

Тема 5. ПРОСТІ ЧИСЛА. ТЕСТУВАННЯ ЧИСЛА НА ПРОСТОТУ

1. Означення простого числа

Криптографія використовує дуже великі прості числа. На жаль, використання стандартних засобів мов програмування надає можливість працювати лише з такими цілими числами, значення яких не виходять за межі довгого цілого типу `LongInt`, для якого найбільше допустиме значення становить 2147483647. При цьому найбільше ціле число рівне 2147302891 (*просте*), що далеко не задовольняє потреби криптографії. Саме тому дуже важливо розробляти швидкодіючі алгоритми обробки простих чисел.

Означення. Натуральне число $p > 1$ називається *простим*, якщо воно не має інших натуральних дільників, крім 1 і p . Простим числом буде найменший, відмінний від 1 дільник цілого a , $a > 1$.

Теорія чисел визначає прості числа наступним чином:

- ✓ всі натуральні числа, крім 1, мають, щонайменше, двох дільників – одиницю та самого себе;
- ✓ ті з них, що не мають ніяких інших дільників, називаються простими; наприклад, декілька перших простих чисел 2, 3, 5, 7, 11, 13, 17, 19;
- ✓ ті числа, які мають ще й інших дільників, називаються складеними; наприклад, 12 – складене число (його дільники 1, 2, 3, 4, 6, 12);
- ✓ число 1 розглядають окремо, не відносячи ні до простих, ні до складених, оскільки одиниця не має всіх властивостей, справедливих для всіх інших простих чисел.

Означення. Натуральні числа a і b , для яких $НСД(a,b)=1$, називаються *взаємно простими*.

Закономірності в розподілі простих чисел на даний час ще не знайдено.

Теорема. Існує нескінченно багато простих чисел.

Теорема. Будь-яке ціле число більше від одиниці розкладається на добуток простих множників. Цей розклад єдиний з точністю до порядку слідування множників. [8]

2. Утворення послідовності простих чисел

Будемо розглядати утворення простих чисел в межах від 2 до деякого заданого X .

Спосіб 1. Пов'язаний з послідовним перебором натуральних чисел від 2 до X . Для кожного з них реалізується тестування на простоту, і у разі позитивного результату чергове число переводиться у послідовність простих. У зв'язку з необхідністю тестування такий спосіб вважається не ефективним за витратами часу.

Спосіб 2. Спосіб відомий під назвою *решето Ератосфена*. Відповідний класичний алгоритм такий:

- 1) виписуємо всі натуральні числа від 2 до X ;
- 2) обводимо перше число 2, а всі інші, кратні 2, викреслюємо;
- 3) відшукуємо найменше необведене і не викреслене, обводимо його, фіксуємо його значення L , а після цього викреслюємо кожне L -те число, тобто всі, кратні йому;
- 4) п.3 повторюємо, поки не залишиться необведених і незакреслених чисел.

Всі обведені числа є простими. Спосіб не вимагає виконання арифметичних операцій, що і визначає його швидкодію. У зв'язку з необхідністю попереднього виписування всіх натуральних чисел, такий спосіб вважається теж не ефективним за витратами пам'яті.

Вдвічі зменшити витрати пам'яті дозволяє *модифіковане решето Ератосфена*. Воно відрізняється від класичного лише тим, що виписується 2 і всі непарні натуральні числа, які не перевищують X . При цьому перше просте число 2 обводиться відразу.

Кількість отриманих простих чисел від 2 до X є значенням, так званої, функції $\pi(x)$, рівне кількості всіх простих чисел, що не перевищують X . [8]

3. Тестування числа на простоту, ймовірнісні тести

Тестуванням деякого числа a на простоту називається перевірка, є дане число a простим чи ні.

Для цього достатньо перевірити всі можливі прості дільники цього числа, за винятком самого числа a . Така можливість пов'язана з тим фактом у теорії чисел, що будь-яке натуральне число a можна єдиним способом представити у вигляді добутку степенів простих чисел, тобто $a = p_1^{k_1} * p_2^{k_2} * \dots * p_s^{k_s}$ – канонічний розклад числа на прості множники, де $k_i \geq 1$ – кількість простих чисел, рівних p , присутніх у поданні числа a .

Якщо остача від ділення числа a на деякий можливий простий його дільник рівна нулю, то таке число a не є простим.

Всі можливі прості дільники числа a , які слід перевірити знаходяться в межах від 2 до $[\sqrt{a}]$ (ціла частина кореня з a). Для великого числа a така перевірка може тривати занадто довго. Тому важливе значення мають різні методи скорочення терміну перевірки.

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.

Для перевірки чисел на простоту користуються ймовірнісними тестами: Ферма, Соловай-Штрассена, 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. [6]

4. Ймовірнісний тест на простоту Ферма

Тест базується на теоремі Ферма, яка стверджує, що якщо n – просте, то для довільного a , $1 \leq a \leq n - 1$, має місце рівність $a^{n-1} \equiv 1 \pmod{n}$. Якщо для заданого n знайдеться хоча б одне таке a , що $a^{n-1} \not\equiv 1 \pmod{n}$, то n не є простим.

Означення. Нехай n – непарне складене число. Число a , $1 < a < n - 1$, таке що $a^{n-1} \not\equiv 1 \pmod{n}$, називається *свідком Ферма* (свідком складеності) для n .

Означення. Нехай n – непарне складене число, a – ціле число, $1 < a < n - 1$.
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 $fl(n)$ (Ferma liars).

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

АЛГОРИТМ

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

Вихід: визначення, чи є число n простим.

1. *for* $i \leftarrow 1$ *to* t *do*
 - 1.1. Обрати довільне ціле a , $2 \leq a \leq n - 2$.
 - 1.2. Обчислити $k \leftarrow a^{n-1} \pmod{n}$.
 - 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
$a^{14} \pmod{15}$	1	4	9	1	10	6	4

A	8	9	10	11	12	13	14
$a^{14} \pmod{15}$	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.

Означення. Число n називається числом *Кармайкла*, якщо воно складене та для довільного a , $1 \leq a \leq n-1$, НСД $(a, n) = 1$, має місце рівність $a^{n-1} \equiv 1 \pmod{n}$. Найменше з них дорівнює $561 = 3 \cdot 11 \cdot 17$.

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 1.

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 2.

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 3.

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. [6]

5. Ймовірнісний тест Соловай-Штрассена

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

$$a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right) \pmod{n} \text{ для всіх значень } a, \text{ для яких НСД}(a, n) = 1.$$

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

1. Якщо $\text{НСД}(a, n) > 1$ або $a^{\frac{n-1}{2}} \not\equiv \left(\frac{a}{n}\right) \pmod{n}$, то число a називається *свідком Ейлера* (свідком складеності) для n .

2. Якщо $\text{НСД}(a, n) = 1$ 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 . Кількість брехунців Ейлера для числа n будемо позначати через $el(n)$ (Euler liars).

АЛГОРИТМ

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

Вихід: визначення, чи є число n простим.

1. *for* $i \leftarrow 1$ to t *do*
 - 1.1. Обрати довільне ціле a , $2 \leq a \leq n-2$.
 - 1.2. Обчислити $k \leftarrow a^{(n-1)/2} \pmod{n}$.
 - 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»). [6]

6. Ймовірнісний 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 $n - 1 = 2^s \cdot r$, де r – непарне.
 Нехай a – таке натуральне число, що $\text{НСД}(a, n) = 1$. Тоді має місце одна із рівностей: $a^r \equiv 1 \pmod{n}$ або $a^{2^j r} \equiv -1 \pmod{n}$ для деякого j , $0 \leq j \leq s - 1$.

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

1. Якщо $a^r \not\equiv 1 \pmod{n}$ та $a^{2^j r} \not\equiv -1 \pmod{n}$ для всіх j , $0 \leq j \leq s - 1$, то 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 , $0 \leq j \leq s - 1$, 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 $n \geq 3$, параметр $t \geq 1$.

Вихід: визначення, чи є число n простим.

1. Записати $n - 1 = 2^s \cdot r$, 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*
 - $y \leftarrow y^2 \pmod{n}$
 - if* $y = 1$ *then return*(«складене»).
 - $j \leftarrow j + 1$
 - if* $y \neq n - 1$ *then return*(«складене»).
3. *return*(«просте»).

Приклад 4.

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

Нехай $a = 5$, $\text{НСД}(5, 221) = 1$. $a^r \pmod{n} \equiv 5^{55} \pmod{221} \equiv 112 \not\equiv -1$.

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

$$j=0: a^r \pmod n \equiv 5^{55} \pmod{221} \equiv 112 \neq -1.$$

$j=0: a^{2^0 r} \pmod n \equiv (5^{55})^2 \pmod{221} \equiv 168 \neq -1$, що підтверджує складеність 221.

$$\text{Нехай } a = 21, \text{ НСД}(21, 221) = 1. a^r \pmod n \equiv 21^{55} \pmod{221} \equiv 200 \neq 1.$$

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

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

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 $sl(221) = 6$. [6]

7. 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 5.

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-Штрассена – $205/221$, 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 ймовірнісних тестів, то вони розташуються так, як показано на рис.



Рис. 5.1 Множини брехунців одного числа для різних тестів

Твердження. Якщо $n \equiv 3 \pmod{4}$, то число $a \in$ 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 $n = p \cdot q$ – добуток двох простих чисел, $d = \text{НСД}(p-1, q-1)$. Тоді кількість брехунців числа n дорівнює $sl(n) = r^2 \cdot (2 + (d-4)/3)$, де $d = 2^r \cdot r$, r – непарне.

Приклад 6.

Обчислимо кількість сильних брехунців складеного числа $n = 221 = 13 \cdot 17$. Маємо: $d = \text{НСД}(12, 16) = 4 = 2^2 \cdot 1$, $r = 1$, $t = 2$. Отже, $sl(221) = 1^2 \cdot (2 + (4^2 - 4)/3) = 2 + 4 = 6$.

Твердження. Нехай $n = p \cdot q$ – добуток двох простих чисел, $p = 2 \cdot r + 1$, $q = 4 \cdot r + 1$, r – непарне. Тоді кількість брехунців досягає своєї верхньої межі: $sl(n) = \varphi(n)/4$.

Приклад 7.

При $r = 1$ маємо: $p = 3$, $q = 5$, $n = p \cdot q = 15$. $sl(15) = \varphi(15)/4 = (3-1) \cdot (5-1)/4 = 2 \cdot 4/4 = 2$. Число 15 дійсно має два сильні брехунці. [6]