Тести на простоту

Проблема належності заданого натурального числа до класу простих чи складених чисел є дуже цікавою не тільки в математиці, а й в 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 твердженні, що операція множення двох великих простих чисел є односторонньою функцією.

Для перевірки числа на простоту користуються ймовірносними (Ферма, Соловай – Штрасена, Мілера – Рабіна, Лемана) та правдивими тестами.

Ймовірностні тести

Означення. Тест на простоту називається ***ймовірносним***, 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 наступну інформацію про непарне ціле число n:

- Якщо тест визначає, що n є складним, то це дійсно так.
- Якщо тест визначає, що n є простим, то з 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 $a^{n-1} \equiv 1 \pmod n$. Якщо для заданого n знайдеться хоча б одне таке a, що $a^{n-1} \neq 1 \pmod n$, 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.

Очевидно, що для довільного складеного n число $a = 1$ завжди буде брехунцем Ферма, оскільки $1^{n-1} \equiv 1 \pmod n$.

Алгоритм

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

Вихід: визначення, чи є чило 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 ← a^{n-1} mod n.

1.3. if k ≠ 1 then return (“складне”).

2. return (“просте”).

Якщо алгоритм дасть відповідь “складне”, то дійсно число є складним. Якщо відповідь буде “просте”, то або n є дійсно простим, або n є складним та 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 наступну таблицю:

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

a	8	9	10	11	12	13	14
a^{14} 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 межі до 100000:

561, 1105, 1729, 2465, 2821, 6601, 8911, 10585, 15841, 29341, 41041, 46657, 52633, 62745, 63973, 75361.

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.

Річард Пінч, провівши велику кількість обчислень, виявив, що кількість чисел Кармайкла у натуральному ряді до 10^{12} дорівнює 8241, до 10^{13} – 19279, до 10^{14} – 44706, до 10^{15} – 105212. З іншого боку декількома авторами наводилася верхня межа для C(n) – кількість чисел Кармайкла від 1 до n. Одна з них (і яка на сьогодні вважається найбільш точною):

$$C(n) \le n^{1 - \{1 + o(1)\} \log\log\log n / \log\log n}$$

Теорема (Чіполла, 1904). Існує нескінченно багато складених псевдопростих чисел за основою b.

Доведення. Нехай $y_p = \dfrac{b^{2p} - 1}{b^2 - 1}$, де p – непарне просте число, НСД(p, $b^2 - 1$) = 1. Тоді $y_p = \dfrac{b^p - 1}{b - 1} \cdot \dfrac{b^p + 1}{b + 1}$ – складене непарне ціле число. Враховуючи що $b^{2p} - 1$ ділиться на $\dfrac{b^{2p} - 1}{b^2 - 1}$, то $b^{2p} \equiv 1 \pmod{y_p}$.

$$y_p - 1 = \frac{b^{2p} - 1}{b^2 - 1} - 1 = \frac{b^{2p} - 1 - b^2 + 1}{b^2 - 1} = b^2 \cdot \frac{b^{2p-2} - 1}{b^2 - 1} = b^2 \cdot (b^{p-1} + 1) \cdot \frac{b^{p-1} - 1}{b^2 - 1}.$$

Оскільки $y_p - 1$ - парне, а також за теоремою Ферма $b^{p-1} \equiv 1 \pmod{p}$ (вираз b^{p-1} - 1 ділиться на p), то $y_p - 1 \equiv 0 \pmod{2p}$.

Отже $b^{y_p - 1} = (b^{2p})^{\frac{y_p - 1}{2p}} \equiv 1 \pmod{y_p}$.

Всі числа y_p є псевдопростими за основою b.

Приклад. Нехай $b = 2$, $p = 5$. Тоді $y_5 = \dfrac{2^{10} - 1}{2^2 - 1} = 341 = 11 * 31$.

Оскільки $2^{340} \equiv 1 \pmod{341}$, то складене число 341 є псевдопростим за основою 2.

<u>Тест Соловай - Штрасена</u>

Тест Соловай – Штрасена базується на критерії Ейлера: якщо n – просте, то

$$a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right) \pmod{n}$$

для всіх значень a, для яких НСД(a, n) = 1.

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

1. Якщо НСД (a, n) > 1 або $a^{\frac{n-1}{2}} \neq \left(\frac{a}{n}\right) \pmod n$, то число a називається ***свідком Ейлера*** (свідком складеності) для n.

2. Якщо НСД (a, n) = 1 та $a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right) \pmod n$, то число n називається ***псевдопростим*** за основою a. Число a називається ***брехунцем Ейлера*** (брехунцем простоти) для n.

Алгоритм

Вхід: непарне ціле число $n \ge 3$, параметр $t \ge 1$.
Вихід: визначення, чи є чило 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

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

Твердження. Нехай n – непарне просте число, при чому $n - 1 = 2^s * r$, де r – непарне. Нехай a – таке натуральне число, що НСД(a, n) = 1. Тоді має місце одна із рівностей:

$$a^r \equiv 1 \pmod n$$

або

$$a^{2^j r} \equiv -1 \pmod n \text{ для деякого } j,\ 0 \le j \le s - 1$$

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

2. Якщо $a^r \equiv 1 \pmod n$ або $a^{2^j r} \equiv -1 \pmod n$ для деякого j, $0 \le j \le s - 1$, тоді 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 $n \geq 3$, параметр $t \geq 1$.
Вихід: визначення, чи є чило 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, $2 \leq a \leq n - 2$.
   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 $j \leq s - 1$ 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”).

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

Приклад. $n = 29$ – просте число. $n - 1 = 28 = 2^2 * 7$. s = 2, r = 7.
Нехай $a = 10$, НСД(10, 29) = 1.
$a^r \pmod n \equiv 10^7 \pmod{29} \equiv 17 \neq 1$.
Вираз $a^{2^j r}$ будемо обчислювати для j = 0, 1 ($0 \leq j \leq 1$) поки не отримаємо -1.
j = 0: $a^r \pmod n \equiv 10^7 \pmod{29} \equiv 17 \neq -1$.
j = 1: $a^{2r} \pmod n \equiv (10^7)^2 \pmod{29} \equiv -1$, 29 може бути простим.

Нехай $a = 19$, НСД(19, 29) = 1.
$a^r \pmod n \equiv 19^7 \pmod{29} \equiv 12 \neq 1$.
j = 0: $a^r \pmod n \equiv 19^7 \pmod{29} \equiv 12 \neq -1$.
j = 1: $a^{2r} \pmod n \equiv (19^7)^2 \pmod{29} \equiv -1$, 29 може бути простим.

Приклад. $n = 221 = 13 * 17$ – складне число. $n - 1 = 220 = 2^2 * 55$. $s = 2$, $r = 55$.
Нехай $a = 5$, НСД(5, 221) = 1.
$a^r \pmod n \equiv 5^{55} \pmod{221} \equiv 112 \neq 1$.
Вираз $a^{2^j r}$ будемо обчислювати для $j = 0, 1$ ($0 \leq j \leq 1$) поки не отримаємо -1.
j = 0: $a^r \pmod n \equiv 5^{55} \pmod{221} \equiv 112 \neq -1$.
j = 1: $a^{2r} \pmod n \equiv (5^{55})^2 \pmod{221} \equiv 168 \neq -1$, що підтверджує складеність 221.
Число 5 є сильним свідком для 221.

Нехай $a = 21$, НСД(21, 221) = 1.

$a^r \pmod n \equiv 21^{55} \pmod{221} \equiv 200 \neq 1$.

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

j = 1: $a^{2r} \pmod n \equiv (21^{55})^2 \pmod{221} \equiv -1$, 221 може бути простим.

Число 21 є сильним брехунцем для 221, а 221 є сильним псевдопростим за основою 21.

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

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

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

де $d = 2^t * r$, r – непарне.

Приклад. n = 221 = 13 * 17. d = НСД(12, 16) = 4 = $2^2 * 1$, r = 1, t = 2.
$sl(221) = 1^2 * (2 + (4^2 - 4) / 3) = 2 + 4 = 6$.

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:

$$sl(n) = \varphi(n) / 4$$

Приклад. При r = 1 маємо: p = 3, q = 5, n = p * q = 15.
$sl(15) = \varphi(n) / 4 = (3 - 1) * (5 - 1) / 4 = 2 * 4 / 4 = 2$.
Число 15 дійсно має двох сильних брехунців.

Тест Лемана [Шнаер. Прикладна Криптография. Стр.297]

Тест був розроблений Леманом (Lehmann). Послідовність дій при перевірці простоти числа *p*:

(1) Обрати випадково число *a*, що менше за *p*.

(2) Обчислити $a^{(p-1)/2} \bmod p$.

(3) Якщо $a^{(p-1)/2} \neq 1$ або -1 (mod p), то *p* не є простим.

(4) Якщо $a^{(p-1)/2} \equiv 1$ або -1 (mod p), то ймовірність того, что число *p* не є простим, не більше 50 відсотків.

Якщо після виконання послідовності дій (1)-(4) *t* разів результат обчислень дорівнює 1 або -1, але не завжди дорівнює 1, то *p* є простим числом з ймовірністю похибки $1/^{2t}$

Істині тести

Означення. Тест на простоту називається ***істиним***, якщо в результаті його застосування можна однозначно встановити, чи є задане число простим чи ні.

Решето Ератосфена

Найпростіший метод встановлення як простоти так і складеності числа був відомий ще у давнину і називається він решетом Ератосфена:

Виписати в ряд числа від 2 до n. Перше число в ряду є простим. Викреслити з ряду числа, які є кратними 2. Далі взяти друге число, що стоїть в ряду і викреслити всі числа, кратні йому. І так далі брати і-те число та викреслювати кратні йому числа поки і < $\sqrt{n}$. Числа, що залишаться в ряду після операцій викреслення, є простими.

Цей метод є ефективним коли число n невелике (n < 10.000.000.000). При цьому його можна використовувати не тільки для тестування на простоту, а й для пошуку простих чисел у вказаному інтервалі та для розв’язку задачі факторизації.