МАТЕМАТИЧНА КРИПТОГРАФІЯ

Алгоритм Евкліда

Теорема (алгоритм подільності) Для $\forall a \in \mathbf{Z}, \forall b \in \mathbf{N}$ однозначно визначені числа $q, r \in \mathbf{N}$ такі, що $a = qb + r$ де q – частка, r – остача, $r \in [0; b)$.

Будемо говорити, що a ***ділиться*** *на* b (націло) або b *ділить* a (позначається $b \mid a$), якщо $r = 0$. $a \bmod b = r$

Найбільший спільний дільник – $НСД(a,b)$.

Числа a та b ***взаємно прості***, якщо $НСД(a,b) = 1$.

Алгоритм Евкліда ґрунтується на співвідношеннях

$НСД(a,b) = НСД(b, a \bmod b)$

$НСД(a,0) = a$

Алгоритм знаходження $НСД(a,b)$, $a \in \mathbf{Z}, b \in \mathbf{N}, b < a$:

1. $r_0 = a$, $r_1 = b$, $i = 1$.
2. Ділимо r_{i-1} на r_i і отримуємо $r_{i-1} = q_i r_i + r_{i+1}$.
3. Якщо $r_{i+1} > 0$, то прийняти $i = i + 1$ і перейти на крок 2.

   Інакше $НСД(a,b) = r_i$.

Твердження. Для кожної пари взаємно простих a та b можна знайти такі числа u та v, що $au + bv = 1$.

Доведення. За умови, що $НСД(a,b) = 1$ на передостанньому кроці алгоритму Евкліда

$r_{m-2} = q_{m-1}r_{m-1} + 1$ звідки $1\ r_{m-2} + (-q_{m-1})r_{m-1} = 1.$

Нехай ця рівність виконується для i-ого кроку:

$u_{i-1}r_{i-1} + v_{i-1}r_{i-1} = 1$

$u_i q_i r_i + u_i r_{i+1} + v_{i-1}r_i = (u_i q_i + v_{i-1})r_i + u_i r_{i+1}$

Враховуючи, що $r_0 = a$, $r_1 = b$ отримуємо твердження.■

Розширений алгоритм Евкліда:

1. Покласти $r_0 = a$, $r_1 = b$, $u_0 = v_1 = 1$, $u_1 = v_0 = 1$, $i = 1$.
2. $r_{i-1} = q_i r_i + r_{i+1}$
3. Обчислити $u_{i+1} = u_i - q_i u_i$, $v_{i+1} = v_{i-1} - q_i v_i$
4. Якщо $r_{i+1} > 0$, то прийняти $i = i + 1$ і перейти на крок 2. Інакше $НСД(a,b) = r_i$

Твердження. $r_i = u_i a + v_i b$, $i = \overline{0,m}$, де m – кількість ітерацій.

Доведення. При $i = 0$ $r_0 > a$, при $i = 0$ $r_1 > b$. Допустимо, що виконується на i-ому кроці. Тоді

$$r_{i+1} = r_{i-1} - q_i r_i = u_{i-1} a + v_{i-1} b - q_i u_i a - q_i v_i b =$$
$$= (u_{i-1} + q_i u_i) a + (v_{i-1} - q_i v_i) b = u_{i+1} a + v_{i+1} b$$

Отже твердження виконується для всіх i. ■

Використовується для знаходження мультиплікативної інверсії за модулем

$$c \times c^{-1} \bmod n = 1$$

Конгруенції

Цілі x та y називають ***конгруентними*** або *рівними за модулем* n, якщо $x \bmod n = y \bmod n$ і позначаються $x \equiv y \pmod{n}$.

Твердження. Наступні умови еквівалентні:

$$x \equiv y \pmod{n} \quad : \quad x = y + kn, k \in \mathbf{Z} \quad : \quad n \mid (x - y) \blacksquare$$

Твердження. Конгруенції мають властивості:

1) відношення еквівалентності:

一) $x \equiv x \pmod{n}$ (рефлективність)

二) $x \equiv y \pmod{n} \Rightarrow y \equiv x \pmod{n}$ (симетричність)

三) $\left.\begin{array}{l} x \equiv y \pmod{n} \\ x \equiv z \pmod{n} \end{array}\right| \Rightarrow y \equiv z \pmod{n}$ (транзитивність)

2) конгруенції можна почленно додавати і перемножувати

$$\left.\begin{array}{l} x_1 \equiv x_2 \pmod{n} \\ y_1 \equiv y_2 \pmod{n} \end{array}\right| \Rightarrow \begin{array}{l} x_1 + y_1 \equiv x_2 + y_2 \pmod{n} \\ x_1 y_1 \quad x_2 y_2 \pmod{n} \end{array}$$

3) обидві частини конгруенції можна скорочувати на їх спільний дільник, якщо він взаємно простий з модулем

$$\left.\begin{array}{l} d \mid x,\ d \mid y \\ НСД(d,n) = 1 \\ x \equiv y \pmod{n} \end{array}\right| \Rightarrow \frac{x}{d} \equiv \frac{y}{d} \pmod{n}$$

4) обидві частини конгруенції і їх модуль можна скорочувати на їхній спільний дільник

$$\left.\begin{array}{l} d \mid x, d \mid y, d \mid n \\ x \equiv y \pmod{n} \end{array}\right| \Rightarrow \frac{x}{d} \equiv \frac{y}{d} \pmod{\frac{n}{d}}$$

5)

$$\left.\begin{array}{l} m \mid n \\ x \equiv y \pmod{n} \end{array}\right| \Rightarrow x \equiv y \pmod{m}$$

6) для простих чисел p та q:

$$x \equiv y \pmod{pq} \Leftrightarrow \begin{array}{l} x \equiv y \pmod{p} \\ x \equiv y \pmod{q} \end{array}$$

Кільце лишків

$\mathbf{Z}_n = \{0, \text{K}, n-1\}$ - множина, наділена операціями додавання та множення за модулем n. $x + y = (x + y) \bmod n$ та $x \times y = (x \times y) \bmod n$.

В такому означенні $\mathbf{Z}_n$ – комутативне кільце з одиницею і називається ***кільцем зведених лишків*** *за модулем* n. $\mathbf{Z}_n^*$ – мультиплікативна група елементів, для яких в $\mathbf{Z}_n$ є обернені відносно множення.

Твердження. $\mathbf{Z}_n$ складається з елементів x взаємно простих з n.

Доведення. (*Необхідність*) Якщо $НСД(x, n) = 1$, то для деяких цілих u та v виконується $ux + vn = 1$. Тоді $ux \equiv 1 \pmod n$, а отже $x^{-1} \equiv u \pmod n$. Шукати обернені можна розширеним алгоритмом Евкліда.

(*Достатність*) Нехай $xx^{-1} \equiv 1 \pmod n$, тоді $xx^{-1} + kn = 1$ і позначивши $u := x^{-1}$ та $v := k$ отримаємо, що x та n – взаємно прості. ■

Ділення на x в кільці $\mathbf{Z}_n$ – це множення на x^{-1}. Віднімання в $\mathbf{Z}_n$ – це додавання $(-x)$. Зауважимо, що $-1 = n-1$ в $\mathbf{Z}_n$.

Твердження. Для простого модуля p - $\mathbf{Z}_n$ є полем.

Означення. Функцією Ейлера $f(n)$ позначатимемо кількість натуральних чисел не більших за n і взаємно простих з n. Отже, функція Ейлера – це порядок групи $\mathbf{Z}_n^*$.■

Теорема Ейлера. Для взаємно простих x 挝$\mathbf{Z}, n$ $\mathbf{N}$ виконується $x^{f(n)} \circ 1 (\mathrm{mod}\, n)$

Доведення. Припустимо $1 £ x < n$ і розглянемо x як елемент мультиплікативної групи $\mathbf{Z}_n^*$. За теоремою Лагранжа порядок елемента x є дільником порядку групи, в нашому випадку $f(n)$. Тому $x^{f(n)} = 1$ в $\mathbf{Z}_n^*$, звідси і випливає теорема. ■

Випадок довільного x зводимо до попереднього, використавши конгруенцію $x^{f(n)} \circ (x \bmod n)^{f(n)} (\mathrm{mod}\, n)$.

Якщо p – просте, то $f(p) = p - 1$, а тому наслідком теореми Ейлера є мала теорема Ферма.

Мала теорема Ферма. Якщо x Ì $\mathbf{Z}$ не ділиться на просте p, то $x^{p-1} \circ 1 (\mathrm{mod}\, p)$.

Китайська теорема про остачі

Нехай $n_1, n_2 \in \mathbf{N}, x_1, x_2 \in \mathbf{Z}$. Якщо n_1 та n_2 – взаємно прості, то існує таке $x \in \mathbf{Z}$, для якого виконується $x \equiv x_1 \pmod{n_1}$ та $x \equiv x_2 \pmod{n_2}$.

Доведення. Оскільки $НСД(n_1, n_2) = 1$, то існують такі числа u та v, що $n_1 u + n_2 v = 1$. Тоді ми можемо вибрати $x := x_2 n_1 u + x_1 n_2 v$, що $x \pmod{n_1} = x_1 n_2 v \pmod{n_1} = x_1 \pmod{n_1} \times n_2 v \pmod{n_1} = x_1 \pmod{n_1}$.

Аналогічно $x \equiv x_2 \pmod{n_2}$.■

Твердження. Нехай $n = n_1 n_2$, $НСД(n_1, n_2) = 1$. Тоді відображення $f : \mathbf{Z}_n \to \mathbf{Z}_{n_1} \times \mathbf{Z}_{n_2}$, де $f(x) = (x \bmod n_1, x \bmod n_2)$ є ізоморфізмом кілець. (2)

Доведення. 1. Доведемо, що це гомоморфізм.

$f(x + y) = (x + y \bmod n_1, x + y \bmod n_2)$, $f_i(x) = x \bmod n_1$,

$((x + y) \bmod n) \bmod n_i = (x + y) \bmod n_i = x \bmod n_i + y \bmod n_i$.

Аналогічно і для операції множення.

2. Сур'єктивність випливає з китайської теореми про остачі.
3. Ін'єктивність випливає із тривіальності ядра, оскільки найменше натуральне число, яке ділиться націло на n_1 та n_2 є n.■

Теорема. Нехай $n = n_1 n_2$, $n_1, n_2 \in \mathbf{N}$ і n_1 та n_2 – взаємно прості. Тоді звуження відображення (2) $\mathbf{Z}_n^* \to \mathbf{Z}_{n_1}^* \times \mathbf{Z}_{n_2}^*$ є ізоморфізмом.

Доведення. Випливає як наслідок попереднього твердження та теореми про обернене відображення. ■

Теорема (Мультиплікативність функцій Ейлера). Для попарно взаємно простих $n_1, n_2, \ldots, n_l$, функція Ейлера рівна $\varphi(n_1 n_2 \ldots n_l) = \varphi(n_1) \cdot \varphi(n_2) \cdot \ldots \cdot \varphi(n_l)$.

Доведення. За індукцією з огляду на те, що при $l = 2$ рівність справджується завдяки попередньому твердженню. ■

Теорема (Формула для функцій Ейлера). Нехай $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ – розклад числа на прості співмножники. Тоді $f(n) = n\left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_k}\right)$

Доведення. Нехай $l = 1$. Тоді $n = p^a$ для деякого простого p. Числами, які не перевищують p^a не є взаємно прості з ним, є $p, 2p, 3p, \ldots, p^{a-1} \cdot p$ – всього p^{a-1} чисел. Отже $f(n) = p^a - p^{a-1} = n\left(1 - \frac{1}{p}\right)$. Далі за індукцією з використанням мультиплікативності функцій. ■

Для $n > 4$ можна оцінити функцію Ейлера знизу без знання розкладу n на прості співмножники:

$$f(n) > \frac{n}{6 \ln \ln n} \blacksquare$$

АРИФМЕТИЧНІ ЗАДАЧІ ТА АЛГОРИТМИ

Задачі

Задача обчислення функції: $f : A^* \to B^*$ полягає в знаходженні для вказаного слова $w \in A^*$ значення функції $f(w)$.

Масова задача

Задано: $w \in A^*$

Обчислити: $f(w)$.

Індивідуальна задача

Задано: $x \in \mathbf{N}$

Обчислити: x^2.

Нехай $L \subseteq A^*$ - множина слів у алфавіті A^*. L називають мовою. **Задача розпізнавання** мови L полягає у визначенні, належить задане слово $w \in A^*$ цій мові

Задано: $w \in A^*$

Розпізнати: $w \in L$.

Задано: $x \in \mathbf{N}$

Розпізнати: чи є x повним квадратом?

Задача пошуку елемента із задаю властивістю

Задано: $w \in A^*$

Знайти: u таке, що $w\#u \in P$.

Задано: $x \in \mathbf{N}$

Знайти: $y \in \mathbf{Z}$ таке, що $x = y^2$.

Алгоритми

Команди – слова, з яких складається прямолінійна програма.

Складність прямолінійної програми – кількість її команд:

- ***мультиплікативна складність*** – кількість команд множення
- ***адитивна складність*** – кількість команд додавання

Складністю обчислення функції F прямолінійної програми називається найменша довжина прямолінійної програми, яка обчислює F. $F(x) = x^4 + x^2$

$$z_1 = x \times x$$
$$z_2 = z_1 \times x$$
$$z_3 = z_2 \times x$$
$$z_4 = z_3 + z_1$$

$$z_1 = x \times x$$
$$z_2 = z_1 + 1$$
$$z_3 = z_1 \times z_2$$

Піднесення до степеня

$f(x) = x^d$ Р

$$z_1 = x \times x$$
$$z_2 = z_1 \times x$$
$$z_3 = z_2 \times x$$
$$\dots$$
$$z_{d-1} = z_{d-2} \times x$$

Бінарний метод піднесення до степеня

Задано: x 挝Z_n, d N. Потрібно обчислити $x^d \bmod n$.

Можна вважати, що $d < n$. Якщо це не так, то степінь можна понизити за теоремою Ейлера.

Подамо d у двійковій системі числення:

$$d = d_l 2^l + d_{l-1} 2^{l-1} + \ldots + d_1 \times 2 + d_0$$

Покладемо $z_0 = 1$ і для $i = 2,\ldots,l+1$ обчислимо

$$z_i = \begin{cases} z_{i-1} \times z_{i-1}, \text{ якщо } d_{l+1-i} = 0 \\ z_{i-1} \text{鬃}_{i-1}\ x, \text{ якщо } d_{l+1-i} = 1 \end{cases}$$

Легко бачити, що $z_i = z_{i-1}$ 鬃$_{i-1}\ x^{d_{l+1-i}}$. На $l+1$ кроці маємо:

$$(\ldots((x^{d_l})^2 x^{d_{l-1}})^2 x^{d_{l-2}} \ldots)^2 = x^{d_l 2^l + d_{l-1} 2^{l-1} + \ldots + 2 \times d_0} = x^d$$

Для обчислення $x^d \bmod n$ бінарним методом потрібно $2l$ Î 轩 $l-1$ 编 + å $d_i, 2\log_2 d$ 鳎 $i=0$ 龋 множень.

Випадковий вибір

Випадкова двійкова послідовність довжини l може розглядатися як двійковий запис випадкового елемента з Z_n при $n = 2^l$ або випадкового елемента з Z_p^* для простого $p = 2^l + 1$.

Якщо n (або просте p) довільне, використовують такий алгоритм:

1. обчислити $l = [\log_2 n]$
2. вибрати випадковий елемент $x \in Z_{2^l}$.
3. якщо $x \geq n$, то перейти на крок 2.

Позначимо a - ймовірність того, що вибраний на кроці 2 $x < n$. Очевидно, $a > 1/2$.
Ймовірність того, що x попаде в Z_n лише за i-им разом, дорівнює $b_i = a(1-a)^{i-1}$.

Тоді $\sum_{i=1}^{N} i b_i = a \sum_{i=1}^{N} i(1-a)^{i-1} = \frac{1}{a} < 2$

Тобто математичне сподівання кількості повторів кроку 2 не перевищує 2.

Якщо потрібно знайти випадковий $x \in Z_{pq}^*$ (p, q - прості числа), то можна використати наслідок з китайської теореми про остачі:

1. знайти випадкові елементи $x_1 \in Z_p^*$ та $x_2 \in Z_q^*$
2. обчислити $x \in Z_{pq}^*$, для якого $x_1 = x \bmod p$ та $x_2 = x \bmod q$.

Розглянемо ще один спосіб знаходження випадкового елемента $x \in Z_{pq}^*$, який використовується у випадку великих значень p та q:

1. вибрати випадковий елемент $x \in Z_{pq}$
2. якщо $x \bmod p = 0$ або $x \bmod q = 0$, перейти на крок 1.

Ймовірність того, що x, вибраний на кроці 1, буде належати множині Z_{pq}^*, дорівнює

$$a = \frac{f(pq)}{pq} = \frac{(p-1)(q-1)}{pq} = \left(1 - \frac{1}{p}\right)\left(1 - \frac{1}{q}\right).$$

Подібний алгоритм можна використовувати для знаходження випадкового елемента $x \in Z_n^*$ для довільного n:

1. вибрати випадковий елемент $x \in Z_n$ і обчислити $\text{НСД}(x, n)$
2. якщо $\text{НСД}(x, n) > 1$, перейти на крок 1.

Первісні корені

Нехай $p \in N$. Число $g \in Z$ називається ***первісним коренем за модулем*** p**,** якщо лишок $g \bmod p$ є твірним елементом групи Z_p^*.

Для простого p група Z_p^* (як мультиплікативна група для скінченного поля) є циклічною. Тому первісні корені існують для всіх простих модулів.

Число g є первісним коренем за простим модулем p, якщо послідовність

$$g^0 \bmod p = 1, g^1 \bmod p, g^2 \bmod p, ..., g^{p-2} \bmod p \qquad (1)$$

містить всі елементи множини Z_p^*. Ця умова рівносильна тому, що всі елементи послідовності (1) попарно різні.

Приклад. $g = 5$ є первісним коренем за модулем $p = 23$. Послідовність (1) у цьому випадку така: 1,5,2,10,4,20,8,17,16,11,9,22,18,21,13,19,3,15,6,7,12,14.

Твердження. Нехай p - просте число і $p - 1 = q_1^{a_1} q_2^{a_2} \ldots q_s^{a_s}$ - розклад $p - 1$ на прості співмножники. Тоді:

1. в Z_p^* є рівно $f(p - 1)$ первісних коренів за модулем p
2. для того, щоб число $g \in Z$ було первісним коренем за модулем p, необхідно та достатньо, щоб

$$g^{(p-1)/q_i} \neq 1 \pmod{p}, \quad i = 1, \ldots, s \qquad (2)$$

Приклад.

Нехай $p = 29 \Rightarrow (p - 1) = 2^2 \times 7$.

Оскільки $2^{14} \equiv 28 \pmod{29}$, $2^4 \equiv 16 \pmod{29}$ $\Rightarrow$ $g = 2$ – первісний корінь за модулем $p = 29$.

$g = 5$ не є первісним коренем за модулем $p = 29$ оскільки $5^{14} \equiv 1 \pmod{29}$.

Квадратичні лишки

Нехай $n \in N$. Ціле число $x \in Z$ називається ***квадратичним лишком за модулем*** n, якщо $\text{НСД}(x,n) = 1$ і $x \equiv y^2 (\text{mod}\, n)$ для деякого числа y. У цьому випадку y називається ***квадратним коренем з*** x за модулем n.

Якщо $\text{НСД}(x,n) = 1$ і x не є квадратичним лишком за модулем n, то x називається ***квадратичним нелишком*** за модулем n.

Квадратичні лишки за модулем n, які набувають значення від 1 до $n-1$, називаються *зведеними*. Множину зведених квадратичних лишків за модулем n позначимо Q_n.

Твердження. Нехай p – непарне просте число. Тоді наступні умови еквівалентні:

1. x є квадратичний лишком за моделям p

2. $x^{(p-1)/2} \equiv 1 (\text{mod}\, p)$

3. Якщо $g \in Z_p^*$ – первісний корінь за модулем p, то для деякого парного k в Z_p^* виконується рівність $x = g^k$.

Критерій Ейлера. Нехай x - ціле, p - непарне просте. Тоді

$$\left(\frac{x}{p}\right) \equiv x^{\frac{p-1}{2}} \pmod{p},$$

де $\left(\frac{x}{p}\right)$ - символ Лежандра:

$$\left(\frac{x}{p}\right) = \begin{cases} 1, & \text{якщо } x \text{ є квадратичним лишком за модулем } p \\ -1, & \text{якщо } x \text{ є квадратичним нелишком за модулем } p \\ 0, & \text{якщо } p \mid x \end{cases}$$

Властивості символу Лежандра. Нехай p - непарне просте, $x_1, x_2 \in Z$. Тоді:

1. $x_1 \equiv x_2 \pmod{p}$ $\Rightarrow$ $\left(\frac{x_1}{p}\right) = \left(\frac{x_2}{p}\right)$

2. мультиплікативність: $\left(\frac{x_1}{p}\right)\left(\frac{x_2}{p}\right) = \left(\frac{x_1 x_2}{p}\right)$

3. $x_2 \pmod{p} > 0$ $\Rightarrow$ $\left(\frac{x_1 x_2^2}{p}\right) = \left(\frac{x_1}{p}\right)$

Символ Якобі

Нехай $n \geq 3$ – непарне ціле число з розкладом на прості співмножники $n = p_1^{a_1} p_2^{a_2} \ldots p_s^{a_s}$, $x \in Z$. Означимо *символ Якобі*:

$$\left(\frac{x}{n}\right) = \left(\frac{x}{p_1}\right)^{a_1} \left(\frac{x}{p_2}\right)^{a_2} \ldots \left(\frac{x}{p_s}\right)^{a_s}.$$

Очевидно, що для простого n символ Якобі буде символом Лежандра.

Властивості символу Якобі. Нехай $x, x_1, x_2 \in Z$, n, n_1, n_2 – непарні цілі числа, більші за 2. Тоді:

1) $x_1 \equiv x_2 \pmod{n} \Rightarrow \left(\frac{x_1}{n}\right) = \left(\frac{x_2}{n}\right)$

2) $\left(\frac{x_1}{n}\right)\left(\frac{x_2}{n}\right) = \left(\frac{x_1 x_2}{n}\right)$

3) $\text{НСД}(x_2, n) = 1 \Rightarrow \left(\frac{x_1 x_2^2}{n}\right) = \left(\frac{x_1}{n}\right)$

4) $\left(\frac{x}{n_1 n_2}\right) = \left(\frac{x}{n_1}\right)\left(\frac{x}{n_2}\right)$

5) якщо x – квадратичний лишок за модулем n, тоді $\left(\frac{x}{n}\right) = 1$.

Квадратичний закон взаємності Гауса. Нехай $m, n > 2$ - взаємно прості непарні натуральні числа. Тоді

1) $\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = (-1)^{\frac{(m-1)(n-1)}{4}}$ 2) $\left(\frac{2}{n}\right) = (-1)^{\frac{n^2-1}{8}}$

Алгоритм обчислення символу Якобі. Можна вважати, що $0 < x < n$, оскільки $\left(\frac{x}{n}\right) = \left(\frac{x \bmod n}{n}\right)$ на основі властивості 1. кожен наступний крок алгоритму зводить обчислення $\left(\frac{x}{n}\right)$ до обчислення $\left(\frac{x'}{n'}\right)$, де $x' < x$ і $n' \le n$.

1. Якщо $x = 2^{2j} y$, то за властивістю 3 отримаємо $\left(\frac{x}{n}\right) = \left(\frac{y}{n}\right)$.
2. Якщо $x = 2^{2j+1} y$, то за властивостями 3 та 2 маємо $\left(\frac{x}{n}\right) = \left(\frac{2}{n}\right)\left(\frac{y}{n}\right) = \left(\frac{y}{n}\right)$.

На підставі пункту 2) квадратичного закону взаємності отримаємо

$$\left(\frac{2}{n}\right) = (-1)^{\frac{n^2-1}{8}}.$$

3. Якщо x непарне, то з пункту 1) квадратичного закону взаємності випливає

$$\left(\frac{n}{x}\right) = \left(\frac{n \bmod x}{x}\right)(-1)^{\frac{(x-1)(n-1)}{4}}.$$

Виконання кроків алгоритму неминуче зведе обчислення $\left(\frac{x}{n}\right)$ до обчислення символу Якобі виду $\left(\frac{1}{n'}\right)$, який (за властивістю 5) дорівнює 1 для довільного непарного n'.

Приклад.

$$\left(\frac{2}{17}\right)\left(\frac{3^2}{17}\right)\left(\frac{2^2}{17}\right)\left(\frac{3}{17}\right) = \left(\frac{3}{17}\right)\left(\frac{17 \bmod 3}{3}\right)(-1)^{\frac{(3-1)(17-1)}{4}} = \left(\frac{2}{3}\right) = (-1)^{\frac{3^2-1}{8}} = -1$$

Розподіл простих чисел

Позначимо $p(n)$ - кількість простих чисел, не більших за n.

Теорема Чебишева (1850р.). Для довільного $n \geq n_0 > 1$ виконуються нерівності

$$\frac{0.92n}{\ln n} < p(n) < \frac{1.1n}{\ln n}.$$

Теорема Адамара – Валле Пуссена.

$$\lim_{n\to\infty} p(n)\frac{\ln n}{n} = 1.$$

Теорема. Для довільного $n \geq 55$ виконуються нерівності

$$\frac{n}{\ln n} < p(n) < \frac{n}{\ln n - 4}.$$

Ліва нерівність виконується при $n \geq 17$.

Постулат Бертрана. Для довільного $n > 2$ існує просте $p \in [n, 2n-2]$.

Теорема. Для довільного $n > 2$ існує просте $p \in [n, n + n^{107/200}]$.

Гіпотеза. Для довільних $c > 2, n > 2$ існує $d > 0$ таке, що інтервал $[n, n + d \times (\log n)^c]$ містить просте число.

Тестування простоти

Алгоритми перевірки, чи число $n \in N$ є простим, називаються тестами простоти.

Сито Ератосфена.

Покладемо $l = 2$.

1. Якщо $l > [n/2]$, тоді алгоритм завершити з результатом n - просте.
2. Якщо $l \le [n/2]$ і $l \mid n$, тоді алгоритм завершити з результатом n - складене.
3. Якщо $l \le [n/2]$ і l не ділить n, покласти $l = l + 1$ та перейти до кроку 1.

Цей алгоритм належить до класу детермінованих і має експоненційну (від n) кількість обчислень.

Найкращий на сьогодні детермінований алгоритм має квазіполіноміальну кількість обчислень $O((\log n)^{c \log\log\log n}), \quad c > 0.$

Ймовірносний тест Соловея-Штрассена.

Для непарного $n \geq 3$ означимо $S_n = \{x \in Z_n^* : x^{\frac{n-1}{2}} \equiv \left(\frac{x}{n}\right) \pmod{n}\}$.

Якщо n - складене, тоді $|S_n| \leq f(n)/2$.

Алгоритм.

1. Вибрати випадковий елемент $x \in [1, n-1]$.
2. Якщо $\text{НСД}(x,n) > 1$, тоді алгоритм завершити з результатом n - складене.
3. Якщо $\left(\frac{x}{n}\right) \neq x^{\frac{n-1}{2}} \pmod{n}$, тоді алгоритм завершити з результатом n - складене.
4. Якщо ж $\left(\frac{x}{n}\right) = x^{\frac{n-1}{2}} \pmod{n}$, алгоритм завершити з результатом n - просте.

Тест побудовано на твердженні, що n є простим тоді і лише тоді, коли

$$\text{НСД}(x,n) = 1 \quad \text{і} \quad \left(\frac{x}{n}\right) = x^{\frac{n-1}{2}} \pmod{n}.$$

Якщо n - просте, то для довільного $x \in [1, n-1]$ перша рівність справедлива за означенням простого числа, а друга – за теоремою Ейлера. А тому для простого n тест завжди дає правильну відповідь.

Якщо ж n - складене, то ці дві умови справедливі лише для $x \in S_n$, тобто ймовірність хибної відповіді дорівнює

$$\frac{\|S_n\|}{n-1} = \frac{f(n)}{2(n-1)} < \frac{1}{2}.$$

Алгоритми обчислення $\text{НСД}(x, n)$ (алгоритм Евкліда), символу Якобі та $x^{\frac{n-1}{2}} \pmod n$ (бінарний метод) роблять $O(\log n)$ операцій множення у кільці Z_n. А тому ймовірнісний тест Соловея-Штрассена має поліноміальну кількість обчислень.

Повторимо тест k разів. Ймовірність того, що k разів буде хибне твердження, менша за $\frac{1}{2^k}$.

Псевдопрості числа

Мала теорема Ферма Якщо n - просте, то $x^{n-1} \equiv 1 (\mathrm{mod}\, n)$ для довільного $x \in Z_n^*$.

Непарне складене n називається *псевдопростим за основою* x, якщо

$$x^{n-1} \equiv 1 (\mathrm{mod}\, n),\ x \in Z_n^*$$

Деякі складені числа є псевдопростими за довільною основою $x \in Z_n^*$. Вони називаються *числами Кармайкла*. Найменше з них – $561 = 3 \cdot 11 \cdot 17$.

Критерій Ейлера стверджує: якщо n - непарне просте, то $\left(\frac{x}{n}\right) \equiv x^{\frac{n-1}{2}} (\mathrm{mod}\, n)$ для довільного $x \in Z_n^*$.

Непарне складене n називається *псевдопростим числом Ейлера за основою* x, якщо

$$\left(\frac{x}{n}\right) \equiv x^{\frac{n-1}{2}} (\mathrm{mod}\, n),\ x \in Z_n^*$$

Нехай n - непарне і $n - 1 = 2^s t$, де t - непарне. Нехай $x \in Z_n^*$.

Якщо або $x^t \equiv 1 (\mathrm{mod}\, n)$, або існує $j \in [0, s]$ таке, що $x^{2^j t} \equiv -1 (\mathrm{mod}\, n)$, то n називається *сильно псевдопростим числом за основою* x.

Теорема.

1. Кожне псевдопросте число Ейлера за основою x є також псевдопростим Ферма за основою x.
2. Сильно псевдопросте число за основою x є також псевдопростим Ейлера за основою x.
3. Непарне складене число n є сильно псевдопростим за основою x щонайбільше для четвертої частини всіх $x \in [1, n-1]$.

Доведено, що лише число 3 215 031 751 є сильно псевдопростим за кожною із основ 2, 3, 5, 7 серед чисел, менших за 25×10^9. Тому для тестування простоти числа $n < 25 \times 10^9$ достатньо перевірити його на сильну псевдопростість за основами 2, 3, 5 та 7.

Ймовірнісний тест Міллера-Рабіна

Нехай n - непарне натуральне число і $n - 1 = 2^s t$, де t - непарне. Сформулюємо алгоритм тестування числа n на простоту.

1. Вибрати випадкове число $x \in [1, n-1]$.
2. Якщо $\text{НСД}(x, n) \neq 1$, тоді алгоритм завершити з результатом n - складене.
3. Обчислити $y_0 = x^t \pmod n$.
4. Якщо $y_0 \neq 1 \pmod n$, тоді алгоритм завершити з результатом n - просте.
5. Обчислювати $y_1 = y_0^2 \pmod n, \ldots, y_j = y_{j-1}^2 \pmod n$, доки при деякому j матимемо: $y_j \neq 1 \pmod n$.
6. Якщо $y_j = 1 \pmod n$, то n - складене, а якщо $y_j = -1 \pmod n$, то n - просте.

Для простого n тест Міллера-Рабіна завжди дає позитивний результат.

У випадку складеного n тест може зробити неправильний висновок з імовірністю не більшою за $\frac{1}{4}$.