Таким чином, при використанні тесту Ферма ймовірність визначення складеності числа 221 з першої ітерації дорівнює 205/221, Соловай–Штрасена – 205/221, Мілера–Рабіна – 215/221.

Нехай n – непарне складене число. Тоді:

1. Якщо a – сильний брехунець для числа n, то a буде брехунцем Ейлера для числа n.

2. Якщо a – брехунець Ейлера для числа n, то a буде брехунцем Ферма для числа n.

Якщо для заданого числа n побудувати множини брехунців для кожного із трьох наведених

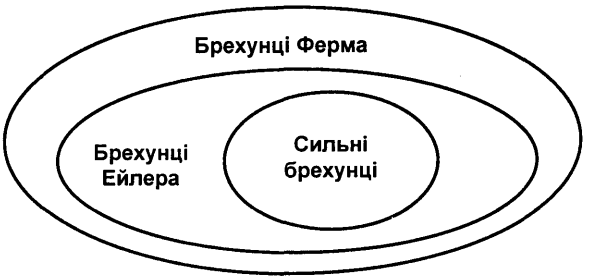

Рис. 1. Множини брехунців одного числа для різних тестів

ймовірнісних тестів, то вони розташуються так, як показано на рис. 1.

Твердження. Якщо $n \equiv 3$ (mod 4), то число a є брехунцем Ейлера тоді і тільки тоді, коли воно є сильним брехунцем.

Твердження. Нехай n – непарне складене число. Тоді якщо $n \neq 9$, то кількість його сильних брехунців не більша за $\varphi(n)/4$.

Твердження. Нехай $n = p * q$ – добуток двох простих чисел, d = НСД($p - 1$, $q - 1$). Тоді кількість брехунців числа n дорівнює

$$\text{sl}(n) = r^2 * (2 + (4^t - 4)/3),$$

де $d = 2^t * r$, r – непарне.

Приклад. Обчислимо кількість сильних брехунців складеного числа $n = 221 = 13 * 17$. Маємо: d = НСД(12, 16) = $4 = 2^2 * 1$, $r = 1$, $t = 2$. Отже,

$$\text{sl}(221) = 1^2 * (2 + (4^2 - 4)/3) = 2 + 4 = 6.$$

Твердження. Нехай $n = p * q$ – добуток двох простих чисел, $p = 2 * r + 1$, $q = 4 * r + 1$, r – непарне. Тоді кількість брехунців досягає своєї верхньої межі:

$$\text{sl}(n) = \varphi(n)/4.$$

Приклад. При $r = 1$ маємо: $p = 3$, $q = 5$, $n = p * q = 15$.

$$\text{sl}(15) = \varphi(15)/4 = (3 - 1) * (5 - 1) / 4 = 2 * 4/4 = 2.$$

Число 15 дійсно має два сильні брехунці.

1. *Rabin M. O.* Probabilistic Algorithm for Primality Testing // Journal of Number Theory- 1980- V. 12- P. 128-138.
2. *Miller G. L.* Ricmann's Hypothesis and Tests for Primality // Journal of Computer Systems Science- 1976-V. 13.-№3.-?. 300-317.
3. *MenezesA., van Oorschot P., VanstoneS.* Handbook of Applied Cryptography.

M. G. Medvedev

PROBABILISTIC PRIMALITY TESTS

The problem of primalily proving is one of the most important in number theory and cryptography. In this article three probabilistic primality tests are given. For each presented test the term "liar" is defined and the power ofprobabilistic tests is presented according to amount ofliarsfor testing number in each test.